COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 12 December 2008

MONEYVAL (2008) 32

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

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

THIRD ROUND DETAILED ASSESSMENT REPORT ON ESTONIA[1]

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

Memorandum
prepared by the Secretariat
Directorate General of Human Rights and Legal Affairs

[1] As adopted by the MONEYVAL Committee at its 28th Plenary Session (Strasbourg, 8 – 12 December 2008).

TABLE OF CONTENTS

I. PREFACE

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of Estonia was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), together with 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 "3rd EU AML 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* (hereinafter "Implementing Directive 2006/70/EC"), in accordance with MONEYVAL's terms of reference and Procedural rules, and was prepared using the AML/CFT Methodology 2004[2]. 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 Tallinn from 3 to 9 February 2008, and subsequently. During the on-site visit, the evaluation team met with officials and representatives of all relevant Estonian government agencies and the private sector. A list of the bodies met is set out in Annex I to the mutual evaluation report.

2. The evaluation team comprised: Ms Csilla ALFÖLDY (executive officer, Hungarian National Bureau of Investigation, Economic Crime Department, Hungary), Ms Mitka ZAHARLIEVA (Head of International Cooperation Department, Ministry of Justice, Bulgaria), Mr Michalis STYLIANOU (Senior Officer, Bank Supervision and Regulation Department, Central Bank of Cyprus, Cyprus); Mr André CORTERIER (Anti-Money Laundering Group, Bundesanstalt für Finanzdienstleistungsaufsicht - BaFin, Federal Financial Supervisory Authority, Germany); and a member of the MONEYVAL Secretariat. The examiners reviewed the institutional framework, the relevant AML/CFT Laws, regulations and guidelines and other requirements, and the regulatory and other systems in place to deter money laundering and financing of terrorism through financial institutions and designated non-financial businesses and professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all the systems.

3. This report provides a summary of the AML/CFT measures in place in Estonia as at the date of the on-site visit or immediately thereafter. It describes and analyses these measures, and provides recommendations on how certain aspects of the systems could be strengthened (see Table 2). It also sets out Estonia's levels of compliance with the FATF 40 + 9 Recommendations (see Table 1). Compliance or non-compliance with the EC Directives has not been considered in the ratings in Table 1.

[2] As updated in February 2007.

II. EXECUTIVE SUMMARY

1. Background Information

4. This report provides a summary of the AML/CFT measures in place in Estonia as at the date of the on-site visit from 3 to 9 February 2008 or immediately thereafter. It describes and analyses these measures, and provides recommendations on how certain aspects of the system could be strengthened (see Table 2). It also sets out Estonia's levels of compliance with the FATF 40 plus 9 Recommendations (see Table 1). The evaluation also includes Estonia's compliance with *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 "3rd EU AML 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* (hereinafter "Implementing Directive 2006/70/EC"). However, compliance or non-compliance with the 3rd EU AML Directive and the Implementing Directive 2006/70/EC has been described in a separate Annex but it has not been considered in the ratings in Table 1.

5. Since the last evaluation there have been significant changes. On 28 January 2008 the new Money Laundering and Terrorist Financing Prevention Act (MLFTPA) entered into force. One of the goals of the new MLTFPA was to harmonise Estonian legislation with the requirements of the 3rd EU AML Directive and Implementing Directive 2006/70/EC. Though it is too early to evaluate the effectiveness of this law, it can already be said that it will significantly strengthen the AML/CFT regime of Estonia. It seems that Estonia now has a sound legal and institutional AML/CFT system and also the results achieved on the basis of the previous legislation are respectable. This assessment is also supported by the fact that there was a good understanding of AML/CFT issues from representatives of the private sector with which the evaluation team met.

6. Turning to the money laundering situation, Estonian authorities advised that it is difficult to establish what crimes have to be considered as typical predicate offences for money laundering in Estonia; the difficulty with such a statement is the small number of money laundering cases so far which does not allow on the identification of trends and typologies. However, in the cases which have been undertaken, violation of the procedure for handling alcohol and/or tobacco products, larceny of forest, computer-related fraud, theft, accepting gratuities and accepting bribes have been predicate offences. Current investigations also indicate that fraud (especially internet fraud), tax crime and drug offences are predicate offences in a number of money laundering cases. In many ongoing cases the predicate offences are committed abroad or the victims are abroad (especially concerning Internet fraud cases).

7. Concerning terrorist financing, the Estonian authorities advised that so far no cases of terrorist financing or any other offences connected with terrorism are known to have been committed on the territory of Estonia or via Estonia. According to Europol's "Terrorist Activity in the European Union: Situation and Trends Report (2006)"[3], Estonia belongs (with 6 other countries) to the least threatened EU countries by terrorism and activities supporting terrorism. It was stated by the Estonian authorities that there were no active terrorist groups in Estonia at the end of 2006 or supporters or financiers of international terrorist organisations. Although such activities cannot be excluded for the future, the Estonian authorities consider it very unlikely.

[3] http://www.statewatch.org/news/2006/may/europol-terr-rep-2004-2005.pdf.

2. Legal Systems and Related Institutional Measures

8. Since the last MONEYVAL evaluation, Estonia has improved its legal framework for the criminalisation of money laundering. The rewording of the definition of the money laundering offence brought it very close to the language of the international conventions on the physical aspects of the offence. Estonia applies an all crimes approach and all the designated offences under the FATF Recommendations can be predicate offences for money laundering, including terrorist financing (as far as it is criminalised in Estonia; concerning the deficiencies in implementation see below para 13).The law now clearly criminalizes money laundering if predicate criminal activity has taken place abroad. It is also positive that the reference to laundered proceeds as property acquired as a direct result of an act punishable pursuant to criminal procedure has been removed. Thus, Estonia may prosecute now for money laundering if the property at stake is acquired directly or indirectly by crime. Money laundering is punishable both with regard to natural and legal persons if committed intentionally (negligent money laundering is not criminalised).

9. There was unanimity amongst prosecutors and judges and also court practice showed that self-laundering is prosecutable in Estonia. However, no such unanimity could be established on the term "*criminal activity*" which replaced the term "*crime*" as underlying criminality for money laundering. The intention of the law drafters (Ministry of Justice) was to relieve the practitioners from the burden of a prior or simultaneous conviction for the predicate offence as required by the previous MLTFPA (which is also mirrored by the fact that all money laundering convictions so far were prosecuted together with the relevant predicate offences or after a conviction for the respective predicate offence). Both the judges and prosecutors would have preferred different language clearly stating that a conviction for the predicate offence is not a prerequisite for the money laundering offence. It is too early to see how practice will interpret this and what level of proof for the underlying predicate crime will be required for a money laundering conviction, i.e. whether a conviction or at least indictment for the predicate offence is a prerequisite for a money laundering conviction. Thus, there are some uncertainties whether the changes in legislation will now allow the conviction of somebody for money laundering without a prior or simultaneous conviction for the predicate offence.

10. Estonian law covers attempt, aiding and abetting, facilitating, and counselling the commission of money laundering. However, Estonia has not yet introduced the full concept of conspiracy for the money laundering offence.

11. Between 2005 and February 2008, 8 convictions for money laundering were achieved in Estonia. 12 natural persons and 1 legal person were convicted. The predicate offences covered various types of crimes (see above para 6). The penalties imposed were between 2,6 to 5 years of imprisonment (all on probation or partially on probation) and the compulsory dissolution of a legal person. Considering the size of the country, the number of inhabitants and the money laundering threats it is exposed to, the number of convictions can be described as satisfactory though more would be preferable.

12. With regard to the criminalisation of terrorist financing, it can be noted that Estonia has ratified the United Nations Convention on the Suppression of Terrorist Financing. In recent years Estonia significantly improved its legal framework for criminalising the financing of terrorism. There is a clear provision dealing with the financing of terrorist acts and also the financing of terrorist organisations is present in Estonian legislation. Financing of terrorism is also a predicate offence for money laundering (as a consequence of the all crimes approach). The sanctions envisaged for terrorist financing offence seem to be effective, proportionate and dissuasive; however, in absence of terrorist financing prosecutions they have never been applied.

13. However, there are some elements of the international requirements which are not covered explicitly enough. One of the major shortcomings is that the financing of individual terrorists is missing. This was also acknowledged by the Estonian authorities who had at the time of the on-site visit already prepared a draft law to remedy this shortcoming. Furthermore, a more detailed provision on financing of terrorism would be preferable to cover explicitly the various elements of the international requirements in a consistent way and with a sufficient degree of legal certainty; e.g. the Penal Code does not cover "*collecting of funds*". The law also does not specifically criminalise the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist. In addition, some conducts as referred to in Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions are not covered.

14. The evaluation team also noted progress in the legislative framework covering confiscation. As of 1 February 2007, confiscation of proceeds of crime is mandatory (§ 83^1 Penal Code) and (according to the firm and unanimous interpretation of judges and prosecutors) may extend to direct and indirect proceeds of crime and to proceeds belonging to third parties. A possibility for *extended confiscation* was introduced where the principle of reversed burden of proof is applied (§ 83^2 Penal Code): in such cases the accused person has to establish the lawful origin of the alleged proceeds of crime.

15. The legislative framework for provisional measures has been improved as well. The new provisions on seizure and confiscation were assessed very positively by practitioners (investigators and prosecutors) and are being widely used by them. This applies also for international co-operation – there are good examples of provisional measures, confiscation and sharing assets with foreign countries in recent Estonian practice.

16. However, there are still some important elements missing in the confiscation and provisional measures regime:
    - 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 applies to only part of the designated 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).

17. Estonia implements the United Nations Security Council Resolutions 1267(1999) and its successor resolutions and 1373(2001) through European Union legislation. However, the definition of "funds" as provided in European Union legislation is not broad enough as required by the aforementioned Resolutions: EC Regulation 881/2002 requires the freezing of all funds and economic resources belonging to, owned or held by a designated person but does not cover funds controlled by them or persons acting on their behalf or at their direction (as required by UNSCR 1267 and 1373). In addition, there is no national system in place which provides for internal implementation of UN Resolutions. Thus, apart from banks no other financial institutions or DNFBP are aware of the procedure to be followed in order to implement the UN Resolutions. There are no publicly-known procedures in place for de-listing, unfreezing or granting access to funds for living expenses. However, the Estonian authorities are aware that the regulation of publicly known procedures for de-listing, unfreezing or granting access to funds for living expenses is undetermined. Thus, a working-group is preparing a draft for a new International Sanctions Act which will address these issues.

18. The Estonian Financial Intelligence Unit (FIU) is a police-type FIU and was established as a separate division under the Criminal Investigation Department of the Police Board on 1 July 1999.

With the coming into force of the previous MLTFPA (1 January 2004), the FIU was made an independent structural unit of the Central Criminal Police. At the time of the on-site-visit, there were 18 staff in place and 6 vacancies. The FIU has all the investigative techniques to fulfil its functions. It has access to various databases and the potential to link data is impressive. It appears to be fully operational, but for exercising its very wide supervision duties in a satisfactory manner it may be necessary to increase staff (going beyond than filling the vacancies). Art. 36 of the MLTFPA is intended to provide independence of the FIU by stating that the FIU is an independent structural unit of the Central Criminal Police. Though the law says that the FIU has to be provided with sufficient funds for performance of its functions, it does not further expand on this, and the FIU has no own budget and depends on the Central Criminal Police when it comes to budgetary issues: The Police Board provides the Financial Intelligence Unit with funds necessary for the performance of the functions provided by law. This means that the FIU is dependent on the Central Criminal Police on budgetary issues such as hiring the staff, salaries and trips to foreign countries. The FIU may have certain influence on the budget as it can make a yearly calculation of expenses or give some explanations of the use and purposes of the necessary amount to the chief commissioner of the Central Criminal Police, but does not have any influence on the final decision. Though this does not appear to be a problem at present, a separate budget would certainly strengthen the independence of the FIU.

19. The FIU cooperates with other authorities both on a domestic and an international level. It is also well regarded by the obliged entities and provides good feedback. The FIU is an active member of the Egmont Group. It has the capacity to exchange information on any data and all relevant banking information with all types of FIU. It is entitled to request additional information from the obligated institutions; only advocates are not covered by this obligation.

20. In general, Estonia has a comprehensive system for reporting suspected money laundering and terrorist financing. The reporting obligation covers reporting of suspicious transactions and - also since 28 January 2008 - above threshold cash transactions (500 000 EEK; 31 955.82 EUR) with certain exceptions. However, some shortcomings exist which should be remedied:
    a) Not all kind of attempted transactions are clearly covered by the reporting obligations.
    b) There is no reporting obligation in case of:
        a) financing of an individual terrorist;
        b) collecting of funds for the purpose of terrorist financing;
        c) the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist;
        d) those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC).

21. Statistics show an increasing trend concerning STRs received by the FIU and cases forwarded to investigative bodies and for prosecution. It can also be concluded that there have been sufficient prosecutions arising out of reports received by the FIU. However, it can also be seen from statistics that savings and loan associations as well as the insurance sector sent no STRs, and lawyers, real estate dealers as well as accountants and auditors sent only a very small number of STRs. The reasons for this underreporting are not entirely clear but further outreach to these entities to enable them to better understand their reporting obligations may help (though it has be noted that the Estonian FIU already provided a number of training seminars to a number of these entities).

22. The number of money laundering related investigations and convictions are adequate with regard to the total number of STRs. Overall from the law-enforcement side the AML and CFT measures seem to be generally in place and effective.

23. Estonia has a new declaration system in place (following *Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or*

leaving the Community). This covers only the transfer of cash or bearer negotiable instruments when entering or leaving the European Union territory and not between Estonia and another EU member-state, which is a requirement of Special Recommendation IX[4].

3. Preventive Measures – financial institutions

24. Turning to the preventive side, most of the provisions dealing with AML/CFT issues can be found in the new MLTFPA. § 3 MLTFPA defines the "*obligated persons*" under the Act, to which the requirements set out in the MLTFPA apply. The MLTFPA sets out a number of provisions which apply equally to DNFBP and financial institutions. Where applicable, the MLTFPA makes specific mention of "*credit and financial institutions*" when measures are required only for these entities. Additionally relevant primary legislation to which the MLTFPA makes reference and which supply additional abilities to government authorities, for example regarding their sanctioning power, exists, e.g. the Credit Institutions Act (CrIA), Insurance Activities Act, Securities Market Act, etc. Primary legislation in many cases gives the authority to create secondary legislation regarding specific subsets of the subject matter of the primary legislation. The MLFTPA has specified that the Minister of Finance shall issue secondary law for areas with low money laundering or terrorist financing risks according and regarding AML/CFT-specific internal rules of procedure for credit and financial institutions. Such secondary law was created with the Minister of Finance Regulations 11 and 10, respectively, both of 3 April 2008. As both came into force only on 11 April 2008 (date of the publication in the Official Gazette) and moreover the Minister of Finance Regulation No 10 stipulates in its § 30 that "*Credit and financial institutions must bring their activities and documents into compliance with the provisions of this Regulation by no later than 1 November 2008*", it was not taken into account in the descriptive part of the report and for rating purposes; where appropriate it was referred to it with a footnote.

25. The new MLTFPA, which transposes the requirements of the 3rd EU AML Directive into domestic legislation, remedied a large number of shortcomings in the Estonian AML/CFT regime. The new MLFTPA now brings all of the relevant professions into the remit of the legal AML/CFT requirements. This particularly relates to providers of trust and company services, providers of payment services, providers of services of alternative means of payment and pawnbrokers.

26. It is fair to say that the new MLTFPA provides a sound legal basis concerning preventive measures. Though the shortcomings of Estonia's preventive law are in the majority of cases only of minor nature, some shortcomings are more severe. A certain shortcoming of the new MLTFPA is its sanctioning regime as the MLTFPA does not provide (direct) administrative sanctions for all of its obligations. Several provisions need to become enforceable via precepts which have to be issued either by the Financial Supervision Authority (FSA) or the FIU. This way of enforcing provisions of the MLTFPA via indirect sanctioning does not amount to a dissuasive and effective sanctioning regime as it is not possible to sanction violations which already have happened; it only allows the issuance of precepts (which can be regarded from a practical point of view like warning letters) to sanction future infringements or failure to comply with the demands made in the precept. Moreover, the amount of the sanctions (a fine up to 50 000 EEK, i.e. 3 195.58 EUR, for the first occasion and 750 000 EEK, i.e. 47 878.53 EUR, for each subsequent occasion) is not proportionate, effective and dissuasive when it comes to the sanctioning of legal persons. This is particularly of concern as a number of obligations outlined in Chapter 2 of the MLTFPA (with the title "Due Diligence") are not covered by a direct sanctioning regime: e.g. constant monitoring of a business relationship, regular verification of data, opening anonymous accounts or saving books,

[4] It has to be noted that the European Commission proposed amendments to the FATF Methodology and to consider in the context of Special Recommendation IX the European Community as one jurisdiction. As a consequence this would not be considered a shortcoming any more. This issue is currently under consideration by the FATF and was at the time of the adoption of this report not yet solved.

some elements of enhanced CDD and treatment of PEPs which are not related to the identification process, correspondent banking provisions.

27. Apart from the sanction regime which amounts to a substantial deficiency of the MLTFPA, the following shortcomings with regard to implementation of Recommendation 5 should be mentioned:
    - Concerning beneficial ownership, the language in the law is not clear as to whether it also covers instances when a natural person acts for another natural person.
    - The Estonian approach to address "*high risk of money laundering or terrorist financing*" sets the level to apply enhanced CDD measures to a higher level than "*higher risk*" in terms of the Methodology. Though the difference in language seems small, it has to be highlighted that there is a difference between "high risk" and "higher risk": while "high risk" is at the upper end of a level of risk, "higher risk" refers only to a situation more risky than average. In this context it is interesting to note that non-resident customers and private banking are not outlined as higher risk situations for money laundering or terrorist financing which would require enhanced due diligence measures; this is particularly surprising concerning the geopolitical position of Estonia and its number of non-resident accounts. Thus, it is recommended that Estonia should change the term of "*high risk*" to "*higher risk*" and consider adding non-resident customers and private banking to the categories which require enhanced CDD measures.

28. 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. Such an exemption is not in line with FATF Recommendation 6 and should be removed. In practice, 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. The larger, internationally active banks generally check one or more of the relevant private-sector databases during their client take-on procedures, which should generate information indicating whether a customer is a politically exposed person.

29. There are no *specific* provision in the law which address financial institutions to have policies in place or take such measures as may by needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

30. With regard to FATF Recommendation 11, it has to be noted that financial institutions are not required to examine the background and the purpose of complex/unusual large transactions and thus to keep a record of the written findings which will be accessible for competent authorities/auditors.

31. The existing legal provisions do not adequately address the requirements of FATF Recommendation 21. Credit and financial institutions are not explicitly required to give special attention to business relationships and transactions with persons from countries which do not or insufficiently apply FATF Recommendations. The existing legal and regulatory framework contains general requirements regarding business relationships and transactions with persons from countries which insufficiently apply FATF Recommendations but does not adequately cover the essential criteria of FATF Recommendation 21. Furthermore, there are no requirements with regard to possible measures for advising credit and financial institutions of concerns and weaknesses in the AML/CFT systems of other countries, the investigation of unusual transactions and the application of counter measures against countries with deficient AML/CFT systems.

32. Concerning Special Recommendation VI, the evaluators were informed that no on-site visits have been made by the FIU to money transmitters and providers of alternative means of payment other than the Estonian Post, and no system for monitoring their operations has been introduced. Overall it has to be assumed that there is a lack of effective supervision of payment service providers.

4. Preventive Measures – Designated Non-Financial Businesses and Professions

33. As for financial institutions, the core obligations for DNFBP are based on the MLTFPA. The coverage of DNFBP in the MLTFPA is very complete and in line with both international standards and the 3rd EU AML Directive. Additionally Estonia has also added pawnbrokers (which are not required by international norms) to the obliged entities. The latter is the only class of professionals covered by the MLTFPA which goes beyond the EU Directive's requirements.

34. Since the core obligations for both DNFBP and financial institutions are based on the same law (i.e. the MLTFPA), it can be noted, that the obligations and also the deficiencies in the AML/CFT preventive measures framework as described for financial institutions apply to DNFBP in the same way as for financial institutions. To recap, DNFBP are obliged to perform client identification; gather and keep information on transactions; submit cash transaction reports and suspicious transaction reports to the FIU; and keep information confidential. A particularity and also a shortcoming concerning DNFBP is that they are not required to set up comprehensive internal control mechanisms for managing AML/CFT risks.

35. Another shortcoming of the law is that casinos are only required to identify but not to verify the name of a client who pays or receives in a single transaction or several related transactions an amount exceeding 30 000 EEK (1 917.34 EUR) or the equivalent in another currency.

36. Concerning effective implementation, it can be noted that the interviewees with whom the evaluation team met were also aware of the new MLTFPA (though not necessarily with its content as it came into force shortly before the on-site visit).

37. Concerning supervision of DNFBP with regard to AML/CFT issues some shortcomings have to be noted:
    a) The Estonian Bar Association and Chamber of Notaries have now been assigned as supervisory bodies for its members but there are some deficiencies concerning effective implementation:
        a) Neither the Estonian Bar Association nor the Chamber of Notaries have yet established mechanisms for supervision.
        b) It is not compulsory for a practising lawyer (independent legal professionals) to be a member of the Bar Association which means that they do not fall under the supervision of the Bar Association; for these lawyers, the FIU would be responsible for supervision but so far the FIU did not yet supervise any of them and it was also acknowledged that the number of lawyers acting outside may be higher than 116.
    b) The MLTFPA makes the Estonian FIU responsible for supervising compliance with the provision of the MLTFPA by organisers of games of chance (i.e. casinos and gambling houses), real estate agents, pawnbrokers, auditors, accountants, tax advisors and trust and company service providers. In 2007, the FIU made more than 200 on-site visits. As a result of this supervision activity, the number of STRs from these sectors increased significantly. However, as noted below (para 49), the evaluators have some doubts about whether the resources of the FIU are sufficient with regard to the high number of entities falling under its supervision competence. It is considered that, currently, the FIU lacks the required manpower to undertake appropriate supervision (as it is commonly understood) of all these entities.

5. Legal Persons and Arrangements & Non-Profit Organisations

38. There are various forms of companies established in Estonia for the purpose of undertaking business and they are required to be registered. The transparency with respect to the legal persons is provided through the register proceedings. Information on the shares of private limited liability companies is available in the Commercial register. The ownership of shares in public limited companies could be traced at the Estonian Central Register of Securities where the issuance of shares and their transfer are registered. As regards management and control, all commercial

companies are required to provide this information to the Commercial Register. The Commercial register is maintained by the Registration departments of County Courts. It contains information on sole proprietors, general partnerships, limited partnerships, private limited companies, public limited companies, commercial associations, European companies and branches of foreign companies. The register is maintained electronically. Entries in the commercial register are public. Everyone has the right to examine the card register and the business files, and to obtain copies of registry cards and of documents in the business files.

39. On the positive side it has to be noted that there are some safeguards in Estonian legislation that the information kept in registers is up to date. Measures are in place to ensure that companies submit their annual accounts, and lack of compliance with this may be sanctioned. There are even penal sanctions for submission of incorrect information to the registrars. However, while this seems to provide efficient measures on the side of the applicants, there are no similar requirements for registrars: though the registrar may demand supplementary documents from the undertaking if these are necessary to determine the facts which are the basis for an entry, but there is no obligation for verification of documents or any kind of ongoing supervision concerning 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.

40. Though the Estonian legal system does not allow for the creation of trusts or similar legal arrangements, it is possible for foreign trusts to operate in the country. However, there are no measures in place to access information on the beneficial ownership and control of these foreign trusts.

41. Concerning Special Recommendation VIII, in May 2007, the Security Police Board together with the Ministry of Justice reviewed the activities, size and other features of the domestic NPO-sector. As mentioned above, Estonia is said to belong to a group of countries which are the least threatened EU countries by terrorism and activities supporting terrorism, although some radical groups do seem to be trying to establish contacts in Estonia and neighbouring countries. However, there was no review of the adequacy of relevant laws and regulations to prevent the abuse of NPOs for the financing of terrorism which should be done as soon as possible. Moreover, there is no adequate system of supervision or monitoring concerning NPOs as envisaged by the Interpretative Note to SR VIII. The registers are electronically based and public, but the information they contain is not reliable: it is not checked and the registrars put in only the information sent by the respective persons. There is no clear supervisory power over the activity of the NPOs. With the exception of the audits conducted by tax authorities, there appears to be no active compliance monitoring by the authorities to ensure that the obligations of NPOs to submit information, keep records, etc are in fact complied with. There are not enough measures in place to prevent terrorist organisations from posing as legitimate non-profit organisations or to prevent funds or other assets collected by or transferred through such organisations being diverted to support the activities of terrorists or terrorist organisations, as required by Criteria VIII.2 and VIII.3.

6. National and International Co-operation

42. In order to improve the domestic AML/CFT legal and institutional framework, Estonian Government established in 2006 a so-called "Government Committee for Coordination of Issues Concerning Prevention of Money Laundering and Terrorist Financing" (hereinafter: Government Committee). It was intended that all the agencies engaged in the prevention of money laundering and terrorist financing are represented in this Committee. It is chaired by the Minister of Finance and consists of the following institutions:
    a) Ministry of Finance
    b) Ministry of Interior
    c) Ministry of Foreign Affaires
    d) Ministry of Justice

e) FIU
f) Advisory Committee of stakeholders
g) Bank of Estonia
h) FSA
i) Police Board
j) Security Police Board
k) Prosecutors' Office
l) Tax and Customs Board

43. The functions of the Government Committee 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 in force and coordinating drafting a new legislation;
- making proposals to the Government of Estonia for improving the measures for prevention of money laundering and terrorist financing and for amendments of the respective legislation;
- coordinating international co-operation on prevention of money laundering and terrorist financing, including coordinating making the respective policy of the EU at the national level.

44. In 2006, Estonia established also a so-called "Advisory Committee on Prevention of Money Laundering and Terrorist Financing" (hereinafter: Advisory Committee) in order to improve the awareness of the private sector on money laundering issues, to take part in the development of the system for the prevention of money laundering and also assisting in drafting of the legal instruments related to money laundering and terrorist financing. One of the major goals of the Advisory Committee is to involve the private sector in elaborating regulations which concern them and to exchange information and to express opinions to the Government Committee.

45. The evaluators were advised that the Estonian FIU liaises on supervision issues with the FSA through regular meetings. There is also an agreement of mutual co-operation for combating financial crime between the FSA, the Police Board, including the FIU and the Prosecutors Office which was signed on 20 January 2003 and provides ground for co-operation on supervisory and mutual training issues. However, the evaluators did not see an English version of this agreement and it is unclear to what extent it is dealing with AML/CFT issues (and not only with financial crimes in general). Leaving aside this uncertainty concerning formal procedures, it can be noted that there is apparently in practice good co-operation between the FIU, Customs, the Police Board, the FSA and the Prosecutors Office.

46. A shortcoming in Estonian national co-operation in AML/CFT issues is that there are now new supervisory authorities (Estonian Bar Association; Chamber of Notaries) and so far the co-operation and coordination between these and the pre-existing supervisory authorities does not yet seem to be formally structured.

47. Concerning international co-operation, Estonian authorities have the power and resources to respond to requests for legal assistance from abroad in a timely, constructive and effective manner. The Ministry of Justice is the central authority for co-operation on criminal matters; it has enough instruments and legal possibilities at its disposal to handle the incoming requests, to check them for compliance and to co-operate with the judicial authorities thus enabling Estonia to handle MLA requests in a timely manner. There is also a mechanism available for prioritizing and expediting assistance in urgent cases. When Estonia is submitting MLA requests to a foreign state and the case is urgent, the request may also be submitted through Interpol and communicated concurrently through the judicial authorities. However, international co-operation in the area of money laundering and terrorist financing could in some instances suffer from certain gaps in the national legislation, in particular in respect of the dual criminality requirement and the deficiencies

concerning the criminalisation of money laundering and terrorist financing. Furthermore, there are no arrangements for coordinating seizure and confiscation action with other countries.

48. According to information from the Estonian authorities, there is also a good level of international co-operation in AML/CFT issues between the FSA, FIU, the Police and respective foreign bodies. This can also be seen by the fact that the Estonian FSA carried out joint on-site inspections (covering inter alia AML/CFT preventive issues) of financial institutions with the financial supervisory authorities of Finland, Sweden, Latvia and Lithuania. The FIU has been a member of the Egmont Group since 2000 and it actively participates in its work; it uses the Egmont secure web site for information exchange and though the FIU can exchange information directly and spontaneously with other FIUs even without having a Memorandum of Understanding in place; it has signed a number of such Memoranda of Understanding.

7. Resources and Statistics

49. Though the resources of the FIU have been significantly strengthened since the 2nd evaluation, both the FSA and the FIU still appear to lack the manpower required to assure a proper level of on-site and off-site supervision in relation to the number of supervised entities. On one hand, the FIU has been granted a number of additional positions (though not all posts are filled). On the other hand, the FIU is now also required to supervise an increased number of entities. The FIU has taken an effective and pro-active approach through outreach programs. It also conducted a considerable number of on-site visits, though the majority of these visits had obviously awareness raising and training purposes and cannot be considered as on-site supervision as commonly understood.

50. The competent Estonian authorities keep comprehensive, informative, user-friendly and up-to-date statistics concerning AML issues (and as far as they occur, also on CFT issues): data concerning convictions, confiscation orders, persons involved and sentences imposed is maintained by the Ministry of Justice in the framework of general criminal statistics. This database allows the Ministry of Justice to produce statistics in case of need. In addition to the database of the Ministry of Justice, the FIU keeps (in order to analyze the effectiveness of the Estonian AML/CFT-system) detailed statistics in the form of an excel spreadsheet concerning investigations, the amount of property frozen, seized and confiscated, prosecutions, convictions, persons involved and sentences imposed in money laundering cases; for this purpose it uses the information from the database of the Ministry of Justice. This statistics of the FIU are updated on a quarterly basis. With regard to statistics only the following shortcomings could be observed:
    - Statistics in MLA-matters are not kept on the predicate offences.
    - The evaluation team was not provided with statistics showing the timeframe in which Estonia responded to extradition requests.
    - There was no statistical information available on the exchange of information of the FSA with foreign counterparts.

III. MUTUAL EVALUATION REPORT

1 GENERAL

1.1 General information on Estonia

51. The Republic of Estonia is a country in Northern Europe in the Baltic region. It is bordered to the north by Finland across the Gulf of Finland, to the west by Sweden, to the south by Latvia, and to the east by the Russian Federation. Estonia is a green land, forests cover 50.5% of the country (22 846 square km). Estonia became a European Union member state on 1 May 2004. Since 21 December 2007, Estonia is a part of the Schengen zone. The population is 1.361 million. The largest ethnic groups (2006) are Estonians (69%), Russians (26%), Ukrainians (2%), Belarusians (1%) and Finns (1%). The capital of Estonia is Tallinn (as of 1.01.2007, the population was 396.9 thousand or 29.6% of total population). Other large cities: Tartu (population 102.0 thousand); Narva (population 66.7 thousand); Kohtla-Järve (population 45.4 thousand) and Pärnu (population 44.1 thousand). The official language in Estonia is Estonian, which belongs to the Finno-Ugric language family and is closely related to Finnish. In addition, Finnish, English, Russian and German are also widely spoken and understood.

Economy

52. The Estonian kroon (hereinafter "EEK" according to ISO 4217) is pegged to the Euro at a rate of 1 EUR = 15.6466 EEK. The exchange rate is equivalent to the former exchange rate against the German mark (1 DEM = 8 EEK), introduced by the monetary reform of 1992. Both the Government and Bank of Estonia have stressed the need to join the Eurozone as soon as possible.

53. The Estonian economy is growing at a moderate speed. The economy will adjust primarily through declining domestic demand. Corrections are continuing in the property sector and there are signs of a slowdown in private consumption growth.

54. The key indicators of Estonia are as follows:

Key Indicators	1999	2000	2001	2002	2003	2004	2005	2006
Population as of 1 January (million)	1.38	1.37*	1.37*	1.36*	1.36*	1.35*	1.35*	1.36
GDP at current prices (billion EUR)	5.2	6.1	6.9	7.8	8.7	9.6	11.2	13.2
Real growth of GDP (%)	0.3	10.8	7.7	8.0	7.2	8.3	10.2	11.2
GDP per capita at current prices (EUR)	3 800	4 400	5100	5700	6400	7100	8300	9800
GDP at market prices, PPS per capita (EUR)	7400	85000	9100	10 200	11 300	12 300	14 100	16 100
Annual FDI (million EUR)	284.3	424.7	602.7	306.8	822.2	775.1	2 254.5	1 341.0
FDI stock, as of 31 December (million EUR)	2 454	2 843	3 573	4 035	5 553	7 378	9539	9616
FDI stock per capita, as of 31 December (EUR)	1 789	2 080	2 625	2 975	4 110	5 477	7066	7176
Consumer price index compared to previous year (%)	3.3	4.0	5.8	3.6	1.3	3.0	4.1	4.4

Key Indicators	1999	2000	2001	2002	2003	2004	2005	2006
Unemployment rate** (%)	12.2	13.6	12.6	10.3	10.0	9.7	7.9	5.9
Average monthly wage (EUR)	284	314	352	393	430	466	516	601
Current account balance (% of GDP)	-4.4	-5.4	-5.2	-10.6	-11.3	-12.3	-10.0	-15.5
Deficit (-)/Surplus of state budget (% of GDP)	-4.3	-0.2	-0.1	0.4	1.8	1.8	1.9	3.6
Exports (billion EUR)***	2.350	3.569	3.698	3.642	4.003	4.769	6.183	7.734
Imports (billion EUR)***	3.227	4.616	4.798	5.079	5.715	6.703	8.204	10.699
Trade balance (billion EUR)***	-0.877	-1.047	-1.100	-1.437	-1.712	-1.934	-2.021	-2.964
Total government expenditures (% of GDP)	38.5	36.5	35.1	35.6	34.6	34.1	33.4	33.0

** Based on the 2000 Population Census*
*** Unemployed/labour force according to ILO methodology;*
**** Trade figures shown in special trade system*

55. The GDP by main fields of economic activity (in % of total GDP) was as follows:

Field of Activity	1999	2000	2001	2002	2003	2004	2005	2006
Real estate, renting and business services	16.0	15.6	16.2	16.2	16.5	16.5	16.5	17.2
Manufacturing	13.6	15.9	16.5	16.1	16.2	15.3	15.1	14.5
Wholesale and retail trade	11.9	11.0	11.7	12.3	12.6	13.7	13.7	13.7
Transport, storage and communication	12.4	13.1	12.2	11.6	11.5	11.3	10.6	10.7
Construction	5.0	5.0	5.0	5.2	5.2	5.1	5.9	6.5
Public administration and defence; compulsory social security	5.8	5.5	5.2	5.1	5.1	5.0	4.7	4.4
Education	4.8	4.6	4.5	4.4	4.3	4.2	4.0	3.8
Financial intermediation	3.4	3.6	3.4	3.7	3.4	3.4	3.2	3.2
Agriculture and hunting	5.1	4.1	3.9	3.5	3.4	3.4	3.0	2.5

56. The main trade partners and main exports and imports in 2006, as a % of total trade, were as follows:

Country	Exports
Finland	18.2
Sweden	12.3
Latvia	8.7
Russia	7.9
USA	6.7
Germany	5.0
Lithuania	4.8
Gibraltar	4.6
China	2.8
Norway	2.7
Others	26.3

Country	Imports
Finland	18.2
Russia	13.1
Germany	12.4
Sweden	9.0
Lithuania	6.5
Latvia	5.7
Poland	3.8
Netherlands	3.5
Italy	2.6
Denmark	2.4
Others	22.8

57. The main commodity groups concerning exports and imports were:

Main Commodity Groups	Exports
Machinery and appliances	24.6
Mineral products	16.2
Wood and articles of wood	9.2
Base metals and articles of base metals	9.2
Furniture and other manufactured articles	7.3
Agricultural products and food preparations	7.0
Transport equipment	6.7
Textiles and textile articles	5.2
Chemical products	4.1
Articles of plastics and rubber	2.8
Paper and articles of paper	2.4
Others	5.3

Main Commodity Groups	Imports
Machinery and appliances	25.4
Mineral products	16.3
Transport equipment	12.1
Base metals and articles of base metals	9.5
Agricultural products and food preparations	7.3
Chemical products	6.5
Textile products	5.1
Articles of plastics and rubber	4.7
Wood and articles of wood	3.2
Furniture and other manufactured articles	2.3
Paper and articles of paper	1.9
Others	5.7

58. The investments in Estonia and from Estonia abroad were as follows:

Direct Investment Position in Estonia by countries as of 31 December 2006

Country	million EUR	% of total
1. Sweden	3 797.2	39.5
2. Finland	2 542.9	26.4
3. Great Britain	362.0	3.8
4. Netherlands	328.0	3.4
5. Norway	314.8	3.3
6. Russia	251.1	2.6
7. Latvia	228.4	2.4
8. USA	201.9	2.1
9. Germany	188.2	2.0
10. Denmark	180.4	1.9
Others	1 221.6	12.6
Total	9 616.5	100.0

Estonia's Direct Investment Position abroad by countries as of 31 December 2006

Country	million EUR	% of total
1. Latvia	940.8	34.3
2. Lithuania	885.8	32.3
3. Russia	243.2	8.9
4. Cyprus	232.7	8.5
5. Finland	130.8	4.8
6. Ukraine	65.3	2.4
7. Belarus	51.5	1.9
8. Spain	31.5	1.1
9. Italy	30.0	1.1
10. Bulgaria	23.1	0.8
Others	109.0	3.9
Total	2 743.7	100.0

59. The banking sector in Estonia has achieved a remarkable growth in the use of modern technology for conducting financial transactions. Payments in Estonia are mostly made through the banking channels or the use of credit or debit cards and cash is not very common for effecting payments. According to the statistics of the Bank of Estonia, the number of payments initiated in cash in credit institutions represents only 0,26% of all payments. The average amount of cash payments is 3 400 EEK (217.29 EUR) and of non-cash payments 22 900 EEK (1 463.57 EUR).

60. Estonia has made significant progress concerning the use of modern technologies:

- 65 per cent of population aged 6 to 74 are Internet users.
- 46 per cent of households have access to the Internet at home.
- All Estonian schools are connected to the Internet.
- There are over 700 Public Internet Access Points in Estonia, 51 per 100 000 people (which is one of the highest numbers in Europe).
- There are more than 1 000 free wireless Internet zones around the country.
- Incomes can be declared to the Tax and Customs Board via Internet. In 2007, the percentage of electronic tax declarations was over 80.
- Expenditures made in state budget can be followed on the Internet in real-time.
- The Government has changed Cabinet meetings to paperless sessions using a web-based document system.
- All of Estonia is covered with digital mobile phone networks.

61. The Estonian Government is supporting companies of the IT-sector which makes this sector one of the fastest growing in the country.

62. By February 2006, ID cards had been issued to 61% of the population (over 900 000 ID cards).

System of Government

63. Estonia is a parliamentary democracy. The Head of the State is the President. The Head of the Government is the Prime Minister. National legislature lies within the unicameral parliament (*Riigikogu*) of 101 members.

Legal system and hierarchy of normative acts

The Court system

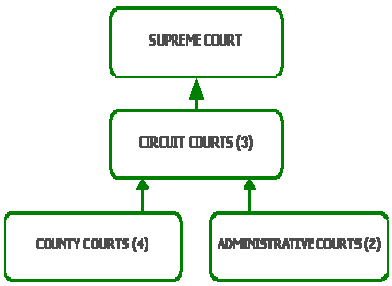
64. The Constitution does not provide for a definition of the judicial power. Nevertheless, it proceeds from the Constitution that the Estonian court system consists of county courts, administrative courts, circuit courts and the Supreme Court. Pursuant to the current Courts Act, there are 4 county courts, 2 administrative courts and 3 circuit courts. The Supreme Court, situated in Tartu, is the court of the highest instance.

65. The Constitution establishes that everyone is equal before the law and everyone has the right of recourse to the courts if his or her rights and freedoms are violated. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial court. The courts shall be independent in their activities and shall administer justice in accordance with the Constitution and the laws. Rules of court procedure are provided by different laws: Code of Civil Procedure, Code of Criminal Procedure, Code of Misdemeanour Procedure and Code of Administrative Court Procedure.

66. In principle, court sessions shall be public. A court may, in the cases provided by law, declare that a session or a part thereof be held in camera:
    a) to protect a state or business secret;
    b) to protect morals or the private and family life of a person;

c) or where the interests of a minor, a victim, or justice so require.

67. Judgments shall be pronounced publicly, except in cases where the interests of a minor, a spouse or a victim require otherwise. Everyone has the right of appeal to a higher court against the judgement in his or her case pursuant to procedure provided by law. See the diagram of the Estonian court system.



68. Courts of first instance and courts of appeal are administered in co-operation between the Council for Administration of Courts and the Ministry of Justice. The main function of the Department of Courts of the Ministry of Justice is (a) the management and supervision of the activities of county, city and administrative courts and courts of appeal and (b) the maintenance of court statistics. The Department of Courts also organises and supervises the activities of the Centre of Registers. This Department is further responsible *inter alia* for the professional activities of notaries and the Chamber of Notaries; management and supervision of the activities of bailiffs, trustees in bankruptcy and the Bar Association; managing and supervising the provision of legal services; managing the representation of the state in judicial proceedings and judicial cooperation in civil and criminal matters and proceeding international letters rogatory.

69. The Supreme Court is divided into three chambers: Administrative Law, Criminal or Civil Chamber. At least three judges shall participate in the hearing of matters in Chambers. The Supreme Court has an independent budget and the Court is independent in its activities.

70. The decisions of courts of first and second instances shall be made public in full in the database of court statistics and court decisions. The court rulings made before 1 January 2006 are available at the website http://kola.just.ee/ and the rulings after 1 January 2006 are available at http://www.kohus.ee/kohtulahendid/index.aspx. All reasoned judgements of the Supreme Court shall be published in the State Gazette. Supreme Court decisions are also electronically available on the homepage of the Supreme Court (www.nc.ee).

71. The Estonian Courts have adopted "Estonian judges` code of ethics". For disciplinary matters a Disciplinary Chamber has been formed in the Supreme Court: it comprises five judges of the Supreme Court, five appeal court judges and five judges of first instance.

Hierarchy of normative acts

72. In Estonia, the hierarchy of normative acts is as follows:
    a) Fundamental Constitutional Principles;
    b) EU Law;
    c) Constitution of Estonia; general principles of International law;
    d) International treaties;
    e) Laws which demand qualified majority vote for amendment (e.g. laws on elections and court procedure);

f) Unqualified laws (which do not demand qualified majority vote for amendment); Presidental Decrees (in extraordinary situations);
g) Regulations (by-laws) of the Government of the Republic;
h) Regulations of Ministers;
i) Regulations of Local Municipalities – with local applicability, equal with governmental and Ministerial Regulations;
j) Internal acts with general character (of state bodies/institutions/organisations; e.g statute, Verwaltungsvorschrift) – with internal applicability.

Guidebooks, directives, handbooks, etc. are not considered to be part of Estonian legal system as these acts do not have a binding character.

Legislation process

73. The steps in the process concerning legislation are in Estonia as follows:
    a) Initiating draft law:
    The rights to initiate a draft law are held by the members of Parliament, Parliamentary faction, Parliament committee and Government. The right to change the constitution is held by the President of the Republic.
    b) Deliberation of draft law in Parliament
    The management board of the Parliament designates among the committees the leading committee, which makes a proposal to the management board of the Parliament within three weeks to take the draft law into agenda or exclude it. If the draft law has not come through the Government, the leading committee sends it to the Government for an opinion. All members of Parliament can send the leading committee their opinions, proposals and positions on a draft law. The draft law is deliberated in the Parliament at least on two readings if the law does not require also a third reading.
    c) Adoption of a draft law by Parliament
    The adoption of a draft as legislation takes place by voting.
    d) Announcement of the legislation by the President of the Republic
    If the draft law has been adopted as legislation, the President of the Republic will make an announcement (not an approval).
    e) Publication in Government Gazette
    After the announcement of the President, the legislation has to be published in the Government Gazette within seven workdays after its announcement.
    f) Enforcement of the legislation
    The legislation becomes effect on the tenth day after the publication in Government Gazette if it is not stated otherwise in the legislation.

<u>Transparency, Good governance, ethics and measures against corruption</u>

74. In 2004, a so-called „Honest State strategy“ was implemented in Estonia. This strategy proposes a number of specific steps aimed at reducing the risk of corruption in Estonia. In June 2007 the Ministry of Justice made an official proposal to develop an Anti-corruption Strategy for the years 2008 to 2012, which is based on the results of the research the Ministry of Justice has carried out regarding corruption in Estonia. The Government endorsed the proposal on 23 August 2007 and the strategy was presented to the Government in January 2008. On 3 April 2008, the Government approved the new Anti-corruption Strategy for the years 2008-2012. The Criminal Law Convention on Corruption (CETS 173) was ratified on 17 October 2001.

1.2 General Situation of Money Laundering and Financing of Terrorism

75. The 5 most frequent criminal offences in Estonia are theft, operating a motor vehicle in a state of intoxication, physical abuse, fraudulent conduct, and aggravated breach of the public order. These five criminal offences account for 73% of all registered criminal offences. Estonian authorities provided the following statistics concerning the crimes which are considered to be the major sources of illegal proceeds in Estonia:

	2004	2005	2006	2007
Crimes of 1st degree[5]	3371	2982	2688	2656
Drug-related crimes (§§183-190 PC)	1044	1190	981	1441
Crimes, which may be related to trafficking in persons (§§ 133, 134, 136, 138-140, 143, 172, 173, 176-178, 259,268, 268[1] PC)	297	161	136	135
Crimes related to bribery and gratuities (§§ 293-298 PC)	98	122	120	110
Tax crimes (§§ 386-393 PC)	207	156	253	267
incl. illicit traffic (§ 391 PC)	108	47	83	81
Fraudulent conduct (§§ 209-213 PC)	2128	2192	2057	2624
Computer crimes (§§ 206-208 PC)	2	9	8	14
All criminal offences (total)	57168	55586	51834	49724

76. The Estonian authorities advised that it is difficult because of the small number of money laundering cases to conclude or anticipate anything about typical predicate offences. In the cases which have been proceeded, violation of the procedure for handling alcohol and/or tobacco products, larceny of forest, computer-related fraud, theft, accepting gratuities and accepting bribe have been predicate offences. However, current investigations indicate that fraud (especially internet fraud), tax crime and drug offences are also predicate offences in a number of money laundering cases. In many ongoing cases the predicate offences are committed abroad or the victims are abroad (especially concerning Internet fraud cases).

77. An analysis of the suspicious transactions reports indicate that the main risk factors are currently the transfer of proceeds of Internet crimes to Estonia or via the Estonian financial system, the sale of accounts, using figureheads, using unconventional payment services and cash flow related to non-residents. In 2007, the Financial Intelligence Unit and the Financial Supervision Authority (FSA) compiled a risk analysis of electronic payments, incl. services of alternative means of payment. The results of this analysis show that a high level of information technology and extensive use of information technology tools poses additional money laundering and terrorist financing risks in practice in Estonia.

78. Concerning terrorist financing, Estonian authorities advised that so far no cases of terrorist financing or any other offences connected with terrorism are known to have been committed on the territory of Estonia or via Estonia. According to Europol's "Terrorist Activity in the European Union: Situation and Trends Report (2006)"[6], Estonia, Finland, Hungary, Latvia, Lithuania, Slovenia and Slovakia are the least threatened EU countries by terrorism and activities supporting terrorism. Representatives of the Securities Police Board stated that there were no active terrorist groups in Estonia at the end of 2006 or supporters or financiers of international terrorist organisations. Estonian authorities do not have any information and there are no indications which would refer to the fact that funds are collected for or forwarded to terrorists or movements

[5] According to § 4 PC, "*a criminal offence in the first degree is an offence the maximum punishment prescribed for which in this Code is imprisonment for a term of more than five years, life imprisonment or compulsory dissolution.*" In contrast, "*a criminal offence in the second degree is an offence the punishment prescribed for which in this Code is imprisonment for a term of up to five years or a pecuniary punishment.*"

[6] http://www.statewatch.org/news/2006/may/europol-terr-rep-2004-2005.pdf.

associated with terrorists through Non-profit associations (NPAs) in Estonia. There is also no information about Estonian NPAs providing any logistic support to terrorists or recruiting persons for terrorist purposes. Although such activities cannot be excluded for the future, Estonian authorities consider it very unlikely. The Security Police Board uses international cooperation to prevent terrorist financing and pursues national cooperation primarily with the Financial Intelligence Unit on the bases provided in the Security Authorities Act and the MLTFPA.

1.3 Overview of the Financial Sector and Designated Non-Financial Businesses and Professions (DNFBP)

1.3.1 Financial Sector

Credit Institutions

79. As of 31 December 2007, there were seven locally licensed credit institutions and eight branches of foreign credit institutions operating in Estonia. At the end of 2007, the share of Estonia's two largest banks totalled ca. 80% of the entire banking sector. This figure has not changed compared to the previous years. The market is characterised by high concentration. The largest market participants are subsidiaries of Scandinavian banks. Market shares by ownership residency:
    - Sweden 87%
    - Denmark 9%
    - Latvia, Russia, Italy, Estonia each ca. 1%

80. Branches of European Union (EU) financial institutions operating in Estonia can offer any of the financial services that they have licenses for in their home country. At the time of the on-site visit, the number of affiliated branches of foreign credit institutions was 10. The supervisory institution in the country of origin is responsible for supervising such branches, and the norms and limitations in local legislation with regard to capital are not applied.

81. Licensed financial institutions from other European Union member states need not apply to the Financial Supervision Authority for a license to provide financial services in Estonia. The provision of cross-border services may commence after the supervision authority in the foreign country has informed the Financial Supervision Authority that the financial institution wishes to provide its services in Estonia and has communicated the information required under the law. As of 31 December 2007, 173 credit institutions from other European Union countries were registered to provide cross border services in Estonia.

82. Estonian authorities provided the following data concerning non-resident accounts in Estonia as of 31 December 2007:

resident/non-resident deposits as of 31.12.2007						
	Residents plus non-residents (in millions)			Non-residents only (in millions)		Percentage of non-residents' deposits*
	A	B	C	D	E	
	in EEK (equivalent in EUR)	in foreign currency (equivalent in EUR)	total (A + B)	in EEK (equivalent in EUR)	in foreign currency (equivalent in EUR)	
Current accounts	3388,23	1937,23	5325,46	107,07	908,92	19,08%
Saving Deposits	83,33	25,00	108,33	1,76	1,69	3,18%
Other	1911,83	1766,25	3678,08	21,22	548,21	15,48%
Total	5383,39	3728,48	9111,87	130,05	1458,82	17,44%

*** in relation to all (resident plus non-resident) accounts: ratio assets; accumulated: both domestic and foreign currency**

Securities market participants

83. § 7 Securities Market Act lists the "professional securities market participants":
    a) investment firms;
    b) credit institutions;
    c) operators of the regulated market;
    d) operators of a securities settlement system;
    e) other persons prescribed by law.

84. To operate as a professional securities market participant, a person must hold a respective activity license. A professional securities market participant can provide only those services for which he has the respective activity license. An activity license is issued for an unspecified term, it is non-transferable and the acquisition and use thereof by other persons is prohibited.

Investment Firms

85. An investment firm is a joint-stock company the permanent activity of which is the provision of investment services for third parties either separately or together with non-core services. A person must hold a respective activity license in order to operate as an investment firm.

Operator of Regulated Market

86. A regulated market is a system of organisational, legal and technical solutions which is directly or indirectly available to the public, which has been created for the purpose of enabling regular dealings in securities, and which enables different persons to make each other proposals, either simultaneously or non-simultaneously, for carrying out transactions with securities, as well as the conclusion of transactions with securities.

Operator of Securities Settlement System

87. A securities settlement system is an aggregate of organisational, technical and legal solutions, set up for the performance of obligations deriving from securities transactions on the basis of a contract concluded among three or more members of the system, and the operator of the system and for securing the performance of obligations deriving from participation in the system. An operator of the system is a person who, pursuant to the rules of the system and the contracts concluded by him or her on the basis of such rules, organises the execution of transmission orders, and depending on the operation of the system, also the set-off of claims among the members of the system.

88. All these entities mentioned above in para 83 are covered by the MLFTPA.

Investment firms

89. According to § 40 of the Securities Market Act, an investment firm is a public limited company, the permanent activity of which is to provide investment services to third parties whether separately from or together with non-core services. An investment firm is deemed to be a financial institution within the meaning of § 5 of the Credit Institutions Act. As of 31 December 2007, there were seven registered investment firms.

Fund Management Companies

90. According to the Investment Funds Act, public limited companies may operate as fund management companies, provided that they hold a relevant activity license. Activity licenses are issued and revoked by the Financial Supervision Authority. In addition to the management of a fund, a management company may provide only the following services:
    a) management of a securities portfolio;
    b) provision of advice upon investment in securities;
    c) safekeeping of units of shares of a fund for a client;

d) fund management services specified in § 10 (1) of the Investment Funds Act to funds or assets which are not managed by the management company.

91. As of 31 December 2007, there were eleven fund management companies and nine cross-border fund management companies in Estonia.

Insurance

92. Companies which want to provide insurance services need a licence by the Financial Supervision Authority (§ 16 Insurance Activities Act). The registered office of an insurance undertaking which has obtained an activity licence from the Financial Supervision Authority must be in Estonia.

93. At the end of 2007, the Estonian insurance industry included eight non-life insurance companies, five life insurance companies and the Estonian Traffic Insurance Fund providing cross-border insurance and reinsurance. In addition, six foreign insurers providing non-life insurance already operate or are in the process of opening a branch in Estonia. At the time of the on-site-visit, a total of 336 providers of life (64) and non-life (272) insurance services have been entered in the register of providers of cross-border services in Estonia. Insurance companies are covered via § 3 (1) in conjunction with § 6 (2) 5 by the MLFTPA.

Savings and loan associations

94. At the time of the on-site visit, there were 14 savings and loan associations (SLA) operating in Estonia. These activities are regulated by the Savings and Loan Associations Act. SLAs are obliged to send monthly a balance sheet to the Bank of Estonia. The market share of SLAs is relatively small. The scope of activities is limited to deposit taking from its own members and subordination of government loans and foreign aid funds to their members, who are mainly natural persons of the county of registration. The total balance of all SLAs is approx. 143 mil EEK (ca 9,1 mil EUR), i.e. 0,05% of the total assets of credit institutions.

1.3.2 Designated Non-Financial Businesses and Professions (DNFBP)

Casinos

95. Games of chance may not be organised outside of designated gaming sites (casinos). For operating games of luck it is obligatory to obtain two different licences, namely an operating license and a gaming license. To be eligible for the license the applicant has to meet specific requirements prescribed in the Gambling Act. The licensee has to pay a state fee before a license can be issued. The licenser for the operating license is the Governmental Commission for the Licenses of Organising the Games of Chance. The gaming license has to be obtained from the Estonian Tax and Customs Board in order to operate a casino at a specific place. The Tax and Customs Board is also the supervisory authority for the requirements of the Gambling Act. There is no legislation explicitly prohibiting internet casinos, but Estonian authorities consider that this could be contradictory to the Gambling Act which stipulates that no licenses can be given to operate a casino without a specified address (though it has to be noted that the law does not require that the operator should be established or registered in Estonia). However, in the absence of practical cases, it is difficult to establish whether these provisions could serve as safeguards against internet casinos.

96. The license is issued for 10 years, separately for each type of gambling. To organise games of luck, the company's share capital has to be at least 2 million EEK (127 800 EUR). The company's only field of activity has to be the organising of gambling activities and the share capital of the company has to be divided into registered shares. Before issuing a license, the Commission must obtain information about the operator, including the data proving the fulfilment of the

abovementioned requirements and the proof of absence of tax arrears as well as copies of the statutes of the company and the audited accounts of the three preceding accounting years. A list of the owners should be provided, together with, copies of the income-tax returns of the last three years if a person's (legal entity's) ownership exceeds 5% of the company, or, (if the owner is a legal entity) the audited accounts of the three preceding accounting years, and the decisions of the appointments of the board members and executives.

97. The licenser (Governmental Commission for the Licenses of Organising the Games of Luck) is situated and served by the Ministry of Finance[7].

98. The gambling license has to be obtained from the Estonian Tax and Customs Board in order to operate games of chance in a specified place. The gambling licence can only be issued to an operator who already has an operating license. § 18 of the Gambling Act lists the documents which have to be presented to the Tax and Customs Board in order to get a licence. The license is issued for 5 years, separately for every casino. The certificate of consent of the rural municipality or city government has to be obtained from the respective municipal authority before applying for the gambling licence. Before the Estonian Tax and Customs Board can issue the licence, a state fee of 50 000 EEK (3 195 EUR) has to be paid.

99. Currently there are 18 operators of games of chance, who organise gambling in 188 gambling sites (casinos) in Estonia (including the gambling sites on ferries). According to § 3 (1) 3) and § 10 MLTFPA, casinos are "obligated persons" under the MLTFPA and the FIU is responsible for its supervision concerning casinos.

Dealers in precious metals

100. For dealers in precious metals the Precious Metal Articles Act applies. There are 701 registered traders of precious metal (including watch traders) in Estonia. The Technical Inspectorate shall exercise supervision of dealers in precious metals concerning their compliance with the requirements established by Precious Metal Articles Act. Dealers in precious metals are subject to the requirements of the MLTFPA if a cash payment in a lump sum or in several related payments is made of no less than 200 000 EEK (i.e. 12 782.32 EUR).

Lawyers

101. Lawyers (advocates) in Estonia are competent to *inter alia* represent and defend clients in court and in pre-trial proceedings; collect evidence; provide legal services; act as an arbitrator or conciliator; act as a trustee in bankruptcy proceedings. In the provision of legal services, an advocate is independent and acts pursuant to law, the legal acts and resolutions adopted by the bodies of the Bar Association and the requirements for the professional ethics of advocates, good morals and conscience. Information disclosed to an advocate is confidential. An advocate or employee of the Bar Association or a law office who is being heard as a witness may not be interrogated or asked to provide explanations on matters that he or she became aware of in the course of the provision of legal services.

102. An advocate is required to maintain the confidentiality of information which has become known to him or her in the provision of legal services, the confidentiality of persons who request the advocate to provide legal services and of the amount of remuneration paid for legal services unless otherwise provided by law. Such obligation has an unspecified term and it applies after the termination of the activities of the advocate. A client or his or her legal successor may, by his or her written consent, exempt an advocate from the obligation to maintain a professional secret. The obligation to maintain confidentiality shall not extend to the collection of costs for legal services

[7] According to the new Gambling Act which will enter into force on 1 January 2009, the gaming license will have to be obtained from the Estonian Tax and Customs Board.

provided by an advocate who participated in a matter. Disclosure of information to the Board in the exercise of supervision over the activities of an advocate or to the court of honour in the hearing of a matter concerning a disciplinary offence is not be deemed to be a violation of professional secrecy. In order to prevent a criminal offence in the first degree[8], an advocate has the right to submit a reasoned written application for exemption from the obligation to maintain a professional secret to the Chairman of an administrative court or an administrative judge of the same court appointed by the Chairman. The legal professional privilege does not extend to cases where an advocate acts as a representative of the client in financial or real estate transactions. The MLTFPA provides exemptions from professional privilege with regard to notification obligations arising from the MLTFPA (for details see below para 732).

103. § 47(3) MLTFPA specifies that the Estonian Bar Association is responsible for the supervision of members of the Bar Association with regard to the provisions of the MLTFPA. At the time of the on-site visit, 646 lawyers were members of the Bar Association. However, it is not compulsory for a practising lawyer (independent legal professionals) to become a member of the Bar Association and 116 lawyers have chosen to remain outside the membership of the professional association which means that they do not fall under the supervision of the Bar Association; for these lawyers, the FIU would be responsible for supervision but so far the FIU did not yet supervise any of them and it was also acknowledged that the number of lawyers acting outside may be higher than 116.

Notaries

104. A notary is a holder of office in public law who is empowered by the state to attest, at the request of persons, facts and events which have legal meaning and perform other notarial acts in order to ensure legal certainty. Notaries perform, inter alia, the following notarial acts: attest transactions and declarations of intention, authenticity of signatures and copies, correctness of translations of documents and authenticity of signatures of translators; attest other facts and events which have a legal meaning, including voting or ballot results, results of the drawing of lots, and sea protests; receive deposits of and transfer money, securities and valuables; issue certificates concerning data entered in registries and printouts from registries; prepare lists of assets; forward petitions and notices; organise and attest auctions; issue certificates concerning the preparation of notarial documents which are subject to completion in the Republic of Estonia which correspond to the standard forms established in Annex VI to the Council Regulation no. 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Notaries settle succession matters in cases pursuant to the procedure provided for in the Law of Succession Act. Notaries are obliged to provide legal assistance to the parties to notarial acts and to prepare corresponding draft documents. Notaries may deposit money, securities, valuables and documents if the depositing is connected with transactions certified by the notaries, and the persons applying for the deposit have a legitimate interest arising from the transactions to ensure the performance of the transactions by deposit. Notaries shall not deposit other things or cash.

105. A notary is required to maintain the confidentiality of information which he or she receives through professional activities. The duty of a notary to maintain confidentiality remains after he or she resigns from office, and extends to the employees of a notary's office, translators and interpreters and other persons who have access to such information. A notary shall disclose information concerning notarial acts performed by the notary only to persons at whose request or concerning whom the notarial acts are performed, or to the representatives of such persons. At the request of a court, a notary shall disclose information to the court concerning notarial acts performed in criminal, civil or administrative matters pending before the court. On the basis of a court order, a notary shall disclose information to investigative bodies concerning notarial acts. The legal professional privilege does not extend to cases where a notary public acts as a

[8] see FN 5.

representative of the client in financial or real estate transactions. The MLTFPA provides exemptions from professional privilege with regard to notification obligations arising from the MLTFPA (for details see below para 732).

106. A notary shall not hold other paid offices besides the office of notary or perform any other paid work except teaching or research, or legal counselling in matters of civil law not related to notarial attestation. Also, a notary shall not engage in enterprise, or participate in a company or be a member of the management or supervisory board or a liquidator or procurator of a company; be the director of a branch of a foreign company; be a trustee in bankruptcy, member of a bankruptcy committee or compulsory administrator. A notary and the employees of his or her office are prohibited from acting as intermediaries between parties entering into transactions unless otherwise provided by law.

107. There are 100 notaries public in Estonia, who act alone or together in offices. The number of notaries has more than doubled since 1993. Estonian authorities advised that services described in the Notaries Act may only be provided by notaries; for notaries the membership to the Chamber of Notaries is mandatory.

Real Estate Agents and Trust and Company Service Providers

108. Estonian authorities advised that according to the data of the Union of Estonian Real Estate Agents (http://www.ekfl.ee/), the number of their members is 46; and according to the data of the Association of Estonian Facilities Administrators and Maintenance Professionals (http://www.ekhhl.ee/) the number of their members is 100.

109. In the Estonian commercial registry 26 Trust and Company Service Providers are registered.

110. Both Real Estate Agents and Trust and Company Service Providers operate on common grounds without any specific regulations.

Bailiffs

111. The status of bailiffs and their duties concerning independence and secrecy are comparable to that of notaries. A bailiff shall not hold other paid offices besides the office of bailiff or perform any other paid work except: teaching or research in educational or research institutions; legal counselling, outside execution proceedings, in the area of civil enforcement or insolvency proceedings if the bailiff conforms to the requirements set in Courts Act; acting as a trustee in bankruptcy or as the liquidator of legal persons if the bailiff has passed the examination for trustees in bankruptcy. Also, a bailiff shall not engage in enterprise, or: be a founder of a company, a member of the supervisory or management board of a company, a procurator or a liquidator of a company, unless she or he has been appointed as liquidator by a court; be the director of a branch of a foreign company; a member of a bankruptcy committee or a compulsory administrator of an immovable. If circumstances exist which cast suspicion upon the impartiality of a bailiff, the bailiff shall not conduct enforcement proceedings and shall remove him or herself from office.

Accountants and auditors

112. The Authorised Public Accountants Act is the legal bases for the professional activities of auditors but does not apply for accountant. In December 2007, there were 365 external auditors registered in Estonia. According to § 3 (1) 7) and § 10 MLTFPA, auditors and providers of accounting services are “obligated persons” under the MLTFPA.

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

113. In Estonia a legal person is either a legal person in private law or a legal person in public law.

114. In accordance with § 25 General Part of the Civil Code Act (GPCCA), a *legal person in private law* means a legal person founded in private interests and pursuant to an act concerning the corresponding type of legal persons. General partnerships, limited partnerships, private limited companies, public limited companies, commercial associations, foundations and non-profit associations are legal persons in private law. Non-profit associations are trade unions, political parties, church congregations, apartment associations etc.

115. The state, local governments and other legal persons founded in the public interest and pursuant to an act concerning such legal person are *legal persons in public law*.

116. 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 registration procedure of private legal persons is provided in the Commercial Code, in the Non-Profit Associations Act and in the Foundations Act.

117. In accordance with § 26 GPCCA, a legal person has passive legal capacity (i.e. the capacity to have civil rights and perform civil obligations). A company may be founded by one or several persons. A founder and shareholder of the company may be a natural person or a legal person. In accordance with § 31 of the GPCCA, the bodies of a legal person in private law are the general meeting and the management board unless otherwise provided by law. The management board is the directing body of a legal person in private law. If the law provides for the existence of a supervisory board, the supervisory board is also a directing body. The competence of a body of a legal person in private law shall be prescribed by law, the articles of association or the partnership agreement. The competence of a body of a legal person shall not be transferred to any other body or person. The activities of a body of a legal person are deemed to be the activities of the legal person. *Only natural persons with active legal capacity may be members of the management board.* The management board is a directing body of the company which represents and directs the company. The management board may have one member (director) or several members. At least one half of the members of the management board shall have their residence in Estonia, in another Member State of the European Economic Area or in Switzerland. A member of a body of a legal person shall not transfer his or her rights as a member of the body arising from law unless otherwise provided by law.

Register

118. According to the Commercial Code (CC), an unattested copy of the approved annual report together with the profit distribution proposal signed by the management board (only in the case of a company) and the auditor's report (if auditing is compulsory) shall be submitted by the accounting entity (all legal persons in private or public law registered in Estonia, sole proprietors, and branches of foreign companies registered in Estonia) to the registrar within six months after the end of the financial year. The list of shareholders shall be annexed to the report (as at the approving of the balance sheet). The annual report with its annexes is public information available on the website of the Commercial Register. A private limited company and public limited company must submit annual reports to the Register even if the company has no economic activities.

119. According to the CC, the management board of a private limited company shall keep a list of shareholders which shall set out the names, addresses, personal identification codes or registry codes. The shareholders, members of the management board and supervisory board, competent state agencies and other persons with a legitimate interest have the right to examine the list of

shareholders. If so decided by the shareholders, shares may be entered in the Estonian Central Register of Securities. In such case, the list of shareholders shall be maintained by the registrar of the Estonian Central Register of Securities. The management board of a private limited company shall ensure the timely submission of correct information provided by law to the person maintaining the list of the shareholders. Upon entry of shares in the Estonian Central Register of Securities, the management board of the private limited company shall promptly submit a notice from the registrar of the Estonian Central Register of Securities concerning the registration of the shares to the registrar of the commercial register.

120. The share register of a public limited company shall be maintained by the registrar of the Estonian Central Register of Securities. The management board of the public limited company shall ensure the timely submission of correct information provided by law to the person maintaining the share register.

121. The Registration Departments of County Courts maintain the following registers: the commercial register since 1995 and the non-profit associations and foundations register since 1998 and some other registers. All companies, non-profit associations and foundations that did not comply with the requirements were subject to compulsory liquidation.

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

122. In the recent past, the Government of Estonia set its crime prevention priorities as follows: fight against organised crime, particularly drug trafficking and human trafficking, more effective discovery and confiscation of criminal proceeds, including proceeds of corruption and discovery of money laundering crimes. According to an agreement of 22 August 2005 between the Minister of Justice and the Minister of Interior, a priority of the authorities is the fight against organised crime, incl. combating proceeds of crime, i.e. income derived from corrupt practices and criminal offences relating to money laundering. To achieve these goals, Estonia made amendments to substantive and procedural laws and assigned more human resources to the respective bodies.

123. The Ministry of the Interior has devised a Strategy for Combating Terrorism, which covers *inter alia* the following topics: improvement of international and national cooperation; prevention of radical terrorism and recruitment for terrorism; prevention of terrorist financing and related money laundering; prevention of illicit trafficking of strategic goods.

124. In spring 2006, a Government committee for the coordination of issues concerning the prevention of money laundering and terrorist financing was established (Order No. 285 of the Government of the Republic of 11 May 2006). All the agencies engaged in the prevention of money laundering are represented in this Committee. For further details see below para 145.

125. The new Money Laundering and Terrorist Financing Prevention Act (MLTFPA) was adopted by the *Riigikogu* on 19 December 2007 and it entered into force on 28 January 2008 (i.e. the tenth day after its publication in the State Gazette). Estonian authorities intended to implement with the new MLTFPA the 3rd EU AML Directive and to remedy shortcomings identified in MONEYVAL's second round evaluation report. One of the most important goals was to strengthen the preventative AML/CFT system of Estonia.

126. Estonia adopted also a so-called "Development Plan of Governmental Authorities 2008-2011" which declares prevention of money laundering and tracing criminal proceeds as one of its

priorities. The Minister of the Interior validated the Development Plan of its area of government and consulted on this with the Prime Minister and other ministers[9].

127. Estonian authorities explained that supervision over the activities of providers of services of alternative means of payment is a priority in supervision. Another priority with the entry into force of the new MLTFPA is the training of obliged persons. Estonia also wants to enhance domestic cooperation between the police, investigative bodies, competent state authorities and obliged persons as well as international cooperation.

128. Estonian authorities are aware of the fact that over 90% of the Estonian financial sector consists of subsidiaries or branches of financial institutions from the European Union, and there is an increasing trend (primarily in the insurance sector) of establishing European trading companies. Therefore, one of the objectives of the activities of the FSA is to cooperate with the supervisory authorities of other countries and to work out an efficient supervision framework for analysing the risks in other countries. The objective is to integrate the FSA into the risk appraisal process of financial groups in these countries.

129. The FSA considers it as one of its priorities to work out a system to detect training needs and carry out training in order to implement risk-based supervision. Continuous changes in supervision regulations and paradigms means increasing requirements for professional and vocational skills. The FSA is replacing step-by-step the norm-based supervision model with a principle risk-based supervision model. The latter means a more individual subject-based approach in which assessments and requirements are designed separately for every financial institution according to its risk profile, activities, etc.

130. To measure the effectiveness of its AML/CFT policies and programmes, the Estonian authorities compared the dynamics of available criminal statistics; however, it was acknowledged that this method is not very effective considering the small number of particular offences proceeded.

b. The institutional framework for combating money laundering and terrorist financing

131. The following are the main bodies and authorities involved in combating money laundering or financing of terrorism:

The Financial Intelligence Unit

132. The Estonian Financial Intelligence Unit (FIU) is a police-type FIU and was established as a separate division under the Criminal Investigation Department of the Police Board on 1 July 1999. On 1 January 2004 a new version of the AML Act came into force, and the FIU was made an independent structural unit of the Central Criminal Police. The core function of the Unit is the collection, registering, processing, analysing and dissemination of information received from reporting parties concerning possible money laundering and terrorist financing. § 37 of the MLTFPA describes the numerous competences of the FIU (see para 312). An important element of its competencies is the supervision of the activities of obligated persons in complying with the MLTFPA, unless otherwise provided by law. At the time of the on-site visit, the FIU was staffed with 18 persons. The FIU is currently structured as follows: Head of the FIU, one assistant, one data processing specialist plus 3 units: Analysis Unit, Asset Recovery Unit, Supervision Unit.

[9] The Development Plan is available in English at the website: http://www.siseministeerium.ee/36496.

The Financial Supervision Authority (FSA)

133. The Estonian FSA exercises the supervision of credit institutions (including foreign banks' branches) investment firms, fund management companies, life and non-life insurance companies, insurance brokers (but not insurance agents), the Traffic Insurance Fund and the Tallin Stock Exchange concerning their fulfilment of the requirements arising from the MLTFPA. The FSA became operational on 1 January 2002 pursuant to the FSA Act which came into force on 9 May 2001. The FSA brought under its umbrella the Banking Supervision Department of the Bank of Estonia, the Securities Inspectorate and the Insurance Supervisory Agency. The latter two supervisory authorities used to be under the Ministry of Finance. According to the FSA Act, the FSA is an independent institution affiliated to the Bank of Estonia with a six-member Supervisory Council comprised of the Minister of Finance, the Governor of the Bank of Estonia, two members appointed by the Government and two members appointed by the Supervisory Board of the Bank of Estonia. The Supervisory Council decides on the strategy and budget of the FSA and appoints the four members of the Executive Management Board which take all management and supervisory decisions.

134. The FSA is fully funded by supervised entities through a scheme of supervisory charges calculated on the basis of capital and volume of business. At the time of the on-site visit, the FSA was staffed with 60 persons.

The National Bank of Estonia

135. The main objective of the National Bank of Estonia (NBE) is to ensure price stability. Leaving aside the tasks of the FSA (which is an independent institution affiliated to the Bank of Estonia), it has to be noted that the competencies of the NBE itself in the AML/CFT area are quite limited as no specific tasks have been assigned to it.

Ministry of Finance

136. The Ministry of Finance has to deal with the coordination and implementation of the planning of the financial and resource management policies of the Government and the budgetary policies of the state, the planning and implementation of taxation and customs policies, economic analyses and forecasts. It is also competent for licencing organisers of the games of Chance (Governmental Commission for the Licenses of Organising the Games of Chance) and for supervision over the activities of the Board of Auditors. The Ministry of Finance is responsible for the preparation of legislation concerning the financial markets, financial supervision, games of chance and AML/CFT legislation. The Ministry of Finance co-ordinates the AML/CFT measures in Estonia. The Government decided on 14 July 2005 that the national AML/CFT policy will be within the competence of the Ministry of Finance (before it was the Ministry of Interior).

Ministry of Interior

137. The Ministry of the Interior is responsible for guaranteeing the internal security of the state and the protection of public order. The following executive agencies and inspectorates are under the umbrella of the Ministry of Interior: the Police Board, the Security Police Board, the Citizenship and Migration Board, the Border Guard Administration. Until summer 2005, the Ministry of Interior was responsible for the national AML/CFT policy (then the Ministry of Finance became responsible for it).

Ministry of Justice

138. The Ministry of Justice is responsible for the coordination of legislative drafting, management of the professional activities of the courts of first and second instance, including Registration Departments of County Courts which maintain the commercial register and the non-profit

associations and foundations register; the Prosecutor's Office; prisons; legal assistance; extradition; legislation concerning the provisions of the Penal Code, the Code of Criminal Procedure, the General Part of the Civil Code Act, the Commercial Code, the Non-profit Associations Act, the Foundations Act etc.

The Public Prosecution Service

139. According to the Prosecutor's Office Act, the Prosecutor's Office has inter alia the following competences/responsibilities: it leads pre-trial criminal proceedings ensuring its lawfulness and effectiveness; it represents public prosecution in court and fulfils other duties imposed on the Prosecutor's Office by law. Being the leader (*dominus litis*) of criminal proceedings, the prosecutor guides the preliminary investigator in collecting evidence and decides whether to bring charges against a person on the basis of the facts established. The Prosecutor's Office consists of two levels: the Public Prosecutor's Office as the superior prosecutor's office and four Circuit Prosecutor's Offices. The work area of the Public Prosecutor's Office covers the whole of Estonia and the work areas of Circuit Prosecutor's Offices coincide with the work areas of police prefectures.

140. In the recent past, Estonia undertook a penal reform which led to substantial amendments to the Prosecutor's Office Act. The institution of assistant prosecutor has been created. Assistant prosecutors are vested with the same powers as prosecutors, except for the right to participate in adversarial procedures. Also the position of special prosecutors has been introduced who deal in a project-based manner with priority crimes such as corruption, drug-related crimes and environmental crimes.

Ministry of Foreign Affairs

141. The Ministry of Foreign Affairs is *inter alia* responsible for planning the foreign policy of the state, international agreements and foreign trade, management of the relations of the Republic of Estonia with foreign states and international organisations. It participates in international cooperation against terrorism and terrorist financing within the framework of the European Union, the United Nations and other international organisations. It is also responsible for the implementation of sanctions imposed by the United Nations Security Council and the EU and for reporting to the UNSC. The drafting of the International Sanctions Act and The Strategic Goods Act was coordinated by the Ministry of Foreign Affaires.

Central Criminal Police

142. The Central Criminal Police coordinates criminal police surveillance activities and the fight against money-laundering in the whole country and is the central institution in Estonia for international criminal information exchange. The main investigative directions of the Central Criminal Police are organised crime, corruption and serious economic, money-laundering, narcotics and information technology crimes. The Central Criminal Police coordinates cooperation with other national and international law-enforcement agencies and international organisations, carries out witness protection and performs surveillance activities in the whole country to prevent financing of terrorism and money-laundering. It has to be noted that the FIU is a part of the Central Criminal Police.

Security Police Board

143. The investigation of terrorist related cases falls into the competence of the Security Police Board (SPB). With the Security Authorities Act, which came into force on 1 March 2001, the status of the SPB was converted from a police authority to a security authority. The investigative competence of the SPB covers offences against the Republic of Estonia or international security; terrorism; offences against humanity and peace; war crimes; the illegal handling of explosive

material and explosive devices prohibited for civilian purposes and the organisation of explosions with these; some office crimes committed by higher state officials; illicit traffic, if the object of the crime was a radioactive substance, explosive material, strategic goods, firearm or ammunition or if the crime was committed by an official using his/her office; offences related to the disclosure of state secrets; incitement to social hatred. The SPB has an important role in counter-terrorism activities and its activities include *inter alia* the following:

- the collection of information, in order to detect possible interest and activities of terrorist organisations, targeted against the Republic of Estonia;
- the suppression of financing of terrorism;
- the suppression of the distribution of weapons of mass destruction;
- international cooperation.

Tax and Customs Board

144. The Estonian Tax and Customs Board deals *inter alia* with ensuring the receipt of state budget revenue from state taxes and customs duties, implementation of the tax and customs arrangements based on the national tax and customs policy, ensuring compliance with tax legislation, customs regulations and other legal acts, the issue of operating permits for gambling and for organisers of lotteries, the supervision of the legality of gambling operations and of the activities of organisers of lotteries as a gambling supervisory inspectorate on the basis of and pursuant to the extent prescribed by law, and providing services to persons by the fulfilment of their tax liabilities and at performing customs formalities including cross-border transportation of currency.

The Government Committee for Coordination of Issues Concerning Prevention of Money Laundering and Terrorist Financing

145. According to Order No. 285 of the Government of the Republic of Estonia of 11 May 2006, the Government Committee for Coordination of Issues Concerning Prevention of Money Laundering and Terrorist Financing was established. It was intended that all the agencies engaged in the prevention of money laundering and terrorist financing are represented in this Committee. It consists of the:

a) Ministry of Finance
b) Ministry of Interior
c) Ministry of Foreign Affaires
d) Ministry of Justice
e) FIU
f) Adv. Committee of stakeholders
g) Bank of Estonia
h) FSA
i) Police Board
j) Security Police Board
k) Prosecutors' Office
l) Tax and Customs Board (TCB)

146. It is intended that a representative of the Ministry of Economic Affairs and Communications will be added to the composition of the Committee. 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 in force and coordinating drafting new legislation;
- making proposals to the Government of the Republic for the improvement of the measures of the prevention of money laundering and terrorist financing and for the amendment of the respective legislation;

- coordinating international cooperation on prevention of money laundering and terrorist financing, including coordinating making the respective policy of the EU at the national level.

147. The meetings of the Government Committee take place no less than once per two months. The Government Committee for Coordination of Issues Concerning Prevention of Money Laundering and Terrorist Financing works in close cooperation with the private sector. Also the "Advisory Committee on Prevention of Money Laundering and Terrorist Financing" comprising of representatives of financial institutions and other relevant institutions governed by the Money Laundering and Terrorist Financing Prevention Act has been established whose functions include the submission of opinions and proposals in AML/CFT matters to the Government Committee.

c. The approach concerning risk

148. A country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is low or little risk of money laundering or terrorist financing. In Estonia, there was no such decisions not to apply certain measures recommended in the FATF 40+9 Recommendations just because of low or little risk of money laundering or terrorist financing.

d. Progress since the last mutual evaluation

149. The progress Estonia made since the last mutual evaluation is impressive. It adopted a new law to combat money laundering and the financing of terrorism (the Money Laundering and Terrorist Financing Prevention Act – MLTFPA), which introduced a significant number of new and useful tools. This law provides - with only a small number of minor shortcomings – a sound legal framework for the governmental authorities to combat money laundering and the financing of terrorism.

150. The staffing of the Financial Intelligence Unit has been significantly improved: the total number of staff in November 2002 was 7, of which 6 posts were filled; the total number of staff at the time of the on-site visit (February 2008) was 24 of which 18 posts were filled (though it has to be noted that the evaluation team nonetheless has some concerns with regard to the staffing in relation to the large number of entities which fall under the supervision of the FIU).

151. The statistics show an increasing trend concerning STRs received by the FIU and cases forwarded to investigative bodies and for prosecution.

152. While at the second round evaluation of Estonia no money laundering convictions could be noted, Estonia achieved 8 convictions for money laundering between 2005 and February 2008. 12 natural persons and 1 legal person were convicted.

153. A number of shortcomings of the money laundering offence identified during the second round evaluation of Estonia have been removed: It is positive that the law clearly criminalises money laundering if predicate criminal activity has taken place abroad. The evaluators also welcome the removal of the reference to laundered proceeds as property acquired as a direct result of an act punishable pursuant to criminal procedure. Thus, Estonia may prosecute now for money laundering if the property in stake is acquired directly or indirectly by crime.

154. Significant progress can be noted also concerning the criminalisation of terrorist financing: there is now a clear provision dealing with the financing of terrorist acts and the financing of terrorist organisations is also present in Estonian legislation. The financing of individual terrorists is missing but also acknowledged by the authorities who have already prepared a draft law to remedy this shortcoming.

155. The evaluation team also noted progress in the confiscation regime. A number of shortcomings identified during previous evaluation rounds were removed:

- Estonia has introduced a system with generally greater mandatory confiscatory elements in it as far as *proceeds* are concerned;
- the restrictive approach identified in the past, which was limited only to the direct object of the crime was changed and now both direct and indirect proceeds are confiscatable;
- a value based confiscation system is in place concerning proceeds of crime;
- there are possibilities for reversing the burden of proof in certain cases.

156. The third round evaluation team was also satisfied that the new provisions on seizure and confiscation are assessed very positively by practitioners (investigators and prosecutors) and are being widely used by them. This applies also for international cooperation – there are good examples of provisional measures, confiscation and sharing assets with foreign countries in recent Estonian practice.

157. Exchange offices, money remitters and real estate businesses as well as other DNFBP have been brought under the supervision of the FIU. In 2007, the FIU made more than 200 on-site visits. As a result of this supervision activity, the number of STRs from these sectors increased significantly.

158. The last report was concerned with the nominee accounts for professional participants in the securities market. According to § 15 (3) MLFTPA, nominee accounts are now prohibited.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of money laundering (R.1 and 2)

2.1.1 Description and analysis

Recommendation 1

159. For the first time money laundering was criminalised in Estonia with an amendment to the old Penal Code (in force between 1992 and 2002) as from 1 July 1999. The Penal Code provided for the punishment of the offence, while the crime itself was defined in the Money Laundering Prevention Act (in force between 1999 and 28 January 2008). This kind of legislative technique of cross-referencing is common practice in Estonia and seems to cause no interpretation or application problems to the practitioners. The reason behind it is that there should not be double definitions in the legislative acts, and the definition should be provided in the act having a more substantial character for the issue in stake. The same approach has also been applied in the new normative package regulating the current money laundering offence: the Penal Code criminalises the money laundering offence in §394 by reference to the definition in § 4 MLTFPA. In general terms the structure of the criminal offence has remained the same in the different versions of the Penal Code. The current money laundering offence reads as follows:

> *„§ 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 § 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 § 83[2] of this Code."*

160. In 2000, Estonia signed and ratified the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention); the 2000 UN Convention against Transnational Organised Crime (the Palermo Convention) was ratified and entered into force in Estonia on 29 September 2003. Nevertheless the evaluation teams of the first and second evaluation round found that some of the substantial physical and material elements of Art. 6 of the Palermo Convention and Art. 3 of the Vienna Convention were not covered and therefore recommended that an amendment which clearly encompasses in its formulation all the language of the aforementioned international conventions on the physical aspects of the offence would be highly beneficial. Estonian authorities took these recommendations into account for making legal

amendments and the definition under § 4 MLTFPA seems now to be to a very high extent covering the material and physical elements of the offence as required by the conventions.

161. §4 (1) MLTFPA defines money laundering as follows:

> *1) concealment or maintenance of the confidentiality of the true nature, origin, location, manner of disposal, relocation or right of ownership or other rights of property acquired as a result of a criminal activity or property acquired 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 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.*

162. Art. 6 (1)(a) (i) of the Palermo Convention seems to be fully covered ("*the conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action*") by § 4 (1) 2) MLTFPA. Art. 6(1)(a)(ii) ("*the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime*") is covered by § 4 (1) 1) MLTFPA. The previous wording of the definition left doubts as to whether the criterion under Art. 6 (1)(b) would be covered by Estonian legislation, i.e. whether simple acquisition or possession of laundered property would be covered. These doubts were removed through the clear text of §*4 (1) 2)*. This can be illustrated by the table below:

MLTFPA 2008	Palermo Convention 2000	Vienna Convention 1988
Money laundering means: ***§ 4** (1) 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 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.*	Criminal offences, when committed intentionally: **Art. 6 (1)(a) (i)** The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;	Criminal offences under domestic law, when committed intentionally: ***Article 3*** b) i) The conversion or transfer of property, knowing that such property is derived from *any* offence or offences established in accordance with subparagraph *a)* of this paragraph, or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;
***§ 4** (1) 1) concealment or maintenance of the confidentiality of the true nature, origin, location, manner of disposal, relocation or right of ownership or other rights of property acquired as a result of a criminal*	**Art. 6 (1) (a)(ii)** The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;	Art 3. ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with

activity or property acquired instead of such property;		subparagraph *a)* of this paragraph or from an act of participation in such an offence or offences;
(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.		
*Section 4 (1) 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 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.*	**Art. 6 (1) (b)** Subject to the basic concepts of its legal system: **(i)** The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;	**Art 3. c)** Subject to its constitutional principles and the basic concepts of its legal system: i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from an offence or offences established in accordance with subparagraph a) of this paragraph or from an act of participation in such offence or offences;
	Art. 6 (1) (b) (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.	**Art 3 iv)** Participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

163. According to the Estonian authorities the concept of money laundering as determined in the MLTFPA covers all types of property. It seems indeed that any type of property derived from criminal activity is covered by § 9 which reads as follows: „*For the purposes of this Act, property is any object as well as the right of ownership of such object or documents certifying the rights related to the object, including electronic documents and the benefit received from the object."* This is also explained in more detail in the explanatory memorandum to the MLTFPA which explains that the law drafters followed the requirements of Article 3 (3) of the 3rd EU AML Directive. With regard to the definition as provided for by the 3rd EU AML Directive[10] and the results of the interviews when on-site (checking whether all various forms of property are covered and whether this is also understood by the different authorities) it can be concluded that this definition matches the definitions of "property" laid down in Art. 1 lit. b of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (the "Strasbourg Convention"), Art. 1 lit. q) of the Vienna Convention and Art. 2 lit. d) of the Palermo Convention:

[10] Article 3 (3) of the 3rd EU AML Directive reads as follows: "*'property' means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets*".

MLTFPA (Estonia) 2008	Strasbourg Convention 1990	Vienna Convention 1998	Palermo Convention 2000
§ 9 Property is any object as well as the right of ownership of such object or documents certifying the rights related to the object, including electronic documents and the benefit received from the object."	**Art. 1 lit. b):** "property" includes property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title to, or interest in such property;	**Art. 1 lit. q)** "Property" means 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;	**Article 2 lit. d)**: Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets).

164. One of the major drawbacks in the definition of the money laundering offence which was identified during the first and second round was the clear reference to laundered proceeds as property acquired as a *direct* result of an act punishable pursuant to criminal procedure. The evaluation team considers this shortcoming rectified: in the current definition of the crime the term "*direct result*" is no longer present. According to Estonian authorities the expression "*property acquired as a result of a criminal activity or property acquired instead of such property*" in § 4 MLTFPA brought clarity for the prosecutorial and judicial authorities enabling them to consider as proceeds of crime also property which was acquired indirectly. This conclusion is also supported by the language of the Explanatory Memorandum to the MLTFPA which states with regard to § 4 that the form of property may be replaced with another or any subsequent form, which takes contamination over (the so-called surrogate or substitute).Thus, it could be concluded that the definition also covers the second degree of proceeds.

165. The money laundering offence as criminalised in § 394 PC in connection with § 4 MLTFPA is not linked to any particular predicate offence. The Estonian authorities stated in their replies to the Questionnaire that a conviction for the predicate offence is not required before initiating money laundering prosecutions. It was explained that the only requirement is that the property has been acquired though a crime. During the on-site visit it could not be established which level of proof is required that proceeds are acquired through a crime. The new definition of the money laundering offence replaced the term "*crime*" with the expression "*criminal activity*". The intention of the law drafters (Ministry of Justice) was to relieve the practitioners from the burden of a prior or simultaneous conviction for the predicate offence as required by the previous MLTFPA (which is also mirrored by the fact that all money laundering convictions so far were prosecuted together with the relevant predicate offences or after a conviction for the respective predicate offence). According to the Estonian authorities the concept of "*criminal activity*", even if not defined in Estonian legal acts, has been used in the acts in context of police activities and statistics. This should enable that whenever a quantity of money may be connected to a criminal activity, money laundering investigations could be commenced and as a result, concrete predicate offences may be discovered as an outcome of the process. Thus, it was explained that not only a conviction for the predicate offence is not a prerequisite, but also no obligation lies on the investigators to prove a predicate offence before the investigation of the offence of money laundering may be commenced.

166. The evaluators were not provided with the necessary level of empirical facts that would substantiate these statements. There are no examples where a person was convicted for money laundering where the predicate offence had not been established with a conviction. In addition, both judges and prosecutors expressed their opinion that they would have preferred different language clearly stating that a conviction for the predicate offence is not a prerequisite for the money laundering offence. The evaluation team shares the doubts expressed by practitioners, as there is not very much difference between the expressions "*criminal offence*" (sometimes translated simply as "*crime*") and "*criminal activity*". Also the explanatory report to the MLTFPA

does not make any reference to this problem. As there is not yet practice (indictments, convictions) on this, the evaluation team sees some uncertainties whether it will now be possible to convict somebody for money laundering without a prior or simultaneous conviction for the predicate offence.

167. Estonia applies an all crimes approach and all the designated offences under the FATF Recommendations can be predicate offences for money laundering, including insider trading and market manipulation as well as offences provided for in Article 2 and 3 of the Strasbourg Convention on the protection of environment. A list of designated offences and the respective provisions in the Estonian Penal Code which cover the designated offences is provided in Annex II. As noted beneath 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.

168. Although according to Estonian authorities the practice based on the old MLTFPA has not made any difference as to the location where the predicate offence has been committed, the evaluation team welcomes the positive development of embodying this possibility expressly in the new MLTFPA. According to § 4 (2) MLTFPA, *"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"*.

169. § 7 of the Penal Code envisages that "*the penal law of Estonia applies to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and is punishable at the place of commission of the act, or if no penal power is applicable at the place of commission of the act and if:1) the act is committed against a citizen of Estonia or a legal person registered in Estonia;3) the offender is a citizen of Estonia at the time of commission of the act or becomes a citizen of Estonia after the commission of the act, or if the offender is an alien who has been detained in Estonia and is not extradited.*" § 8 of the Penal Code further provides for the applicability of the Estonian penal law for crimes committed abroad: "*regardless of the law of the place of commission of an act, the penal law of Estonia shall apply to an act committed outside the territory of Estonia if the punishability of the act arises from an international agreement binding on Estonia*".

170. According to § 7 (1) Penal Code, Estonia requires dual criminality in order to prosecute under Estonian law against natural persons, i.e. the particular conduct must be a crime in the place where it occurred. This corresponds to the requirements of criterion 1.5. § 4 (2) MLTFPA states that it is enough for prosecuting for money laundering if the predicate offence has occurred outside Estonia (extra-territorial predicate offence). Estonian authorities advised the team that they could prosecute for money laundering even if the foreign predicate offence was not capable of being prosecuted in Estonia, though this has yet not been tested in practice.

171. Another issue in this context could be the level of proof of the extra-territorial predicate offence which is required in order to prosecute the money laundering offence in Estonia (which is also an aspect of criterion 1.2.1). From the seven convictions for money laundering none has been based on a predicate offence which took place abroad. Therefore it is up to the court practice to confirm the understanding of the authorities with which the evaluation team met that a conviction for an extra-territorial predicate offence is not a necessary element in a prosecution for money laundering.

172. During the first evaluation round, Estonian law did not allow for the prosecution of money laundering in cases where the person committed the predicate offence ("self-laundering"). Due to the different opinions expressed by Estonian authorities, the second round evaluators strongly advised that the issue of "own proceeds" is put beyond doubt in legislation. While there is no explicit legal provision for self-laundering, during the third round evaluation there was unanimity amongst prosecutors and judges that self-laundering is prosecutable in Estonia. Examples of the

court practice were brought to the attention of evaluators which convincingly showed that there is no obstacle to prosecute persons who committed the predicate offence themselves. Persons charged with a predicate offence were charged also with a money laundering offence when they have committed both the offences.

173. Concerning ancillary offences, Estonian law covers attempt, aiding and abetting, facilitating, and counselling the commission of money laundering. A punishment shall be imposed on an accomplice (i.e. abettor or aider) pursuant to the general part of the Penal Code (§§ 22, 25):

> *§ 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 § 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.*
>
> *§ 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."*

174. *Conspiracy* as such is not provided for in the Estonian criminal system. However, there is no fundamental principle that conspiracy (i.e., an agreement between two or more natural persons to pursue a course of conduct which would involve the laundering of criminal proceeds - whether or not laundering was actually committed) could not be introduced into Estonian legislation. The only provision covering some but not the essential elements of conspiracy can be found in § 255 of the Penal Code "Criminal organisation", which reads as follows:

> *(1) Membership in a permanent 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 in the second degree for which the maximum term of imprisonment of at least three years is prescribed, or criminal offences in the first degree[11], is punishable by 3 up to 12 years' imprisonment.*

175. Though § 255 could be, in principle, applied to the money laundering offence (the requirements of § 255 match with the conditions of the money laundering offence), it has to be concluded that it insufficiently addresses the concept of conspiracy (as described in the previous

[11] see FN 5.

paragraph) as § 255 requires amongst other things the involvement of at least 3 persons and a permanent organisation.

Additional elements

176. Concerning an activity generating proceeds which is not an offence in the foreign country, but where the proceeds were laundered in Estonia, the Estonian authorities considered that they could prosecute for money laundering on the basis that the activity committed abroad would constitute a "*criminal activity*" under § 4(1) MLTFPA. For further details and the requirement of dual criminality for certain occasions, see above para 168 ff.

Recommendation 2

177. Money laundering is punishable both with regard to natural and legal persons if committed intentionally. The mental element is knowledge as required by international conventions. The Penal Code provides in § 15 that only intentional acts shall be punishable as criminal offences, unless a punishment for a negligent act is provided by the Code. Since neither the Penal Code, nor the MLTFPA penalises negligent money laundering, this offence cannot be prosecuted on a negligence basis. According to § 16 PC, intent can be deliberate, direct and indirect. The Estonian authorities declared during the on-site visit that plans for introducing negligent money laundering were at a very early stage of inter-ministerial discussion[12].

178. The Estonian criminal legislation contains no explicit provision whether the intentional element of a criminal offence, including money laundering, may be inferred from objective factual circumstances. However, during the meetings with prosecutors, judges and representatives from the Ministry of Justice, it was confirmed that it is possible to infer the commission of the underlying offence from objective factual circumstances, because the general rules of proving intent are applicable for the offence of money laundering. §§ 60 ff CPC provide for the principle of free assessment of evidence. According to this principle, the judge is not bound by strict rules in assessing and evaluating the evidence gathered but may decide according to his own conviction. This principle of free evaluation of evidence provides the legal basis for inferring the intentional element of the money laundering-offence from objective factual circumstances. Though this system formally fulfils the requirements of criterion 2.2, a more explicit provision in the law would be preferable.

179. Estonia introduced criminal liability of legal persons in 2002. § 14 of the Penal Code (which is in the general part of the Penal Code) clarifies that the criminal liability of legal persons is only possible in cases where this is specifically provided for by law:

> *(1) In the cases provided by law, a legal person shall be held responsible for an act which is committed by a body or senior official thereof in the interest of the legal person.*
> *(2) Prosecution of a legal person does not preclude prosecution of the natural person who committed the offence.*
> *(3) The provisions of this Act do not apply to the state, local governments or to legal persons in public law.*

180. Criminal liability for legal persons for money laundering is provided for in § 394(3) and (4) PC:

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

[12] The draft of the Amendment Act to the Penal Code regarding criminalisation of negligent money laundering has passed inter-ministerial discussions.

(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.

181. Though these provisions formally fulfil the requirements of criterion 2.3, some deficiencies of implementation need to be noted: § 14 PC requires as a prerequisite "*an act which is committed by a body or senior official thereof in the interest of the legal person*". It was understood that "*body*" refers to the general meeting, the management or supervisory board of a company. It becomes clear from the term "*senior official*" (Estonian authorities advised that the term *senior official* refers to members of management of all levels, who have the ability to direct the acts of the legal person) that this does not cover employees at a lower level, e.g. clerks[13]. Furthermore § 14 PC requires that one can link the criminal act with a particular person (arg. ex "*committed by a body or senior official thereof*"). This could cause difficulties in complex money laundering cases where it might be difficult to connect criminal behaviour with individual person(s) in involved enterprises; this may be particularly a problem with large enterprises which have complex structures. However, it seems that in practice there was already some success with these new provisions: out of 7 achieved convictions 1 was for a legal person.

182. Prosecution of a legal person does not preclude prosecution of the natural person who committed the offence. This is explicitly provided for in § 14 (2) Penal Code. Neither does it preclude any other sanctions from being imposed where provided by law.

183. The criminal sanctions for natural persons may be pecuniary punishment or imprisonment (minimum 30 days and maximum 5 years) for the basic form of the offence (§ 394 (1) PC); in aggravating circumstances the only sanction is imprisonment which reaches from 2 to 10 years. The minimum term of imprisonment has been reduced in 2002 from 3 to 2 years, which was considered as not very appropriate by the second round evaluators. In order not to belittle the aggravated form of money laundering, the current evaluation team would like to again invite the Estonian authorities to analyse whether the sanctioning of an aggravated money laundering offence is appropriate in relation to the domestic circumstances.

184. In the case of a legal person, the court may impose a pecuniary punishment of 50 000 (approx. 3 200 EUR) to 250 Mio EEK (approx. 16 million EUR) on the legal person. A pecuniary punishment may be imposed on a legal person also as a supplementary punishment together with compulsory dissolution (§ 44 PC). Overall it can be concluded that the sanctions applicable for natural and legal persons are effective, proportionate and dissuasive in relation to the Estonian system (compared with the sanctions for similar offences and taking into account the economic situation); the same can be said in comparison with the sanctions provided for in other MONEYVAL or FATF countries.

185. The penalties actually imposed by the courts for money laundering offences show that the judicial authorities in Estonia follow a direction which is around the middle terms of the penalties envisaged in the Penal Code. The penalties imposed in the 8 convictions were between 2,6 to 5 years of imprisonment (on probation or partially on probation) and one compulsory dissolution of a legal person. Estonian authorities advised that in some cases persons convicted were already detained for more than 1 year during the investigative procedures; this time of detention was then taken into account for the final sanction imposed.

Statistics

186. Data concerning convictions, confiscation orders, persons involved, sentences imposed in money laundering cases is maintained by the Ministry of Justice in the framework of general

[13] This shortcoming has in the meanwhile been remedied as § 14(1) PC has been amended during 2008 (entered into force on 28 July). According to the new wording, *an act which is committed by a body, a member of a body, senior official, or a competent representative of a legal person in the interest thereof* may be imputed for the legal person.

criminal statistics. This database allows the Ministry of Justice to produce statistics in case of need. In addition to the database of the Ministry of Justice, the FIU keeps (in order to analyze the effectiveness of the Estonian AML/CFT-system) detailed statistics 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; for this purpose it uses the information from the database of the Ministry of Justice. This statistics of the FIU are updated on a quarterly basis.

187. Between 2005 and February 2008, 8 convictions for money laundering were achieved in Estonia. 12 natural persons and 1 legal person were convicted. The predicate offences covered various types of crimes (violation of procedure for handling alcohol and/or tobacco products, larceny of forest, computer-related fraud, theft of property, accepting gratuities and accepting bribes). The penalties imposed were between 2,6 to 5 years of imprisonment (all on probation or partially on probation) and the compulsory dissolution of a legal person. Considering the size of the country, the number of inhabitants and the money laundering threats it is exposed to, the number of convictions can be described as satisfactory though more would be preferable.

2.1.2 Recommendations and comments

188. Estonia has improved its legal framework for the criminalisation of money laundering since the last evaluation. The examiners welcome the rewording of the definition of the money laundering offence adapting it very closely to the language of the international conventions on the physical aspects of the offence. It is positive that the law clearly criminalises money laundering if predicate criminal activity has taken place abroad. The evaluators also welcome the removal of the reference to laundered proceeds as property acquired as a direct result of an act punishable pursuant to criminal procedure. Thus, Estonia may prosecute now for money laundering if the property in stake is acquired directly or indirectly by crime.

189. The evaluation team was satisfied by the unanimity amongst prosecutors and judges and the court practice that self-laundering is prosecutable in Estonia. However, no such unanimity could be established on the term "*criminal activity*" which replaced the term "*crime*" as underlying criminality for money laundering. It is too early to see how practice will interpret this and which level of proof for the underlying predicate crime will be required for a money laundering conviction, i.e. whether a conviction or at least indictment for the predicate offence is a prerequisite for a money laundering conviction. Thus, the evaluation team sees some uncertainties whether the changes in legislation will now allow the conviction of somebody for money laundering without a prior or simultaneous conviction for the predicate offence. Clarification in law, guidance and/or training of judicial bodies may help to solve this shortcoming.

190. Estonia should introduce the full concept of conspiracy for the money laundering offence.

191. The sanctions available in the legislation and imposed so far seem effective, proportionate and dissuasive.

2.1.3 Compliance with Recommendation 1 and 2

	Rating	Summary of factors underlying rating
R.1	**LC**	• Unclear if money laundering may be convicted without a prior or simultaneous conviction for the predicate offence. • Conspiracy to commit money laundering is insufficiently covered in legislation.
R.2	**C**	

2.2 Criminalisation of terrorist financing (SR.II)

2.2.1 Description and analysis

192. Special Recommendation II requires the criminalising of the financing of terrorism, terrorist acts, and terrorist organisations and ensuring that such offences are money laundering predicate offences. The Methodology specifies that financing of terrorism should extend to any person who wilfully provides or collects funds by any means, directly or indirectly with the unlawful intention that they should be used in or in the knowledge that they are to be used, in full or in part:
1. to carry out a terrorist act(s);
2. by a terrorist organisation; or
3. by an individual terrorist.

193. The United Nations International Convention for the Suppression of the Financing of Terrorism from 1999 (Terrorist Financing Convention) was ratified and entered into force for Estonia on 21 June 2002.

194. In 2007, the Penal Code was amended introducing financing of terrorism as a separate criminal offence in § 237^3. This provision criminalises financing of terrorist activity as defined by § 237, §237^1 (Terrorist organisation) and § 237^2 (Preparation of and incitement to acts of terrorism) and reads as follows:

> *(1) Financing or supporting a criminal offence provided in §§ 237, 237^1, 237^2 of this Code in another manner 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.*

195. The terrorism offence, which provides one of the basic elements of the financing of terrorism offence (§ 237^3 PC) is regulated in § 237 PC as follows:

> *(1) Commission of a criminal offence against international security, against the person or against the environment, 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, interference with electronic data or obstruction of the functioning of computer system[14] 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 five to twenty years' imprisonment, or life imprisonment.*
> *(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.*

196. Although the legislative approach used in this section is quite different from the usual listing of crimes constituting specific acts of terrorism, § 237 in conjunction with other provisions of the PC (§§ 110, 111, 112, 135, 246, 248 etc) seems wide enough to cover the majority of the various situations and acts referred to in Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions. However, though the law drafters intended to comprehensively cover all these conducts with § 237^3 PC, a certain deficiency occurs as § 237 PC (the terrorism offence) does not cover all the acts as referred to in Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions; e.g. the provisions related to the

[14] The dotted underlined part was introduced with an amendment after the on-site visit (entry into force on 24 March 2008).

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 are contained in §§ 246 ff of the Penal Code (under the chapter: "Offences Against Foreign States or International Organisations"). This chapter is not mentioned by § 237 PC and thus it has to be concluded that these provisions are not covered by the terrorist financing provision. Also some conducts as described by the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970, are not covered.

197. § 237^3 also refers to §§ 237^1 and 237^2 PC which read as follows:

> *§ 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 § 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.*
>
> *§ 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 § 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."*

198. There is no definition of "funds" for the purpose of terrorist financing in Estonian legislation. Universally recognized principles and norms of international law are considered an integrated part of the Estonian legal system. If a law conflicts with a ratified international treaty, the treaty prevails. Nevertheless it is not clear whether definitions in international conventions are directly applicable in Estonia. Estonian authorities referred to the definition of funds provided in the Terrorist Financing Convention as directly applicable but no legal provision or ruling of the Supreme Court was cited to substantiate this understanding.

199. The Terrorist Financing 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, traveller cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit*". The definition of "*property*" as provided for by § 9 of the MLTFPA reads as follows: "*for the purposes of this Act, property is any object as well as the right of ownership of such object or documents certifying the rights related to the object, including electronic documents and the benefit received from the object*." Though it is not so detailed it seems to correspond with the definition of "funds" as given by the Terrorist Financing Convention (for further reasons see also above para 163).

200. According to Estonian authorities, the term "*supporting [...] in another manner*" in § 237^3 may be understood to include the provision of all kinds of support. The judges interpreted the term "*support*" as broad enough and covering every possible contribution to terrorists: financing and any other kind of support. The interviewees with which the evaluation team met were of the opinion that the structure of the provision covers all conducts as required by the international standards and matches with the requirement "*provision and collection of funds by any means, directly or indirectly, to be used in full or in part*". However, the evaluation team is less convinced of this interpretation and sees difficulties that such a wide interpretation of the term "*support*" could cover all the elements as required by criterion II.1; this is particularly the case concerning the requirement "*collection of funds*". In the absence of court practice in the application of this

provision, abstract examples discussed during the on-site visit showed as well that the legislation does not fully correspond with the requirements of Art. 2 of the Terrorist Financing Convention. It would be quite far fetched to read in the notion of "*supporting*" the collection of funds with the unlawful intention that they should be used in full or in part by terrorists. Thus the evaluation team considers Criterion II.1 a) not fully covered. In the evaluators' view, § 237[3] is not very articulate and therefore it is difficult to say to what extent such elements as the a) *collection of funds by any means*, b) *directly or indirectly,* c) *unlawful intention that they should be used in or in the knowledge that they are to be used*, d) *in full or in part* are included in Estonian legislation.

201. According to the Estonian authorities the absence in the legislative act of an explicit reference to direct or indirect support suggests that both forms are in principle covered. Similarly, there is no reference to the legitimate or illegitimate origin of the funds. The Estonian authorities are of the opinion that the Penal Code is clear enough that "*supporting terrorist activities*" is a criminal act and therefore there is no difference whether the support is through legitimate or illegitimate funds. There is no stipulation or reference in the law stating that it is not necessary that the funds were actually used to carry out terrorist acts or be linked to a specific terrorist act. Yet, the Terrorist Financing Convention is more detailed in this respect and in the absence of any court decisions, it is difficult to conclude whether, if the case would occur, the law enforcement and judicial authorities would be aware and would apply the Convention standards as described. In the evaluators' view it would be beneficial if the definition of the financing terrorism offence could be widened in respect of more adequate correspondence to the language of the Terrorist Financing Convention. This would prevent problems in practice.

202. Bearing in mind the deficiencies pointed out in the definition of the term financing of terrorism against the requirements of SR II, it can be summarised that in Estonian law financing of acts of terrorism, financing of a terrorist organisation and financing of preparation of and incitement to acts of terrorism are criminalised.

203. Financing a single terrorist is not criminalised as required by Criterion II.1(a)(iii). At the time of the on-site visit, the Ministry of Justice had elaborated a Draft Amendment to the Penal Code which provides for such criminalisation. It was expected that this amending Law will be adopted by Parliament in October 2008 and the law be promulgated and enter into force before 1 December 2008[15].

204. The Methodology requires that it should also be an offence to attempt to commit the offence of terrorist financing. The common ancillary offences in Estonia are also applicable in terrorist financing context. Reference is made to the general part of the Penal Code, in particular § 25 "Attempt" on the basis of which attempted terrorism financing is punished. § 22 "Accomplice" also provides for the offence of participation (criteria II.1.d and e with reference to Article 2(5) of the Terrorist Financing Convention).

205. The Estonian money laundering offence follows an all crimes-approach, i.e. all crimes may be predicate offences for money laundering, and thus also terrorist financing as far it is criminalised can be a predicate offence for money laundering.

206. According to § 8 Penal Code regardless of the law of the place of commission of an act, the penal law of Estonia shall apply to an act committed outside the territory of Estonia if the punishability of the act arises from an international agreement binding on Estonia. Estonian authorities stated, that though there is no practice available, the terrorist offence (§ 237 PC) could be considered as par excellence offence subjected to the universal jurisdiction (§ 8 PC) where

[15] The draft of the Amendment Act to the Penal Code concerning criminalisation of financing of individual terrorists has been sent to Parliament on 13 October 2008.

neither the location of the offence nor the law in force in that location impede the jurisdiction of Estonian Penal Code.

207. Estonian criminal legislation contains no explicit provision as to whether the intentional element of a criminal offence, including financing of terrorism, may be inferred from objective factual circumstances. However, as described above, the principle of the free evaluation of evidence permits the intentional element of the terrorist financing offence to be inferred from objective factual circumstances (for details see above para 178).

208. All the terrorist (financing) offences are punishable by a pecuniary punishment or a compulsory dissolution if committed by a legal person (§§ 237(2), 237^{1}(2), 237^{2} (2)). According to the General Part of Estonian Penal Code (§ 14 (2) prosecution of a legal person does not preclude the prosecution of the natural person who committed the offence. Neither does it preclude any other sanctions from being imposed where provided by law.

209. The terrorism financing offence provides as sanction for natural persons only imprisonment ranging from 2 to 10 years; if committed by a legal person the sanctions are pecuniary punishment or compulsory dissolution. These penalties, possibly combined with any of the applicable administrative penalties, appear to be effective, proportionate and dissuasive. However, since there have been no financing of terrorism cases, it is not possible to evaluate its application in practice.

Statistics

210. The existing legislative framework has not been tested before courts (no criminal proceedings, indictments or convictions for terrorist financing have been completed so far). As a result, there is no case-law or practice on the exact scope of the current provisions. The Estonian authorities stated that statistics would be maintained if there were any cases. One investigation was initiated but it was terminated early due to the absence of the elements of the offence.

2.2.2 Recommendations and comments

211. The sustainable commitment of Estonia to improve the legal framework for the criminalisation of terrorism financing is commendable. At present, there is a clear provision dealing with the financing of terrorist acts. The financing of terrorist organisations is also present in Estonian legislation. However, the financing of individual terrorists is missing but also acknowledged by the authorities who have already prepared a draft law to remedy this shortcoming. Furthermore, some conducts as referred to in Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions are not covered.

212. As far as the financing of terrorism is criminalised, it is also a predicate offence for money laundering.

213. The sanctions envisaged for terrorist financing offence seem to be effective, proportionate and dissuasive however they have never been applied.

214. However, there are some elements of the international requirements which are not covered explicitly enough. The examiners consider that a more detailed provision on financing of terrorism would be preferable to cover explicitly the various elements of the international requirements in a consistent way and with a sufficient degree of legal certainty; e.g. the Penal Code does not cover "collecting of funds" and "whether the funds were actually used to carry out or attempt a terrorist act" neither does it define "legitimate or illegitimate source". It is recommended to amend the legal text criminalising terrorist acts and the provision criminalising terrorist financing in a way that they would be broad and detailed enough to cover, besides the financing of terrorist organisations,

also all terrorist acts as required by the UN Conventions and the financing of individual terrorists. These provisions should also:

- clearly cover the various elements required by SR.II, in particular the collection of funds by any means, directly or indirectly, and their use in full or in part for terrorist financing purposes;
- clarify that it is not necessary that funds were actually used to carry out terrorist acts or be linked to a specific terrorist act.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**PC**	• Financing of an individual terrorist is not criminalised. • The terrorist financing offence does not cover "collecting of funds". • Current law does not specifically criminalise the 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 are not covered.

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

2.3.1 Description and analysis

215. Estonian Penal Code provides for a general regime of confiscation (§§ 83, 83[1],83[2], 84, 85) and there are special provisions in the money laundering part (§§ 394 (5) (6) PC). The general regime applies to most of the designated predicate offences including the financing of terrorism offence, as far as it is criminalised (for the deficiencies in the coverage of terrorist financing see above Section 2.2). Annex II lists the predicate offences how they are covered in Estonian legislation and whether the provisions of the general confiscation regime are applicable.

216. As already stated in the Second Round Evaluation Report, laundered property, where money laundering is the only offence being proceeded with, is not covered by the Estonian mandatory confiscation regime: this is neither covered by § 83(1) PC (it cannot be considered as "*the object used to commit an intentional offence*" which refers to instrumentalities only), nor by the recently introduced § 83[1] ("*Confiscation of assets acquired through offence*" which refers to proceeds only), nor by the specific confiscation provisions of the money laundering offence.

217. § 394(5) PC allows for the discretionary application of confiscation to laundered property which was the direct object of a money laundering offence. The recommendation from the second evaluation report to Estonian authorities to consider the introduction of a mandatory confiscation regime for laundered property was partially followed as Estonia introduced with § 394(6) PC for certain predicate offences an extended confiscation regime for proceeds of the money laundering offence (see below para 223).

218. Since 1 February 2007 *confiscation of proceeds of crime is mandatory* (§ 83[1] Penal Code). The court may refrain from confiscation if it would constitute an "*unreasonably burdensome*" or if the value of the assets is disproportionately small compared to the costs of confiscation. The property to be confiscated must belong to the offender at the time of judgment. Estonian authorities explained that as the confiscation of proceeds of an offence is now mandatory, courts have to reason in a decision why they refrained from confiscation in the relevant verdict or ruling.

219. Confiscation of proceeds from *third parties* is possible if an item belonging to a third party
- was acquired (wholly or partially) as a gift,
- at considerably below market value, or
- with knowledge that the object of the transfer was to avoid confiscation.

An object of a crime can also be confiscated from a third party who "*aided in the use of the objects or substance for the commission or preparation of the offence*".

220. According to the firm and unanimous interpretation of judges and prosecutors met during the on-time visit, it can be concluded that confiscation may extend to *direct and indirect proceeds of crime including income, profits or other benefits from the proceeds from crime* and to proceeds belonging to third parties. It appears that Estonian practitioners are aware of the wide meaning of the term "*proceeds*" under the Strasbourg Convention ("*any economic advantage from criminal offences*") and the restrictive approach identified in the past, which limited proceeds only to the direct object of the crime, is overcome.

221. A considerable novelty after the second round evaluation is the introduction of *extended confiscation of proceeds of crime* (as from 1 February 2007) where the principle of reversed burden of proof is applied (§ 83² PC). The extended confiscation of proceeds may comprise "*a part or all of the offender's assets"* and is *mandatory* applied by the court when certain preconditions are fulfilled:
- a final conviction; or
- penalty of imprisonment more than 3 years or life imprisonment; or
- the proceeds belong to the offender at the time of the judgment; or
- 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.

The confiscation may be avoided if the person establishes the lawful origin of the alleged proceeds of crime. Due to the use of the definite article in the English version of § 83^2 (1) Penal Code ("*through commission of <u>the</u> criminal offence*"), the question arose whether the proceeds must be obtained from a specific offence. The evaluators were assured that the Estonian language does not use either definite or indefinite articles and that this text refers to criminal activity in general and has not to be linked with a specific offence. This statement was also confirmed by practitioners with whom the evaluators met.

222. The second subsection of § 83^2 allows the extended confiscation of proceeds of a crime even if it belongs to a *third party* (thus corresponding to the requirements of criterion 3.1.1 b). This is done by way of exception and when the following conditions are met:
- the property was 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
- the third person knew that the assets were transferred to the person in order to avoid confiscation.

Assets of a third party which have been acquired more than five years prior to the commission of a criminal offence shall not be confiscated.

223. *Extended confiscation* is applied in the cases when the Special Part of the Penal Code makes explicit reference to this institute. This is the case for the following designated offences: participation in an organised criminal group and racketeering, terrorism, including terrorist financing, enslaving (as part of the designated offence trafficking in human beings and migrant smuggling), aiding prostitution and prostitution involving minors (as part of the designated offence sexual exploitation, including sexual exploitation of children), illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking, accepting bribes (as part of the designated offence corruption and bribery) and smuggling (see also Annex II).

224. The *confiscation of the instrumentalities used in* the commission of a crime is regulated in § 83 (1) as a non-mandatory option and only when the property belongs to the offender at the time of ruling of judgement. The provision of § 83 (1) has been amended after the second evaluation round in the way that the confiscation of proceeds has been regulated separately in the new § 83[1] "Confiscation of assets acquired through offence" which was dealt in the previous paragraphs. The remaining parts of this section remained to great extent the same and therefore the main criticism towards them from the second evaluation are still valid.

225. The *confiscation of the instrumentalities intended for use in* the commission of a crime is provided for in § 83 (2) as a non-mandatory possibility only in cases provided by law in cases where the preparation of a crime is criminalised itself. The property should belong to the offender at the time of the ruling of the judgement. As neither the preparation of money laundering nor the preparation of terrorist financing are separately criminalised, it is not possible to confiscate the instrumentalities *intended to be used* in the commission of the money laundering or the financing of terrorism offence.

226. Again designed as an exception, a court may confiscate instrumentalities belonging to a *third person* who "*has, at least through recklessness, aided in the use of the objects or substance for the commission or preparation of the offence; 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 knew that the objects or substance was transferred to the person in order to avoid confiscation thereof*" (§ 83 (3) PC).

227. The confiscation of instrumentalities based either on § 83 (1) and (2) is only possible when a person has committed an offence. An act is considered to be an offence when it has reached at least the stage of the attempt (and there are no circumstances eliminating the unlawfulness of it). The other articles of the general part of the Penal code do not distinguish between a completed offence and attempt. When an article of the Penal code refers to the offence, it comprises both completed offences and attempts.

228. The preparation of a crime in accordance with Estonian penal law is generally not punishable (the preparation is the stage which can take place before the attempt has started). The preparation is punishable only when it is explicitly mentioned in the special part of the PC. In case the preparation of a crime is punishable, all articles of the General part are applicable to that.

Application of confiscation of instrumentalities in case of terrorist financing

229. Despite the fact that, as mentioned before, the preparation of a crime as a rule is not punishable (as it is also the case with terrorist crimes) the completed crimes may have also the stage of preparation. For example the perpetrator makes or acquires the instrumentalities needed for committing a crime (e.g. gets himself the equipment needed for copying credit cards). In these cases, when the act already reaches the stage of an attempt, it may be needed to confiscate also these instrumentalities which were not directly used for committing a crime but for the preparation of a crime. But the precondition for confiscation in such cases is that the crime has reached at least the stage of attempt.

230. § 83 is applicable only when a terrorist offence has reached at least the stage of the attempt. But when the offence is already punishable based on PC, both (1) and (2) are applicable. The money used for terrorist financing would definitely be the object used to commit an offence.

231. Concerning value confiscation, § 84 PC provides that 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. This provision however applies only to proceeds of crime and not to instrumentalities used or intended to be used in the commission of a crime.

232. The Penal Code provides that the confiscated property goes to the state or, in cases provided for in an international agreement, may be transferred to a foreign state. During the on-site visit the Estonian authorities explained that there are no international agreements concluded, but there was a case of asset sharing with two foreign states on an ad-hoc basis.

233. Evaluators were informed that § 40 (7) MLTFPA provides a useful tool for prosecutors and investigative bodies to "*transfer property to state ownership*" in specific cases where the ownership of the property is uncertain or could not be proven by the relevant person. § 40 (7) has to be read in conjunction with § 40 (6) MLTFPA which allows the FIU or an investigative body to "*restrict the disposal of property until identification of the actual owner of the property as well as upon termination of criminal proceedings if it has not proven possible to establish the actual owner of the property and if the possessor of the property declares that the property does not belong to the possessor and relinquishes possession thereof*". After measures in accordance with § 40 (6) MLTFPA have been imposed, § 40 (7) MLTFPA comes into play which allows that:

> *(7) The Prosecutor's Office or an investigative body may apply to an administrative court for permission to transfer property to state ownership if, within a period of one year as of establishment of the restrictions on the disposal of the property, it has not proven possible to establish the owner of the property and if the possessor of the property declares that the property does not belong to the possessor and relinquishes possession thereof. In the event where possession of movable property or immovable property is relinquished, the property shall be sold pursuant to the procedure provided in the Acts regulating enforcement procedure and the amount received from the sale is transferred to the state budget. The owner of the property has the right to reclaim an amount equivalent to the value of the property within a period of three years as of the date on which the property is transferred to state ownership.*

The evaluators were informed that both prosecutors and the FIU had already applied these provisions several times. However, it has to be noted that these provisions do not deal particularly with money laundering or terrorist financing cases but provide only supplementary confiscation/seizing powers in cases where the ownership of property is uncertain.

234. § 142 of the Code of Criminal Procedure gives the definition of seizure: "*Seizure of property' means recording the property of a suspect, accused, 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*"[16]. The Estonian authorities confirmed that this definition applies to the seizure of property which can be both proceeds or instrumentalities of a predicate offence or object of money laundering or terrorist financing.

235. The objective of the seizure of property is to secure a civil action, confiscation or fine to the extent of assets. The seizure is applicable for any object that can be confiscated pursuant to the Criminal Code including proceeds from crime as well as instrumentalities of or objects resulting from a criminal act. The examiners in the second round evaluation had the impression that provisional measures were taken more frequently to secure civil actions rather than to ensure that proceeds were available (which could be subject to criminal confiscation) and recommended to the Estonian authorities to review their provisional measures regime to ensure that it fully enables the freezing and seizing of all criminal proceeds swiftly. Estonian authorities met during the third round evaluation provided the examiners with impressive examples of seizure actions, many of which resulted in a confiscation after the final conviction. Therefore the evaluators concluded that the current provisional measures regime is geared towards preserving assets likely to be confiscated as proceeds of crime.

[16] § 142 CCP was recently amended (entering into force on 23 May 2008) and now the convicted person has been added to the list of persons whose property may be seized.

236. Property is seized at the request of the prosecutor and on the basis of an order of a preliminary investigation judge or on the basis of a court ruling (§142 (2) CCP). The Estonian authorities stated that the standard of proof for obtaining a seizure order is generally lower then that required for confiscation. The examiners were also given examples of the relatively fast realisation of the seizure orders. The legislative framework is supportive to the swift development of this procedure: in cases of urgency, property, except property which is the object of money laundering, may be seized by the prosecutor or investigator without the permission of a preliminary investigation judge. The preliminary investigation judge must be notified of the seizure within 24 hours after the seizure and the judge immediately decides whether to grant or refuse permission. If the preliminary investigation judge refuses to grant permission, the property is released from seizure immediately. (§142 (3) CCP).

237. There are also special provisions regulating the seizure of movables, construction works, buildings which are movable and motor vehicles.

238. The CCP does not require that *prior notice* be given to the person subjected to seizure. §142 (5) CCP provides that a ruling on the seizure of property shall be submitted for examination to the person whose property is to be seized or to his or her adult family member upon the performance of the procedural act. The person or family member shall sign the ruling to that effect. Thereafter the person has the right to appeal the court ruling in accordance with § 384 CCP which states that the parties to a court proceeding and persons not participating in the court proceeding have the right to file appeals against a ruling of a county court if the ruling restricts their rights or lawful interests. The appeal does not postpone the procedures. Estonian authorities stated that in practice, the person subjected to seizure is not present when seizure is ordered.

239. Law enforcement agencies appear to have sufficient powers to trace and identify property as required by Criterion 3.4. Chapter 3 of the Criminal Procedure Code provides for all investigative measures that may be used by investigation and prosecution authorities for gathering evidence in order to trace the proceeds of crime. The same investigative measures may be used for tracing the proceeds of crime, as are used for gathering evidence in general.

240. In particular, the hearing of witnesses (§ 68 CCP), search (§ 91 CCP), seizure and inspection of documents (§ 86 CCP) may be used for tracing the proceeds of crime. The surveillance measures (§§ 110-122 CCP) include covert surveillance, covert examination of postal or telegraphic items, wire tapping or covert observation of information transmitted through technical communication channels or other information. The Estonian authorities advised that account monitoring, controlled delivery of cash and electronic surveillance are also being used accordingly to the CCP with the permission of the preliminary investigation judge.

241. The Penal Code provides for protection of the rights of *bona fide third parties* in cases of confiscation but there are no provisions concerning the protection of the rights of bona fide third parties in cases of seizure.

242. According to § 85 PC, in case of *confiscation*, the rights of third persons remain in force. If the authorities have unjustly damaged lawful rights of third parties during the confiscation procedure, the state is obliged to pay compensation to them, except in the cases provided for in §83(3) and (4), §83^1 (2) and §83^2 (2) PC. As mentioned above (para 222), assets of a third party which have been acquired more than five years prior to committing a criminal offence may not be confiscated.

243. § 40^1 CCP by reference to § 34 CCP provides that if confiscation of the property of the third party is decided in criminal proceedings, the third party has the right to know the content of the suspicion and give or refuse to give testimony with regard to the content of the suspicion. He/she also has the right to know that his or her testimony may be used in order to bring charges against him or her, to be interrogated and participate in confrontation, comparison of testimony to

circumstances and presentation for identification in the presence of a counsel, taking account of the specifications of confiscation.

244. The legislation stipulates the freezing of property from third parties in § 142 CCP as follows: "*'seizure of property' means recording the property of a suspect, accused, 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*".

245. As to the question what happens to the rights of these third parties if no confiscation follows there are no legal provisions in place dealing with such a situation. However, the Supreme Court has clearly expressed that the absence of such provisions may not exclude the state's obligations towards individuals and in such cases the claim may be based on the general principles of the law[17].

246. The Estonian authorities assured the evaluation team that in current court practice such claims have been implemented on general principles of the law. In addition, it was also stated that the Ministry of Justice has acknowledged this omission and is currently working on a draft law. Evaluators would encourage such a legislative development taking into account the established activity of Estonian investigation and prosecutorial authorities to use more frequently the institute of confiscation. The expressive legislative provision for the protection of the rights of bona fide third parties during the phase of securing the confiscation would contribute to the legal certainty and rule of law.

247. The 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

248. Membership of 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 § 255 PC. The property of the organisation is considered as means intended to commit a crime and therefore liable to confiscation. The Penal Code provides that the court imposes extended confiscation (for details see above para 223) of the property obtained by the criminal offence; though extended confiscation is not exactly the same as required by criterion 3.7a), this feature at least addresses some elements of it.

249. The confiscation system in Estonia is based on criminal conviction and does not allow for civil forfeiture. Confiscation orders cannot be made where a defendant has died or absconded or where his whereabouts are otherwise unknown. According to § 199 CCP, among the circumstances precluding criminal proceedings are that the suspect or the accused is dead or the suspect or accused who is a legal person has been dissolved unless "*it is necessary for the rehabilitation of the deceased person, or upon detection of new facts, for the resumption of criminal proceedings with regard to another person*." According to § 206 (2) CCP, the order on termination of criminal proceedings shall set out the annulment of the preventive measure applied or other means of securing criminal proceedings how to proceed with the physical evidence or objects taken over or subject to confiscation.

[17] Ruling nr 3-3-1-10-01 (Decision of Administrative Law Chamber from 17 April 2001, section 4; http://www.nc.ee/?id=11&tekst=RK/3-3-1-10-01).

Statistics

250. In five of the proceedings which led to the 7 convictions for money laundering, provisional measures (seizure) were imposed on different kind of property (cars, real estates, land, bank accounts, electronic devices, money in different currencies). Confiscation was ordered for instrumentalities of crime (a car, a computer), objects and proceeds of crime (cars, electronic devices, real estate, money). The evaluators were provided with these figures from one prosecutor under special request when on-site; it was explained that this data stems from the courts' information system but that so far it was not kept in form of a chart etc. It has to be noted that the courts' information system is beyond doubt a useful tool, yet it is not the same as commonly understood under "statistics" which means not only the collection but also the analysis, interpretation, explanation and presentation of data (e.g. in a table, graph etc.). With other words, the data kept by courts provide the basis to produce statistics but they do not present statistics *per se*. However, the figures given to the evaluation team were presented in form of a chart and it is recommended that this chart is regularly updated.

251. Concerning statistics on seizure and confiscation orders, the same situation as described above applies, i.e. the Ministry of Justice keeps the data in the courts information system and the FIU produces statistics on this data: this means in practice that the FIU keeps statistics concerning

a) seizure orders,
b) extended confiscation (§ 83^2 PC) which were imposed in all criminal cases;
c) all kind of confiscations connected with money laundering cases.

252. After the plenary and following a request of the plenary, Estonian authorities provided the following table showing the confiscation and seizure orders including the respective amounts of the last three years:

	2005	2006	2007	2008[18]
No of money laundering convictions	2	1	5	4
→ No of convictions where property was seized	0	0	3	1
→→ *Seized objects*	-	*0*	*Bank account, real estate, electronic devices, 4 cars, 39 160 EUR*	*Bank account*
→ No of convictions where confiscation was used	0	0	4	0[19]
→→ No of convictions where the object used to commit offence was confiscated (§ 83 PC)	0	0	3	0
→→→ *Confiscated objects*	-	-	*1 car, computers*	-
→→ No of convictions where the assets acquired through the offence were confiscated (§83^1 PC)	0	0	3	0
→→→ *Confiscated objects*	-	-	*3 cars, real estate, electronic devices, 43 470 EUR*	-
→→ No of convictions where extended confiscation of assets acquired through the offence was used (§83^2 PC)	0	0	0	0

2.3.2 Recommendations and comments

253. The evaluation team noted significant progress in the Estonian confiscation regime. A number of shortcomings identified during previous evaluation rounds were removed:

- Estonia has introduced a system with generally greater mandatory confiscatory elements in it as far as *proceeds* are concerned;

[18] 2008 data represents the verdicts of 11 months.

[19] In one of the proceedings where the person acquired criminal assets through an offence, these assets had been already confiscated in another court proceeding (in which the person was convicted in another offence).

- the restrictive approach identified in the past, which was limited only to the direct object of the crime was changed and now both direct and indirect proceeds are confiscatable;
- value based confiscation system is in place concerning proceeds of crime;
- there are possibilities for reversing the burden of proof in certain cases.

254. The third round evaluation team was also satisfied that the new provisions on seizure and confiscation are assessed very positively by practitioners (investigators and prosecutors) and are being widely used by them. This applies also for international cooperation – there are good examples of provisional measures, confiscation and sharing assets with foreign countries in recent Estonian practice.

255. However, there are still some important elements missing and it is recommended to amend accordingly the relevant provisions of the general confiscation regime and also the specific provisions of the money laundering offence:
- laundered property, where money laundering is the only offence being proceeded with, is not covered by the Estonian mandatory confiscation regime: this is neither covered by § 83(1) PC, nor by the recently introduced § 83^1 PC, nor by the specific confiscation provisions of the money laundering offence;
- Confiscation of instrumentalities used or intended to be used is non mandatory and applies to only part of the designated offences (among which neither money laundering nor terrorist financing offences are included);
- 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).

256. Notwithstanding these deficiencies, it has to be noted that the authorities invested substantial efforts to promote the use of confiscation. They pursue systematically the approach of "following the proceeds of crime". For this purpose several training seminars for different law enforcement authorities were organized for the financial investigators, policemen, prosecutors and judges. Training included theoretical information, practical examples and case studies. The features of confiscation has been discussed and analysed frequently. The recently introduced extended confiscation regime is widely used by practitioners and a number of confiscation orders and seizure orders happened: In 5 cases of the 7 convictions seizures were imposed and significant numbers of confiscation orders could be achieved.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**LC**	• 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 applies to only part of the designated offences (among which neither money laundering nor terrorist financing offences are included). • 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.

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

2.4.1 Description and analysis

257. Criteria III.1 and III.2 require that countries have effective laws and procedures to freeze terrorist funds or other assets of persons designated either by the United Nations Al-Qaida and Taliban Sanctions Committee in accordance with S/RES/1267(1999) or in the context of S/RES/1373(2001).

Legal framework for implementing international sanctions

258. As a member of the European Union, Estonia implements the sanctions imposed by the Security Council of the United Nations under Chapter VII of the UN Charter by using the EU Common Foreign and Security Policy framework. The corresponding internal legislation comprises of the International Sanctions Act (in force since 2 January 2003, last amended in February 2004) and several Governmental Orders. The International Sanctions Act regulates the "*internal application of international sanctions where the imposition of international sanctions has been decided by the United Nations Security Council, the Council of the European Union, other international organisation, or Estonia at its own initiative*". The evaluators were told that currently this act is in the process of being redrafted.

259. Estonian authorities explained that the United Nations Security Council Resolutions (UNSCR) are not directly applicable in Estonia. The national system for implementing UNSCR is the following:

a) The Ministry of Foreign Affairs forwards the resolution or the decision to the competent authorities in Estonia which supervise the implementation of international sanctions.
b) The Ministry of Foreign Affairs in cooperation with national competent authorities assesses the need for national implementing measures. The Government of the Republic shall, on the proposal of the Ministry of Foreign Affairs, make a resolution on taking the necessary measures for the internal application of international sanctions (§ 4(1) ISA).

260. Among the measures to be taken by the Government of Estonia prescribed by the ISA are (§3):

- the prohibition of the granting of loans and credit and the payment of funds to a blocked entity or the legal and natural persons thereof;
- the prohibition of the transfer, pledging or any other use of funds, including bills of exchange, cheques and other means of payment, securities, precious metals or stones and other such assets which belong to a blocked entity or the legal and natural persons thereof;
- the prohibition of the transfer, pledging or grant of use of any funds, including bills of exchange, cheques and other means of payment, securities, precious metals or stones and other such assets to a blocked entity or the legal and natural persons thereof;

The FIU is empowered to exercise supervision over the application of the above mentioned measures specified in § 3 (1) 3) to 5) of the International Sanctions Act, "*unless otherwise provided by the Act or legislation of the European Union*" (§37 (1) 9 MLTFPA).

261. The definitions of entities and persons to whom these measures could be applied are listed in § 2 ISA:

- *blocked entity* means a state, certain territory, regime, organisation or other entity against whom the measures prescribed by the act are used;
- *legal person of a blocked entity* means a legal person who is registered in a blocked state, whose permanent seat is in a blocked entity, whose sole shareholder is a blocked entity or who is otherwise controlled by the blocked entity;
- *natural person of a blocked entity* means an alien who acts in the interests of a blocked entity or who is a citizen of a blocked state.

262. Financial sanctions imposed by UNSCR falls within the scope of the Treaty establishing the European Community. Therefore, with a view to ensuring their uniform application in all Member States, the Council of the European Union adopts a regulation, which is binding in its entirety and directly applicable in all Member States (Art. 249 TEC). For the purpose of EU Regulations concerning international sanctions, the territory of the Community is deemed to encompass the territories of the Member States to which the Treaty is applicable and is binding to any person elsewhere who is a national of a Member State, to any legal person, group or entity which is incorporated or constituted under the law of a Member State and to any legal person, group or entity doing business within the Community. On the entry into force of a European Union regulation, all natural and legal persons shall take all necessary measures, to ensure the fulfilment of the obligations arising out of the regulation. Member States should lay down rules on sanctions applicable to infringements of the provisions of the regulation and ensure that they are implemented.

263. UN Security Council Resolution 1267(1999) and its successor resolutions require countries to freeze the funds and other assets of persons who are designated by the United Nations Security Council. Names of the persons are sent to UN delegations and then circulated back to country authorities. All 1267 designations relate to freezing the funds and other assets of the Taliban, Osama Bin Laden and Al-Qaida and other individuals, groups, undertakings and entities associated with them. Freezing must occur without delay and without prior notice to targets. For the purposes of S/RES/1267(1999), the phrase *without delay* means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban Sanctions Committee.

264. UNSCR 1267(1999) and its successor resolutions had been implemented in the European Union via Council Common Positions 96/746/CFSP, 1999/727/CFSP, 2001/154/CFSP and 2001/771/CFSP. These Common Positions have been replaced by the Council Common Position 2002/402/CFSP of 27 May 2002, concerning restrictive measures against Osama Bin Laden, members of the Al-Qaida organisation and the Taliban and other individuals, groups, undertakings and entities associated with them and repealing Common Positions. As some of the measures foreseen in the Council Common Position 2002/402/CFSP fall under the European Community competence, the European Council adopted *Council Regulation (EC) No 881/2002 of 27 May 2002* imposing certain specific restrictive measures directed against certain persons and entities associated with Osama Bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan.

265. On 18 September 2001 the Government of Estonia adopted Governmental Order No 646-k, the aim of which was to take measures in order to implement the Council Common Positions 96/746/CFSP and 2001/154/CFSP. The Governmental Order No 646-K has been replaced by *the Governmental Order No 768-k* (adopted 27 November 2003).

266. On 5 August 2003, the Government of Estonia adopted Governmental Order No 477-k, the aim of which was to take measures in order to implement the Council Common Position 2002/402/CFSP and Council Common Position 2003/140/CFSP. Governmental Order No 477-k ordered inter alia that the Estonian Financial Supervisory Authority (FSA) is responsible to ascertain that the subjects of the financial supervision:

1) refrain from granting of loans and credit and from paying of funds to persons specified in Article 1 of the Council Common Position 2002/402/CFSP;
2) *refrain from transferring, pledging or using of funds, including bills of exchange, cheques and other means of payment, securities, precious metals or stones and other such assets which belong to the persons* specified in Article 1 of the Council Common Position 2002/402/CFSP, in any other way;

3) *refrain from transferring, pledging or making available of funds, including bills of exchange, cheques and other means of payment, securities, precious metals or stones and other such assets to the persons* specified in Article 1 of the Council Common Position 2002/402/CFSP.

267. After Estonia's access to the European Union (1 May 2004), the Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Osama Bin Laden, the Al-Qaida network and the Taliban, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan became directly applicable in the Republic of Estonia. However, Governmental Order No 477-k, which clarifies the competences of the competent national authorities regarding the implementation of the European Union's implementing measures, remained in force.

268. Article 2 of Council Regulation (EC) No 881/2002 provides for an obligation to freeze all funds and economic resources belonging to, or owned or held by, a natural or legal person, group or entity designated by the UNSC 1267 Committee. Article 2 also prohibits the making available of funds or economic resources, directly or indirectly, to, or for the benefit of, the designated persons, groups or entities. The designated natural and legal persons, groups and entities are listed in Annex I of the Regulation. The Commission, as authorised by article 7, amends or supplements Annex I on the basis of determinations made by either the UNSC or the 1267 Committee.

269. UN Security Council resolution 1373(2001) has been implemented in the European Union and its member states via Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP). As some of the measures foreseen in the Council Common Position 2001/931/CFSP fall under the European Community competence, the Council adopted *Council Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view of combating terrorism.*

270. On 26 September 2003 the Government of Estonia adopted Governmental Order No 591-k, the aim of which was to take measures in order to implement the Council Common Position 2001/931/CFSP. The Governmental Order No 591-k has been replaced by the Governmental Order N 768-k (adopted 27 November 2003).

271. Both Governmental orders require the FSA to ascertain that the subjects of the financial supervision:
1) refrain from *granting of loans and credit* and from paying of funds to the persons specified in the annex of the Council Common Position 2003/651/CFSP;
2) refrain from *transferring, pledging or using of funds*, including bills of exchange, cheques and other means of payment, securities, precious metals or stones and other such assets which belong to the persons specified in the annex of the Council Common Position 2003/651/CFSP (excluding persons marked with asterisk), in any other way;
3) refrain from *transferring, pledging or making available of funds*, including bills of exchange, cheques and other means of payment, securities, precious metals or stones and other such assets to the persons specified in the annex of the Council Common Position 2003/651/CFSP (excluding persons marked with asterisk).

272. After Estonia's access to the European Union (1 May 2004), the Council Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view of combating terrorism (which implements the Council Common Position 2001/931/CFSP and the UN Security Council resolution 1373(2001)) became directly applicable in Estonia. The Governmental Order No 768-k, which clarifies the competencies of the competent national authorities regarding the implementation of the European Union's implementing measures, also remained in force.

273. Article 2 of the Council Regulation 2580/2001 provides for an obligation to freeze all funds, other financial assets and economic resources belonging to, or owned or held by, a natural or legal

person, group or entity listed by the Council of the European Union. Article 2 also prohibits the making available of funds, other financial assets and economic resources, directly or indirectly, to, or for the benefit of the listed persons, groups or entities. Furthermore, article 2 imposes a prohibition on the provision of financial services to, or for the benefit of, listed persons, groups or entities. The list of persons, groups and entities to which these provisions apply is maintained by the Council acting by unanimity. The Council reviews and amends the list of targeted persons, groups and entities in accordance with article 1(4) to 1(6) of Common Position 2001/931/CFSP.

274. According to § 37(1)9) MLTFPA, the supervisory authority for the implementation of financial international sanctions is the Estonian FIU which is responsible for exercising supervision over the application of the measures specified in § 3 (1) 3) to 5) of the International Sanctions Act (unless otherwise provided by the Act or legislation of the European Union).

275. In the event of suspicion of terrorist financing, the FIU "*may issue a precept suspending a transaction or to imposing restrictions on the disposal of an account or other property constituting the object of the transaction for up to thirty days as of the delivery of the precept*". In the case of property registered in the land register, ship register, traffic register or commercial register, the FIU may, in the event of justified suspicion, restrict the disposal of the property for the purpose of ensuring its preservation for up to thirty days (§ 40 (1) MLTFPA). On the basis of a precept, the FIU may restrict the use of property for up to 60 days for the purpose of ensuring its preservation if there is suspicion that the property is used for terrorist financing (§ 40 (3) 2) MLTFPA).

276. If financial sanctions imposed by European Union measures are narrower than required by UNSCR, then in addition to European Union legislation, the International Sanctions Act prescribes the adoption of national implementing measures. The ISA does not establish a practical administrative procedure for freezing the accounts of names on the respective lists but could serve as the legal basis for introducing such a procedure. The Government could, on the proposal of the Ministry of Foreign Affairs, make a resolution on taking the measures necessary for the internal application of international sanctions (§ 4(1) ISA). In every single case the Ministry of Foreign Affairs in cooperation with national competent authorities supervising the implementation of international sanctions would have to assess the need for national implementing measures in addition to European Union measures. As confirmed by the Estonian authorities, there have been no cases to implement UNSCR through additional national implementing measures yet which means that this law has not yet been applied in any concrete case.

277. As an EU Member State, Estonia relies on EC Regulation 2580/2001 and Common Position 931/2001 for the implementation of UNSCR 1373 and its successor resolutions. EC Regulations are immediately effective on national legal systems of EU member states. However, to fully implement UNSCR 1373, EU Member States also need to have national systems in place. EC Regulation 2580/2001 (which relates to freezing action taken pursuant to UNSCR 1373) only deals with freezing the funds/other assets of "non-EU nationals" (meaning persons/entities that have a connection outside of the EU). EU member states must have domestic procedures or mechanisms in place to freeze the funds/other assets of "EU-internals" (persons, groups and entities having their roots, main, activities and objectives within the European Union). The list in Council Regulation 2580/2001 includes only the names of the persons and entities linked or related to third countries as well as those who otherwise are the focus of the CFSP aspects of Common Position 2001/931/CFSP (recital 13 of the Regulation). Hence, persons and entities having their roots, main activities and objectives within the EU may only be listed in Common Position 2001/931/CFSP. In the Common Position, they are marked with an asterisk that indicates that they are only covered by article 4 (commitment of member States to afford each other police and judicial co-operation), and thus they are not subject to the requirement of asset freeze, nor included in the list of the Council Regulation. Therefore Estonia cannot administrate freezing measures against EU-internals without additional legislation in place. In respect of the

requirements of SR III, this is an important shortcoming in the ability to effectively freeze and seize terrorist-related assets.

278. Estonia's implementation of Recommendation 3, including the laws and procedures to take actions initiated under other jurisdictions, has already been explained above in Section 2.3. However, in relation to Special Recommendation III, the legal situation is less comprehensive: states that are not members of the EU can 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 article 1 of Common Position 2001/931/CFSP, have to be fulfilled. Requests from non-EU members for freezing must be sent to the EU and are considered by the EU Council, which must agree unanimously to act on the request. If no such listing takes place, in practice a situation may arise where a request for freezing is sent to Estonia which, although substantiated, could not be followed because the respective person was not on the list of the EU.

279. As already stated, Estonian authorities may freeze funds of designated persons. The EC Regulations require the freezing of assets of every kind, including immovable property, undertakings and vehicles. However, the definition of "funds" in the relevant EU regulations is not broad enough: Article 1 of both Council Regulation 2580/2001 and Regulation 881/2002 defines the funds and economic resources to which freezing may be applied. These assets are belonging to, owned or held by a designated person. Regulations do not cover funds controlled by them or persons acting on their behalf or at their direction (as it is required by UNSCR1267 and 1373). As confirmed by the Estonian authorities, there is no additional system in place outside the EU legal framework. In addition, the limited nature of the terrorist financing offence in Estonia does not include funds for individual terrorists where there is no link to a specific terrorist act. Thus, the evaluators consider criterion III.4 only partially observed.

280. The Estonian authorities described the system for communicating to the financial sector actions under the freezing mechanisms as based on the provisions of the International Sanctions Act and encompassing consultations among Ministry of Foreign Affairs, FIU and the Financial Supervision Authority, and in co-operation with other relevant government agencies and the relevant EC body.

281. The Estonian authorities explained the procedure as follows: Though the Ministry of Foreign Affairs sends the consolidated UNSCR lists to the FSA and the FIU, the FIU does not need this information as it checks itself the updates on the website of the United Nations Al-Quaida and Taliban Sanctions Committee. There is a link on the website of the FIU to both the list of the United Nations Al-Quaida and Taliban Sanctions Committee and to the "Consolidated list of persons, groups and entities subject to EU financial sanctions" (including information regarding its latest update). The website of the FIU allows the obligated entities to do a name-search in both of these lists. Representatives of the FIU also advised that it was agreed within the "Advisory Committee on Prevention of Money Laundering and Terrorist Financing" that the FIU does not send regularly updates to the obligated entities but that the FIU provides such an "update service" on its website and that the obligated entities are obliged to check themselves whether there are updates. Furthermore, on the web-site of the FSA is a link to the Official Journal of the European Union and the credit institutions are obliged to follow this list which is updated by the European Union in the relevant regulations. Both the Ministry of Interior and the Police receive information on these lists directly from the Ministry of Foreign Affairs. There are no obstacles for the Estonian authorities to use other lists. However, the Estonian authorities are not actively looking for other lists than the ones mentioned above. Nonetheless, it was explained that if the FIU would receive information (not restricted to lists) from foreign FIUs or other jurisdictions/international organisations, the FIU would forward it to banks. If the State Prosecutors Office receives additional information about listed persons, it coordinates the tasks of the other bodies (mainly Police and FIU) to undertake further investigations.

282. However, concerning the services provided by the FIU and the FSA on their respective websites (name-search and web-links), it has to be noted that during the on-site visit only representatives from the insurance and currency exchange sectors were aware of the lists; representatives from the other obligated entities could not report about such a procedure: representatives from banks explained that they take this list from the website of the European Union; their IT specialists make out of it a searchable document and this is weekly updated. Some foreign owned banks have screening tools from their parental banks covering both EU lists and also OFAC list. Investment firms use the list of the EU but explained that they had not received a list from Estonian authorities since 2005. Representatives from Savings and Loan Associations were not at all familiar with procedures or lists related to Special Recommendation III.

283. The obligated entities are obliged to include in their rules of procedure instructions for how to effectively and quickly identify whether or not a person is "*a person with regard to whom international sanctions are imposed*" (§ 30 (4) 4) MLTFPA). The evaluators were told by the Estonian authorities that if a bank detects a designated name in its database, it has to be reported to the FIU immediately (though such an obligation is not explicitly mentioned in the MLTFPA and can only be deferred from the context of the MLTFPA). The possibilities for the FIU in the event of a suspicion of terrorist financing have been described above (para 275).

284. The Ministry of Foreign Affairs has a special section on its web-site named "International Sanctions" where the competent authorities for the implementation of EU restrictive measures are also placed. The FIU and the FSA are stated as responsible for the implementation of financial sanctions (freezing of funds and economic resources) with reference to their coordinates, including web addresses (FIU: http://www.politsei.ee/?id=814; FSA: http://www.fi.ee/)

285. According to Art. 30 MLTFPA, the application of international sanctions (restrictive measures) on designated persons should be part of the financial institutions' internal procedures, which are subject to the FIU's supervisory activities.

286. In January 2008, after the promulgation of the new MLTFPA the FIU issued "*Financial Intelligence Unit's Advisory Guidelines Regarding Characteristics of Transactions Suspected of Terrorist Financing*". These guidelines (both in Estonian and English) are accessible to the public on the web-site of the FIU[20]. Under point 6 of the Guidelines it is explicitly clarified that the credit and financial institutions and other subjects are obliged to verify upon establishment of customer relationships and execution of transactions whether the natural person, legal person or another entity has been included in the consolidated list of financial sanctions of the European Union or UN.

287. The FIU maintains an Internet site aimed at financial institutions and accessible to all. The web-site describes the obligations based on the sanctions' regulations, underlines the obligations based on the sanctions regulations and includes information concerning the status and legal effects of Council and Commission Regulations and a list of the sanctions in force, and a link to the EU list of financial sanctions in force. The FIU also sends circulars to financial institutions and provides the necessary guidance on their duties, including the duty to report the existence of funds belonging to targeted persons.

288. According to § 63 (2) 6 of the Credit Institutions Act, credit institutions have to establish internal rules to combat money laundering and terrorist financing. On the basis of § 57 of the Financial Supervision Authority Act, the FSA has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and to provide guidance to subjects of financial supervision. In 2004 the FSA issued "Additional measures for supplementing internal procedures related to implementing the sanctions established according to International Sanctions

[20] http://www.politsei.ee/files/rab/Guidelines_terrorism_financing.pdf.

Act or request of mutual legal assistance in credit and financial institutions" which have been made available on the FSA public web-page.

289. Notwithstanding all the information measures undertaken by the Estonian authorities, the evaluators were under the impression from the meetings with representatives of the obliged entities and private sector that there is no widespread knowledge or everyday use of the sanctions lists. Apart from banks, no other financial institutions or DNFBP are aware of the procedure to be followed in order to implement the UN resolutions (see also para 281 above).

Mechanisms for de-listing, unfreezing and challenging measures

290. The Estonian authorities explained that all the EC Common Positions and other international sanctions (restrictive measures) are considered as directly applicable. 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). All the relevant measures, including contra measures, i.e. de-listing conditions, are also provided in relevant EC positions.

291. There is no established national procedure for the purpose of considering de-listing requests. With regard to both the Al Qaeda/Taliban list and the EU terrorist list, the designated persons and entities also have the right to institute proceedings before national courts or the European Court of Justice.

292. Concerning de-listing of persons by the Al Qaeda and Taliban Sanctions Committee or the EU, the Estonian system allows quick updates as the lists are not circulated but only available as daily updated links on the website of the FIU (and concerning the EU terrorist list also on the website of the FSA).

293. There is no national procedure in Estonia for unfreezing, in a timely manner, the funds or other assets of persons or entities inadvertently affected by freezing mechanism upon verification that the person or entity is not a designated person. According to the Estonian authorities all unfreezing procedures are subject to the internal procedures of competent authorities and the institutions. During the on-site discussions the authorities stated that in a situation where a person seeks unfreezing of assets, the institution holding the frozen funds will notify the FIU or (FSA in case of a subject of financial supervision) of the customer's request for unfreezing. They respectively will pass this information to the Ministry of Foreign affairs which will bring the case to the UN/ EU for consideration. Theoretically, in case sanctions would have been imposed according to the International Sanctions Act, the Ministry of Foreign affairs would pass the draft decision on unfreezing to the Government of Estonia. Estonian authorities referred concerning unfreezing requests also to §§ 18 and 19 of the Public Information Act which read as follows :

> *§ 18. Terms for compliance with requests for information and calculation of terms for processing*
> *(1) A request for information shall be complied with promptly, but not later than within five working days.*
> *(2) If a request for information cannot be complied with due to the insufficiency of the information submitted by the person making the request for information, the holder of information shall notify the person making the request for information thereof within five working days in order to specify the request for information.*
> *(3) The terms for processing requests for information provided for in this Act shall be calculated as of the working day following registration of the requests for information.*
> *§ 19. Extension of terms for compliance with requests for information*
> *If a holder of information needs to specify a request for information or if identification of the information is time-consuming, the holder of information may extend the term for compliance with the request for information for up to fifteen working days. The holder of information shall notify the person making the request*

for information of extension of the term together with the reasons therefore within five working days.

However, it has to be noted that these provisions are only general obligations of authorities within which timeframe they have to comply with requests subject to the Public Information Act but do not provide a specific legal basis for unfreezing requests.

Authorising access to funds for certain expenses

294. The EU Council Regulations lay down exceptions to the application of financial sanctions. Council Regulation (EC) No 561/2003 introduced a new article 2a on exceptions into Council Regulation (EC) No 881/2002 and thereby implemented the S/RES/1452(2002). There are also exceptions included in Council Regulation No 2580/2001, articles 5 and 6. With regard to Estonia, in the annexes to the Council Regulations, the Ministry for Foreign Affairs is determined as the competent authority for the implementation of sanctions, and the Financial Supervision Authority as the competent authority concerning sanctions linked with the freezing of funds (Act of Accession 2004, Annex II, section 20, point 11 (OJ L 236, 23 September 2003, p. 773). Therefore, the competent authority in Estonia to grant the authorisations referred to in the provisions on exceptions is the Financial Supervision Authority, which may authorise the release of certain frozen funds or economic resources or make available certain funds or economic resources, under such conditions as it deems appropriate, after having determined that the funds or economic resources concerned are:

- necessary to satisfy the basic needs of persons subject to the international sanctions and their dependent family members, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges;
- intended exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services; or
- intended exclusively for payment of fees or service charges for routine holding or maintenance of frozen funds or economic resources.

295. Any person who feels aggrieved by a decision whereby his funds or other assets have been attached or frozen, may apply to courts for redress. Persons dissatisfied with actions taken to freeze their assets or funds can also apply to the European Court of Justice and the European Court of Human Rights for a remedy. In particular, the Estonian authorities advised that the procedures are as follows:

- If a person claims that a financial institution has frozen his/her funds or assets by mistake causing damage to him/her and that the financial institution has been negligent by doing so, this person can file an action against the negligent financial institution to an Estonian civil court according to the Code of Civil Procedure.
- If a person concerned seeks to contest a national implementing act or measure, then he/she has to file an action or protest to the Estonian administrative court according to the Code of Administrative Court Procedure.

Freezing, Seizing and Confiscation in other circumstances

296. The general criminal law framework and mechanisms on seizure and confiscation have been described in Section 2.3. They also constitute to a large extent the basis for measures under criterion III.11. The Estonian prosecutorial and judicial authorities may apply some other measures in the context of a criminal investigation or prosecution to freeze, seize or confiscate assets suspected or proven to be related to terrorist financing. These measures include:

- Financial and other institutions covered by the *MLTFPA* can suspend or decline a transaction for the purpose of carrying out further inquiries, provided that there is reason to suspect that the funds involved in the transaction are used for the financing of terrorism.
- In the event of suspicion of terrorist financing, the FIU may issue a precept to suspend a transaction or to impose restrictions on the disposal of an account or other property constituting the object of the transaction for up to thirty days following the delivery of the

precept. In the case of property registered in the land register, ship register, traffic register or commercial register, the FIU may, in the event of justified suspicion, restrict the disposal of the property for the purpose of ensuring its preservation for up to thirty days. During the time that restrictions on using an account are in force, the credit or financial institution shall not execute any orders issued by the account holder for debiting the account. On the basis of a precept, the FIU may restrict the use of property for up to 60 days for the purpose of ensuring its preservation if there is suspicion that the property is used for terrorist financing. If criminal proceedings have been commenced in the matter the disposal of property may be restricted for a term exceeding the specified terms.

- The Code of Criminal Procedure sets out in § 142 that in the case of the suspicion of terrorist financing, the property or object of the crime will be 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.
- In cases of urgency, property 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 of the seizure and the 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.
- The court may also seize property or place it under restraint or freezing order upon a request for international legal assistance

Protection for the rights of bona fide third parties

297. The general rule is that a person or entity complying with the obligations under Council Regulation 881/2002 cannot be held liable vis-à-vis a designated person or entity for any damage that may be suffered by the latter as a result. This is also indicated in the *EU Best Practices for the effective implementation of restrictive measures*. According to article 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*". In this case, compensation may be provided. In the case of assets frozen under Council Regulation 2580/2001 (S/RES/1373(2001)), there is no compensation envisaged. However, the Estonian authorities advised that *bona fide* third parties may use the available civil remedies under Estonian law, including those for damages, if he feels aggrieved by any measure taken. In this regard the Estonian authorities referred to § 25 of the Constitution of the Republic of Estonia, according to which everyone has the right to compensation for moral and material damage caused by the unlawful action of any person. Furthermore, they referred to Supreme Court Decisions and the State Liability Act (§ 14).

Monitoring compliance with freezing obligations

298. The relevant Council Regulations impose an obligation on banks, other financial institutions and insurance companies as well as other bodies and persons to provide information facilitating compliance with the Regulations, such as accounts and amounts frozen, to the competent authorities of the Member States - in Estonia this is the Ministry for Foreign Affairs (Article 5 of Council Regulation (EC) No 881/2002 and article 4 of Council Regulation (EC) No 2580/2001). The Estonian authorities informed the evaluation team that financial institutions and others contact the FIU in cases of close matches to the names on the lists. The FIU and MFA then have to determine whether the person/entity concerned is in fact the designated person. The FIU has not yet used its power to postpone a transaction on the basis of such a disclosure.

299. The violation of measures necessary for the application of international sanction is criminalised according to § 93^1 of the PC as follows:

"(1) Violation of an internal measure necessary for the application of an international sanction is punishable by a pecuniary punishment or up to 5 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section."

Additional Elements

300. The Estonian authorities explained that the Ministry of Foreign Affairs is drafting a new law dealing with international sanctions, which would establish a more precise legal basis for enacting measures necessary for the implementation of international sanctions, taking into account the Best Practices Paper for SR.III hereby making it easier for Estonia to fulfil its international obligations

301. Under article 5 of Council Regulation 2580/2001, EU member States may on occasion and under appropriate conditions authorise the use of frozen funds to meet essential human needs (food, medicine, rent, etc.) and to pay taxes, compulsory insurance premiums, utility fees and charges due to a financial institution for the maintenance of accounts. The Estonian authorities advised that in practice, persons or entities whose assets have been frozen are entitled to submit applications to the FSA for granting access to funds to cover living expenses. When the FSA would receive such an application, it would immediately inform the Ministry of Foreign Affairs, which should coordinate the exchange of information with other states and international organisations.

Statistics

302. So far no terrorist assets have been frozen in Estonia pursuant to the relevant UNSC Resolutions.

2.4.2 Recommendations and comments

303. Estonia mainly relies on EU mechanisms to implement the obligations under Special Recommendation III; as these mechanisms do not fully cover the requirements of this Recommendation, Estonia needs to introduce supplementary national provisions in this regard.

304. Estonia should implement a national mechanism to give effect to requests for freezing assets and designations from other jurisdictions and to enable the freezing of funds of EU internals (citizens and residents). It is also recommended that a national de-listing process be established as part of these measures.

305. The definition of "funds" (as taken from the EU Regulations) does not explicitly cover funds owned 'directly or indirectly' by designated persons or those controlled directly or indirectly by designated persons; this should be amended and be brought in compliance with the requirements of UNSCR 1267 and UNSCR 1373.

306. Apart from banks, no other financial institutions or DNFBP are aware of the procedures to be followed in order to implement the UNSC Resolutions. Thus, the Estonian authorities should consider providing clear and practical guidance to financial institutions and other entities concerning their responsibilities under the freezing regime.

307. Estonia should introduce clear provisions regarding the procedure for unfreezing 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.

308. It is worth noting that the Estonian authorities are aware that the regulation of publicly known procedures for de-listing, unfreezing or granting access to funds for living expenses is undetermined and the new version of the International Sanctions Act will address this issue. A working-group is preparing a draft for a new International Sanctions Act. It is expected that the draft Law will be submitted to Parliament before the end of 2008.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**PC**	• Estonia does 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) does not cover funds controlled by a designated person or persons acting on their behalf or at their direction (as it is required by UNSCR 1267 and UNSCR 1373). • Estonia does 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 are aware of the procedures to be followed in order to implement the UNSC Resolutions.

Authorities

2.5 The Financial Intelligence Unit and its functions (R.26, 30 and 32)

2.5.1 Description and analysis

309. The Estonian Financial Intelligence Unit (FIU) is a police-type FIU and was established as a separate division under the Criminal Investigation Department of the Police Board on 1 July 1999. On 1 January 2004 a new version of the AML Act came into force, and the FIU was made an independent structural unit of the Central Criminal Police.

310. The FIU has its own permanent staff and is currently composed of the Head of the FIU, one assistant, one data processing specialist and the employees of 3 subunits (Analysis Unit, Asset Recovery Unit and Supervision Unit). Since the second round evaluation (November 2002), the staffing of the FIU has significantly changed: the total number of staff in November 2002 was 7, of which 6 posts were filled; the total number of staff at the time of the on-site visit (February 2008) was 24 of which 18 posts were filled. While the head and members of analysis and asset recovery units are police officers, employees of supervisory unit are all civil servants (for further details and an organisational chart see below para 349 ff).

311. Though each of the three subunits (Analysis Unit, Asset Recovery Unit and Supervision Unit) has its own specific functions and area of activity, they work in close cooperation due to their common objective. The *Analysis Unit* is responsible for the analysis and dissemination of STRs and CTRs. After its analysis, it forwards the material to the competent investigative bodies. The *Supervision Unit* is responsible for the supervision of activities of the obligated entities. There is

also a specific post of a strategic analyst within the Supervision Unit who is responsible for gathering and analysing statistics, money laundering trends, organising feedback to reporting entities, awareness rising etc. The *Asset Recovery Unit* is a new body not only within the structure of the FIU, but in the Estonian Police as a whole. It comes into play after the analysis of STRs and CTRs: the unit is then responsible for identifying possible assets belonging to criminals and also assists investigators and prosecutors to identify criminal assets. The unit is also a contact point for the foreign asset recovery offices, exchanging information with them and helping them in tracing, identification, seizure and confiscation of assets.

312. The powers and responsibilities of the FIU are described in § 37 of the MLTFPA as follows:

(1) The functions of the Financial Intelligence Unit are:

1) to gather, register, process and analyse information received pursuant to §§ 32 and 33 of this Act. In the course thereof, the significance of the information submitted to the Financial Intelligence Unit for the prevention, identification or investigation of money laundering, criminal offences related thereto and terrorist financing shall be assessed;

2) to inform the persons who submit information to the Financial Intelligence Unit of the use of the information submitted for the purposes specified in clause 1) of this section in order to improve the performance of the notification obligation;

3) tracing criminal proceeds and application of the enforcement powers of the state on the bases and within the scope provided by law;

4) to supervise the activities of obligated persons in complying with this Act, unless otherwise provided by law;

5) information of the public of prevention and identification of money laundering and terrorist financing, analysing the respective statistics, and preparing and publishing an aggregate overview at least once a year;

6) cooperation with obligated persons, investigative bodies and police institutions in the prevention of money laundering and terrorist financing;

7) training obligated persons, investigative bodies, prosecutors and judges in matters related to prevention of money laundering and terrorist financing;

8) organisation of foreign communication and exchange of information pursuant to § 46;

9) exercising supervision over the application of the measures specified in clauses 3 (1) 3) to 5) of the International Sanctions Act, unless otherwise provided by the Act or legislation of the European Union;

10) to conduct proceedings in matters of misdemeanours provided for in this Act.

(2) The Financial Intelligence Units analyses and verifies information about suspicions of money laundering or terrorist financing, taking measures for preservation of property where necessary and immediately forwarding materials to the competent authorities upon detection of elements of a criminal offence.

It becomes obvious from this list that these functions cover all the activities as required by criterion 26.1.

313. The new MLTFPA defines certain misdemeanours where the FIU has the role of a body conducting extra judicial proceedings. These offences are:

- Non-performance of the obligation to register and store data
- Failure to submit mandatory information data in time (according to the new MLTFPA – a delay in the submission of data)
- Failure to apply internal security measures
- Unlawful notification of information submitted to the FIU
- Failure to comply with the identification requirement
- Failure to report suspicion of money laundering or terrorist financing and submission of incorrect information

- Non-performance of registration obligation (while the previous MLTFPA only concerned currency exchange services, the new MLTFPA concerns financial institutions with no supervision, providers of trust fund and company services, providers of alternative means of payment services, pawn shop owners)
- Non-performance of the obligations of a provider of payment services

Guidance on reporting, reporting forms and procedures

314. According to § 33 (2) MLTFPA, the obliged entities have to send their STRs "*orally, in writing or in a format which can be reproduced in writing*". If a report was submitted orally, it shall be submitted the next working day in writing or in a format which can be reproduced in writing. According to § 33 (4) of the new MLTFPA, the format of reporting to be forwarded to the FIU and instructions for the preparation thereof shall be established by a regulation of the Minister of the Interior. The Estonian authorities explained that this has been done (even before the new MLTFPA came into force) with Regulation No. 18 of the Minister of Interior "*Establishment/Approval of Instructions for Filling in Notifications Given to the Financial Intelligence Unit and Forms of Notifications*" which was signed on 11 March 2004. This Regulation contains guidance on the manner of reporting, specification of reporting forms and procedures to be followed when reporting. The Regulation itself and also the report form have been made available on the public website of the Estonian FIU[21]. In January 2008, a new electronic form for reporting was issued. The use of this new form is not mandatory; however, the FIU sent an information letter to the obligated entities suggesting the use of the new format for sending reports. In practice, more than 99% of the STRs are submitted electronically (and digitally signed).

315. In 2006, the officials of the FIU carried out 28 training courses for 1000 people, and in 2007, 29 training sessions for 985 participants. These training courses were mostly, but not exclusively, targeted for persons with reporting obligations. Training concerning the activities of the FIU was provided to auditors and accountants, notaries, real estate agents, police officials, trustees in bankruptcy, bank officials, currency exchange workers and intermediaries of valuable goods. These training courses also covered guidance regarding the manner of reporting, information on the reporting forms to be used, and the procedures that should be followed when reporting.

316. The new MLTFPA also introduced an obligation to report transactions above a certain threshold (for details see below Section 3.7).

317. When a report is registered, the data is entered into the FIU information system and checked on the basis of available databases; each report received in the FIU is analysed with the help of analytical software. If necessary, the FIU asks for further information from domestic or foreign counterparts. "*Upon detection of elements of a criminal offence*" (§ 37 (2) MLTFPA), the material is forwarded to the competent bodies either for starting a criminal investigation or to be used as additional information in an ongoing procedure. The FIU is obliged "*to forward significant information, including information subject to tax and banking secrecy to the prosecutor, the investigative body and the court*" (§ 43 (2) MLTFPA). The investigative body may be – depending on the predicate offence – the Central Criminal Police, a police prefecture, Tax and Customs Board, Security Police, etc. If the result of analysis shows well-founded grounds of money laundering or terrorist financing, the FIU is entitled to suspend the transaction or establish a restriction as regards the use of the account.

318. The Head of the Analysis Unit is responsible for the decision whether a report is sent to archive or for further investigations to another investigative body. It usually takes 1 month for an

[21] http://www.politsei.ee/files/rab/Regulation_No_12.pdf.

analyst to carry out the necessary measures to be able to make a decision on it. However, there is no specific time limit for analysis work and it can also last several months.

319. No STRs should go to another police department or prefecture simply for analysis. In case of a suspicion of *terrorist financing* the contact person of the Security Police Board is informed; the latter is only authorised to have a look into STRs related to terrorist financing. The contact person does not have access to the database of the FIU and can only be provided with the necessary information, but there is no direct access allowed. Such messages are sent by e-mail with a Secure ID, and they can only be opened by the contact person.

320. An analyst usually has 20 cases to deal with at the same time; this does not refer to the number of STRs, but is the number of open files, which can cover more STRs.

321. § 42 of the MLTFPA empowers the FIU to make enquiries to and to receive data from state and local government databases and databases maintained by persons in public law. In practice, the Estonian FIU has direct access to surveillance and other law enforcement information through police information systems (databases) and to various state and local government databases. In particular, the FIU has direct access by its information system RABIS to the following databases:

- Commercial Register,
- Inhabitants Register,
- Register of Real Estate,
- Social Security Register and Vehicle Register, which is merged with the small tonnage register.

Furthermore, the FIU has direct access via Internet to the following registers:

- Buildings Register,
- Cadastral Register,
- Firearms Register,
- Register of Economic Activities,
- to the tax register of the Tax and Customs Board (which includes tax declarations),
- Criminal Procedures Register,
- Court Judgments Register and Supreme Court Register;

Via the police intranet, the FIU has access to:

- Criminal and Administrative Records Register,
- Stolen Documents Register,
- Police Criminal Intelligence Register and
- Schengen Information System.

The FIU has powerful IT-facilities and can link the information of these databases in an impressive way. Furthermore, the FIU can request information from the Tax and Customs Board concerning customs data; the FIU mainly requests cross border cash and goods declarations.

Access to additional information

322. According to § 41 (1) of the MLTFPA, the FIU has the right to request additional information regarding circumstances, transactions or persons related to suspicion of money laundering or terrorist financing if the FIU has reason to believe that any of them is, or could be, in possession of information that is valid or contributes to the work of the FIU. The FIU can ask the FSA, state and local government authorities and the obligated persons for such additional information. It was explained that it usually takes 10 days to get an answer for a request. According to § 41 para 3 MLTFPA, "*the Financial Intelligence Unit has the right to obtain, pursuant to the procedure provided by legislation, relevant information, including information collected by surveillance, from any surveillance agency*" – this authority is limited to requests related to prevent money laundering only (and not terrorist financing). The Estonian authorities explained that the reason for this restriction is that the Security Police Board has the exclusive authority for investigating

terrorist related (and also terrorist financing) crimes (§ 6 para 2^1 and § 31 Security Authorities Act). In this respect it is worth to refer to § 45 para 1 MLTFPA which stipulates that the FIU and the Security Police Board shall "*cooperate in investigation of transactions suspected of terrorist financing through mutual official assistance and exchange of information*".

323. The evaluators were provided with the following statistics showing the number of additional information requests done by the FIU:

	Credit institutions	Other legal persons	Individuals
2004	441	34	2
2005	784	38	29
2006	1320	53	13
2007	1356	72	1

Disseminating financial information

324. According to § 43 (2) and (3) of the new MLTFPA, the Financial Intelligence Unit is obligated to forward significant information, including information subject to tax and banking secrecy to the prosecutor, the investigative body and the court in order to prevent or identify money laundering or terrorist financing or criminal offences related thereto and in order to facilitate the pre-trial investigation thereof.

325. The Head of the FIU is authorised to make a decision about the dissemination of an STR and also where to send it (Central Criminal Police, police prefecture, etc.).

326. There is no need for the FIU to conclude any cooperation agreement to be able to exchange or obtain the necessary information. However, the FIU found it useful to have a cooperation agreement with the customs authorities on related tax crime. Customs authorities appointed a contact person who can be contacted by the FIU to get the necessary information.

327. According to the opinion of representatives of the FIU, the FIU is not allowed to send the STR itself for dissemination and is only entitled to provide a statement of the result of analysis containing all details of the suspicious transaction report (including bank secrecy, etc.) without any information on the name of the person who sent the report. Though this is not explicitly regulated in the MLTFPA, one can defer this from § 43 (5) which stipulates**: "***The Financial Intelligence Unit shall not disclose the personal data of the person performing the notification obligation or a member or employee of the directing body of the obligated person.***"** Thus, one can conclude that it would not be allowed to disseminate an STR containing such information.

328. According to § 43 (3) MLTFPA, the information registered by the FIU can only be used for the purposes of the fight against money laundering, terrorist financing and criminal offences related thereto[22].

Reporting

329. The Estonian FIU keeps records of STRs for 10 years and filled in the following tables concerning the number of STRs received by the FIU and the outcome of these reports. The table for 2008 contains also the number of CTRs received (an obligation which was introduced with the new MLTFPA in 2008).

[22] In the English version of the MLTFPA with which the evaluation team was provided, "terrorist financing" was not included in § 43 (3) MLTFPA. However, the Estonian authorities explained that this was an omission due to a translation error (which could be verified by the evaluation team in comparing it with the original Estonian version of the MLTFPA).

2003							
Statistical Information on reports received by the FIU				Judicial proceedings			
Monitoring entities	reports about suspicious transactions[23]	cases opened by FIU	notifications to law enforcement/ prosecutors	indictments		convictions	
	ML/FT	ML/FT	ML/FT	ML	FT	ML	FT
commercial banks	1147	1293	6	0	0	0	0
insurance companies	0						
Notaries	1						
Currency exchange	1						
broker companies	0						
securities' registrars	0						
lawyers	0						
accountants/auditors	0						
company service providers	0						
others (foreign FIUs, Ministries, Police, FSA, other government agencies, others)	144						
Total	**1293**						

2004							
Statistical Information on reports received by the FIU				Judicial proceedings			
Monitoring entities	reports about suspicious transactions[23]	cases opened by FIU	notifications to law enforcement/ prosecutors	indictments		convictions	
	ML/FT	ML/FT	ML/FT	ML	FT	ML	FT
commercial banks	1169	1430	29	0	0	0	0
insurance companies	0						
Notaries	14						
Currency exchange	0						
broker companies	0						
securities' registrars	0						
lawyers	0						
accountants/auditors	0						
company service providers	0						
Other financial institutions (leasing companies etc.)	6						
Savings and loan associations	0						
organisers of gambling and lotteries	12						
others (foreign FIUs, Ministries, Police, other government agencies, others)	229						
Total	**1430**						

[23] Estonian authorities confirmed that one STR may contain several transactions.

2005							
Statistical Information on reports received by the FIU				**Judicial proceedings**			
Monitoring entities	**reports about suspicious transactions[23]**	**cases opened by FIU**	**notifications to law enforcement/ prosecutors**	**indictments**		**convictions**	
	ML/FT	**ML/FT**	**ML/FT**	**ML**	**FT**	**ML**	**FT**
commercial banks	1213	1697	64 (involving 160 STRs)	1	0	1	0
insurance companies	0						
Notaries	10						
Currency exchange	15						
broker companies	0						
securities' registrars	0						
lawyers	2						
accountants/auditors	0						
company service providers	0						
Savings and loan associations	0						
Other financial institutions (leasing companies etc.)	3						
providers of cash transfer services	111						
organisers of gambling and lotteries	36						
Persons who carry out or act as intermediaries in transactions with real estate	1						
others (foreign FIUs, Estonian FIU, FSA, Ministries, Police, other government agencies, others)	306						
Total	**1697**						

2006							
Statistical Information on reports received by the FIU				**Judicial proceedings**			
Monitoring entities	**reports about suspicious transactions[23]**	**cases opened by FIU**	**notifications to law enforcement/ prosecutors**	**indictments**		**convictions**	
	ML/FT	**ML/FT**	**ML/FT**	**ML**	**FT**	**ML**	**FT**
commercial banks	1589	2601	120 (involving 358 STRs)	1	0	1	0
insurance companies	0						
Notaries	47						
Currency exchange	32						
broker companies	0						
securities' registrars	0						
lawyers	2						
accountants/auditors	0						
company service providers	0						
Savings and loan associations	0						
Other financial institutions (leasing companies etc.)	90						
providers of cash transfer services	419						
organisers of gambling and lotteries	90						
intermediaries of high-value goods	3						
others (foreign FIUs, Estonian FIU, Ministries, Police, other government agencies, others)	329						
Total	**2601**						

2007										
Statistical Information on reports received by the FIU							**Judicial proceedings**			
Monitoring entities	**reports about suspicious transactions[23]**		**cases opened by FIU**		**notifications to law enforcement/ prosecutors**		**indictments**		**convictions**	
	ML	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**
commercial banks	2206	Non available.	5199	73	196 (involving 397 STR)		8	0	0	0
insurance companies	0									
Notaries	96									
Currency exchange	222									
broker companies	0									
securities' registrars	0									
lawyers	6									
accountants/auditors	1									
company service providers	0									
Other financial institutions (leasing companies etc.)	94									
providers of cash transfer services	1528									
organisers of gambling and lotteries	566									
Persons who carry out or act as intermediaries in transactions with real estate	1									
intermediaries of high-value goods	112									
foreign FIU	127									
Tax and Customs Board	54									
Ministries, other public sector institutions	1									
Estonian FIU	186									
police	45									
others	27									
Total	**5199**	**73**								

2008 (1.1. – 31.3)											
Statistical Information on reports received by the FIU								Judicial proceedings			
Monitoring entities, e.g.	reports about transactions above threshold (legal obligation since 28.1.)	reports about suspicious transactions[23]		cases opened by FIU		notifications to law enforcement/ prosecutors		indictments		convictions	
		ML	FT	ML	FT	ML	FT	ML	FT	ML	FT
others	**0**	**3**	**0**								
financial institutions	**626**	**22**	**0**								
credit institutions	**5**	**544**	**7**								
other private enterprises	**104**	**187**	**351**								
…postal offices	0	132	351								
…hotels	0	0	0								
…traders	12	18	0								
…real estate companies	1	0	0								
…others	0	6	0								
…pawnhouses	0	1	0								
…gambling organisations	4	30	0								
professionals	**30**	**19**	**0**	448	0	37	0	0	0	0	0
…lawyers	0	2	0								
…auditors	0	1	0								
…bailiffs	0	0	0								
…other legal advisors	0	0	0								
…notaries public	30	16	0								
state institutions	**1**	**32**	**0**								
…FIU	1	2	0								
…ESA	0	2	0								
…Tax and Customs Board	0	10	0								
…Police	0	18	0								
foreign institutions	**0**	**42**	**0**								
Total	**766**	**849**	**35824**								

330. The Estonian authorities explained that the FIU had, until 2008, no system for automatic case management procedures. Therefore, the FIU had to analyse each case received which means that the number of cases opened by the FIU is the same as the number of STRs received by the FIU. Since the implementation of the new information system "RABIS" in January 2008, the FIU has a case management system which does an automatic analysis and it is no longer necessary for the staff of the FIU to manually analyse all reports received (in all cases only the IT-based analysis is made and if there is no suspicious activity detected, the report is archived until new information is received).

[24] The Estonian authorities explained that the high number of STRs with suspicion of terrorist financing is caused by the fact that at the beginning of 2008 the FIU sent to the obligated persons a list of countries with a higher risk of terrorist financing (a list which was created by the SPB) and asked to report about each transaction sent to or from such a country.

331. Moreover, until the introduction of the new system "RABIS", the FIU did not keep statistics which would allow a distinction between money laundering and terrorist financing (instead all reports are only under the category of "suspicious transactions").

332. In analysing this data, it can be emphasised that in 2007 the FIU received 5272 STRs which is more than twice than in 2006 (2601 STRs). Comparing this figure with the year 2005, the number of STRs has increased more than three times. The Estonian authorities explained this increase with the higher awareness of the obligated entities which was considered as a result of training and monitoring inspections carried out by the officials of the FIU. The increase of received STRs can be seen in the table below:

Monitoring entities	**2003**	**2004**	**2005**	**2006**	**2007**
Banks	1147	1169	1213	1589	2206
Providers of currency exchange services	1	0	15	32	222
Providers of cash transfer services	0	0	111	419	1528
Organisers of gambling or lotteries	0	12	36	90	566
Persons who carry out or act as intermediaries in transactions with real estate	0	0	1	0	1
Intermediaries of high-value goods	0	0	0	3	112
Accountants, Auditors	0	0	0	0	1
Lawyers	0	0	2	2	6
Notaries	1	14	10	47	96
Savings and loan associations	0	0	0	0	0
Other financial institutions (leasing companies etc.)	0	6	3	90	94
Other*	22	31	23	103	214
Foreign FIU	78	90	81	106	127
Customs Service	21	70	129	73	54
Ministry of Foreign Affairs	5	13	8	0	0
Police	18	25	29	47	45
FIU**	na	na	31	na	0
Other government agency	na	na	5	na	0
Total	**1293**	**1430**	**1697**	**2601**	**5272**

* individuals, representatives of businesses belong to this category, who are not listed in the MLTFPA

** number of STRs, registered and analysed by the own initiative of the FIU

Operational independence

333. § 36 of the new MLTFPA states that the Estonian FIU is an independent structural unit of the Central Criminal Police. The Head of the Financial Intelligence Unit is appointed by the National Police Commissioner of the Police Board on the proposal of the Police Chief of the Central Criminal Police for five years. After the five-year period the head can be re-appointed again.

334. Although part of the Central Criminal Police, the FIU is operationally independent in its decisions and free from any undue influence or interference.

335. The only risk to its operational independence could be that the FIU has no own budget and depends on the Central Criminal Police when it comes to budgetary issues. The Police Board provides the Financial Intelligence Unit with the funds necessary for the performance of the functions provided by law. This means that the FIU as a part of the Central Criminal Police has no independent budget. It is dependent on the Central Criminal Police for budgetary issues such as hiring staff, salaries and trips to foreign countries. The FIU is functioning from the budget of the Central Criminal Police and there is a certain amount separated for different allowances such as gasoline, phone calls, international cooperation and trips abroad. Representatives of the FIU were not satisfied with the amount of funds provided for its functioning by the Central Criminal Police before, but according to certain changes for the last two years, the FIU has been provided with additional funds in order to obtain several IT staff and other technical resources necessary to fulfil its obligations effectively. The salaries of staff have also been raised. The FIU may have a certain influence on the budget as it can make a yearly calculation of expenses or give some explanations of the use and purposes of the necessary amount to the chief commissioner of the Central Criminal Police, but does not have any influence on the final decision.

336. The only provision addressing budgetary issues of the FIU can be found in § 36 (3) MLTFPA which stipulates that "*the Police Board provides the Financial Intelligence Unit with sufficient funds for performance of the functions provided by law*". As it is nowhere determined what has to be understood under "*sufficient funds*" there is a potential risk of budgetary constraints. Though representatives of the FIU are of the opinion that this was not a problem in the past, in the evaluators view a separate budget would definitely strengthen the independence of the FIU.

Protection of Information

337. The evaluators were given the opportunity to visit the premises of the FIU during the on-site visit to have a general overview about the resources of data protection and the ability to protect sensitive information. Several measures have been adopted for the objective of data protection:
- the Unit is located on a separate floor of in one of the buildings of the Central Criminal Police,
- the electronic locks of doors can only be opened with cards of the employees,
- entrance to the FIU premises is guarded by video cameras and an alarm system,
- all computers in the FIU are protected by firewalls and are accessible only by using personal passwords,
- the database is in an autonomous computer, which does not have any physical connection with other computers,
- reference files in paper form are in lockable metal cupboards.

338. The circumstances under which the FIU is entitled to disseminate information has been described above (para 317).

Public Reports

339. § 37 (1) 5) MLTFPA obliges the FIU to inform the public of the prevention and identification of money laundering and terrorist financing, to analyse the respective statistics, and to prepare and publish an aggregate overview at least once a year. Every year the Estonian FIU releases its Annual Report (starting in 2005). The evaluators were provided with the annual report of 2007, which had been published by the beginning of the on-site visit. The evaluators were also provided with the annual report for 2006 and a summary report which gives an overview on prevention of money laundering in Estonia from 1999 to 2005. Further to information on the activities of the Unit, the annual report contains statistics, trends, sanitised cases and typologies. The annual reports have been made publicly available on the FIU's public web-page[25].

[25] http://www.politsei.ee/?id=1627.

Egmont Group

340. The Estonian FIU has been a member of the Egmont Group and exchanges information with other FIU's since June 2000. The Estonian FIU actively participates in the operational working group of Egmont and is an initiator of the E-money laundering sub-working group together with FINCEN.

341. In 2007 the FIU received 147 enquiries and sent 45 enquiries to 14 countries. The number of incoming enquiries has increased year by year, the number of outgoing inquiries was less.

	2004	2005	2006	2007
Incoming enquiries	91	81	111	147
Outgoing enquiries	30	48	64	45

342. The biggest number of enquiries sent abroad goes to Russia and Latvia, and the biggest numbers of enquiries which come to the FIU are from Russia, Latvia, Finland and Ukraine.

343. All the analysts (5 persons) and heads of units (3) are in charge of information exchange through the Egmont Secure Web.

Information exchange with other FIUs

344. There are no restrictions on exchanging information with other FIUs. The Estonian FIU can provide other FIUs with any data and information, including banking and also police intelligence information. Though the FIU can exchange information with other FIUs even without having a Memorandum of Understanding (MoU) in place, it has signed a number of MoUs.

Country	Year of signature
Lithuania	1999
Latvia	2000
Belgium	2000
Czech Republic	2001
Poland	2001
Russia	2003
Israel	2003
Ukraine	2003
Italy	2003
Slovenia	2004
Australia	2004
Netherlands Antilles	2004
Albania	2004
Georgia	2004
Thailand	2004
Rumenia	2005
Moldova	2005
Ireland	2006

345. As a police-type FIU, the Estonian FIU can also cooperate directly with Europol, Interpol and it uses this opportunity in some cases, but not on a regular basis.

346. § 37 (1) 8) of the new MLTFPA states that one of the core functions of the FIU is the organisation of foreign communication and the exchange of information pursuant to § 46 of the MLTFPA. The same provision was stated in the previous MLTFPA. According to § 46 the FIU has the right to exchange information and enter into cooperation agreements with foreign agencies which perform the functions of a financial intelligence unit.

Other issues

347. Besides its obligations already described above, it is worth noting that the FIU is also responsible for supervising the compliance of the obligated entities with the MLTFPA. Since 2005 the FIU has performed random on-site inspections. There are 4 people in the Supervisory Unit to carry out the necessary tasks. Usually 2 people go on-site. Inspections might be planned, but they may be also done *ad hoc* based on risk analysis or received reports. In the first two years (2005, 2006) the number of on-site inspections was 61 and 62; in 2007 the number increased to 205. Based on the infringements discovered, misdemeanour procedures were initiated in 5 cases. In other cases the FIU informed the entity about its findings and the entity was given 1 month to improve its deficiencies. In case of failure to do so, the entity will receive an administrative punishment. For the second misdemeanour a criminal investigation is initiated. Until the time of the on-site visit, the highest fine imposed so far was 10 000 EEK in the case of legal persons and 1 000 EEK in the case of a natural person.

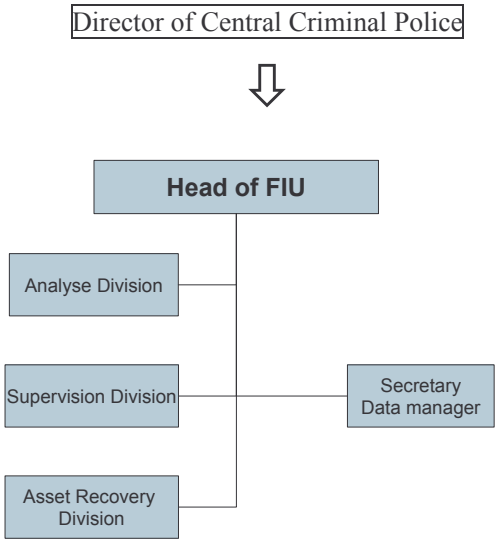
348. The FIU is also involved in legislative activities. It participated in the process of creating the new version of the MLTFPA.

Recommendation 30

Structure, staff, technical and other resources for the FIU

349. § 36 of the new MLTFPA states that the Financial Intelligence Unit is an independent structural unit of the Central Criminal Police. The Head of the Financial Intelligence Unit is appointed by the National Police Commissioner of the Police Board on the proposal of the Police Chief of the Central Criminal Police for five years.

350. The current structure of the FIU is:



351. As noted, the FIU has its own permanent staff which has increased from 7 (November 2002) to 24 (December 2007); however, at the time of the on-site visit, only 18 of the 24 positions had been filled[26]. The FIU is currently structured as follows: Head of the FIU, one assistant, one data processing specialist plus 3 units which have the following staff:

Analysis Unit: 5,
Asset Recovery Unit: 4,
Supervision Unit: 6.

352. The budgetary situation of the FIU and the concerns of the evaluation team regarding to the operational independence of the FIU because of the lack of a clear provision determining the budget of the FIU has been explained above (para 335 f).

Professional standards (confidentiality, integrity and other skills)

353. Concerning the process of recruitment, the Head of the FIU makes a proposal which has then to be approved by human resources of the Central Criminal Police. As the Estonian FIU is an independent structural police unit within the Central Criminal Police, for the staff of the FIU the same professional standards (confidentiality, integrity and other skills) as for other police officials apply (see below para 410 ff). In addition, § 44 of the new MLTFPA regulates the requirements for officials of the Financial Intelligence Unit as follows:

> *(1) Only a person with impeccable reputation, the required experience and abilities, and high moral qualities may be appointed as an official of the Financial Intelligence Unit.*
> *(2) 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.*

354. To be recruited the candidates have to undergo the recruitment procedure which usually contains an interview with heads of units and other testing. There is also a written exam to check the language skills of the candidate. The evaluators were informed that the background of each candidate is checked thoroughly. There are different kinds of security checking, criminal record and various other databases. It usually takes one month period to go through all the checking procedure. When a new head is appointed, he is checked by the police internal control service.

355. The current staff of the FIU has sufficient skills to deal with their obligations: all analysts have police background, there is staff from customs with financial and tax backgrounds, members of the asset recovery unit have police and financial backgrounds. There are also 2 legal specialists within the FIU. The IT system is centralised in the Police Board, so there is no special unit or an IT expert working for the FIU.

356. All information held by the FIU is protected and disseminated according to the law. § 43 (1) to (5), § 44 (2) and § 45 (3) MLTFPA contain confidentiality requirements concerning the unit, its officers and agents, regardless of whether they still work for the unit. § 43 (1) of the new MLTFPA states that "o*nly officials of the FIU shall have access to and the right to process information in the FIU database"*. The FIU has different level of access to its database. All staff can see all the STRs, but not all are allowed to make any changes or add data or information in it. There are 4 levels of access: Level 1 – just for inserting STRs, Level 2 - analyst level, Level 3 - decision making level for chiefs, Level 4 – administrative/management level to change names of users, rights, structure. Theoretically officials of the FIU do not need to sign a confidentiality

[26] In November 2008, 20 of the 24 positions have been filled.

agreement as all the protective measures they have to comply are stated in the MLTFPA and there is no need for additional requirements. However, there is a kind of agreement they sign when recruited.

357. According to § 43 (3), the information registered in the Financial Intelligence Unit shall only be forwarded to the authority engaged in the pre-trial procedure, the prosecutor or a court in connection with criminal proceedings on the basis of a written request of the preliminary investigation authority, the Prosecutor's Office or the court or on the initiative of the Financial Intelligence Unit, if the information is significant for the prevention, establishment or investigation of money laundering or a criminal offence related thereto.

Training

358. The staff of the FIU is regularly provided with adequate and relevant training for combating money laundering and terrorist financing at both domestic and international level. There are three kind of training:

1) internal training of the FIU which is scheduled each year,
2) external training on a domestic level (together with judiciary, Police, etc.)
3) private sector

359. In 2006, officials of the FIU participated in 32 training courses, out of which 14 courses were held abroad. There were several internal training sessions held by heads of different divisions for FIU staff. In 2007, officials of the FIU participated again in 32 training courses.

2.5.2 Recommendations and comments

360. The Estonian FIU meets the requirements of Recommendation 26 and appears to be a generally effective FIU.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors underlying rating
R.26	**C**	

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27 and 28)

2.6.1 Description and analysis

Recommendation 27

361. The investigation and prosecution of offences and confiscation and freezing of assets is regulated by the Code of Criminal Procedure (CCP), the Penal Code (PC), the Surveillance Act, the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) and Regulation No 193 of 19 July 2007 of the Government of the Republic of Estonia.

362. In accordance with the CCP, preliminary proceedings in money laundering cases shall be conducted by the Police Board, the Central Criminal Police and the Security Police Board. Within the limits of their competence, the Tax and Customs Board, the Border Guard Board, the

Competition Board and the Headquarters of the Defence Forces act also as investigative bodies. In cases when a predicate offence falls within their competence, they also conduct investigations of related money laundering. If necessary, the Prosecutor's Office has the authority to entrust another investigative body with the investigations if this seems more appropriate (i.e. it may alter investigative jurisdiction in a particular criminal matter by an order); this has often been the case with money laundering cases related to tax offences. However, most cases are investigated by the Central Criminal Police, the four Police Prefectures and the Tax and Customs Board. These investigative bodies have all rights to investigate properly all kinds of crimes related to money laundering and financing of terrorism. The sanction of the mentioned crimes gives the possibility of doing intelligence work as well, also controlled delivery, undercover operations etc.

363. The **Estonian Police** is a body established under the competence of the Ministry of Internal Affairs and is governed by the Police Board. The Head of the Police is the National Police Commissioner who is appointed by the government for a 5-year term.

364. The Estonian Police Board is divided into the Central Criminal Police, the Personal Protection and Law Enforcement Police plus 4 territorial police prefectures:

- Northern Prefecture (Pohja)
- Southern Prefecture (Louna)
- Eastern Prefecture (Ida)
- Western Prefecture (Laane)

365. Each police prefecture has 3 functional departments:

- Law-enforcement department
- Service department
- Crime department

366. The tasks of the **Police Board** are: to manage and develop police activities, to analyse and control the activities of police agencies and to coordinate cooperation amongst them, to develop trends and activity plans of the police, to develop cooperation with other national authorities, local government units, public organisations and also with other countries and international law-enforcement bodies, to coordinate financial activities, to develop information and communication systems.

367. The Criminal Department of the Police Board deals with administrative and coordination work on money laundering and criminal assets issues. The Department started its activity on 1 November 2007. It consists of 7 people plus head of department who is a civil servant (former prosecutor). All staff deal with coordination work but in different areas: 1 person in the field of money laundering, 1 person with intelligence, 1 person with the database, 1 with international cooperation, 2 people with forensic issues, 1 with human trafficking and organised crime. The department has access to the whole police database for all kinds of data in order to be able to prepare the statistical data for the police.

368. The **Central Criminal Police** gathers and analyses information regarding police activities. It provides guidelines for the harmonisation of police activities in the area of the criminal police. The main investigative directions of the Central Criminal Police are international organised crime (for domestic organised crime mainly the territorial Police Prefectures are responsible), corruption and serious economic offences, money-laundering, drug offences and information technology crimes. The Central Criminal Police coordinates cooperation with other national and international law-enforcement agencies and international organisations, carries out witness protection and performs surveillance activities in the whole country to prevent financing of terrorism and money-laundering.

369. The Central Criminal Police consists of the following Departments:

- Investigation Department
- Operational Department
- Criminal Intelligence Department
- Financial Intelligence Unit
- Development and Analysis Bureau
- Supporting Bureaus

370. The Investigation Department consists of 4 units responsible for drug crime, economic crime, organised crime and witness protection. The Economic Crimes Unit investigates money laundering cases; however, it has to be noted that this power has been granted to all police forces (including 4 Police Prefectures). Money laundering cases are investigated according to the competence of the police prefecture, which depends for instance on the residence of the offender. There were 2 money laundering cases in the Central Criminal Police in 2007 and as a result 10 persons were indicted. The predicate offence was IT crime (internet fraud/phishing case).

371. A criminal investigator has usually to deal with 2-3 active cases (criminal files) at the same time.

372. The Central Criminal Police has a total number of 262 officers, officials and auxiliary staff members.

373. **Prosecutors' Offices** are responsible for ensuring that money laundering and terrorist financing offences are properly investigated and are competent to:
- perform procedural acts when necessary;
- be present at the performance of procedural acts and intervene in the course thereof;
- terminate criminal proceedings;
- demand that the material of a criminal file and other materials be submitted for examination and verification;
- issue orders to investigative bodies;
- annul and amend orders of investigative bodies;
- alter the investigative jurisdiction over a criminal matter (see above para 362);
- demand that an official of an investigative body submits oral or written explanations concerning the circumstances relating to a proceeding etc.

374. The total number of prosecutors in Estonia is 198. In the Prosecutor's Office are also prosecutors who are specialised in economic crimes, including money laundering offences. The number of prosecutors specialised in financial crimes, including money laundering is as follows (the number of all prosecutors in the relevant district are mentioned in brackets):

▪ Prosecutors' Office General	3 (27)
▪ Northern District Prosecutors' Office	12 (79)
▪ Southern District Prosecutors' Office	7 (38)
▪ Western District Prosecutors' Office	3 (24)
▪ Viru (Eastern) District Prosecutors' Office	1 (30)

The number of specialised prosecutors to the offices mentioned above is based on the number of criminal cases with which the particular office has to deal.

375. When a criminal proceeding is ongoing and it becomes evident during the investigation that a money laundering offence has also taken place, the prosecutor who is responsible for the investigation of the predicate offence shall also be responsible for investigation of the money laundering offence.

376. The investigation of terrorist related cases (PC §§ 231-237³, based on the Government of the Republic of Estonia Regulation No. 193 of 19 July 2007 § 2 (1)) falls into the competence of the **Security Police Board (SPB)**. The SPB gained the status of an independent institution on 18 June

1993. With the Security Authorities Act, which came into force on 1 March 2001, the SPB was converted from being a police authority to a security authority. The investigative competence of the SPB covers offences against the Republic of Estonia or international security; terrorism; offences against humanity and peace; war crimes; illegal handling of explosive material and explosive devices prohibited for civilian purposes and organisation of explosions with these; some office crimes committed by higher state officials; illicit traffic, if the object of the crime was radioactive substance, explosive material, strategic goods, firearm or ammunition or if the crime was committed by an official using his/her office; offences related to disclosure of state secrets; incitement to social hatred.

377. The SPB as a security authority has a firm role in counter-terrorism activities and it is first and foremost engaged in collecting information, conducting security and surveillance operations, assessing hazards and information, pre-trial investigation and developing national and international cooperation. One of the main goals of the SPB is to prevent terrorism in Estonia and contribute to international counter-terrorism activities. Activities of the SPB at prevention of terrorism include *inter alia* the following:

- collection of information, in order to detect possible interest and activities of terrorist organisations, targeted against the Republic of Estonia;
- suppression of financing of terrorism;
- suppression of distribution of weapons of mass destruction;
- international cooperation.

378. According to the information provided by representatives of the SPB, there were no acting terrorist groups in Estonia, and no supporters of financiers of international terrorist organisations. However, it was mentioned by the authority, that some fundamentalist Islamic organisations are interested in making contacts in Estonia and its neighbouring countries.

379. The SPB does not produce a separate list of terrorists or terrorist organisations, it uses mainly the consolidated list of the European Union and the UN. The Analytical Department regularly updates it on a monthly basis. The Ministry of Foreign Affairs has to inform the SPB if the list is updated.

380. The SPB has cooperated with the FIU on a daily basis since 2005. A contact person for the communication between the SPB and the FIU was appointed by the Director General of the SPB. The SPB sends the above mentioned list to the FIU or informs it on the update. Some information also goes through Europol or the Interpol system and the Central Criminal Police. The FIU is the agency with which the SPB has the closest cooperation. However, access to the FIU database is not direct, it has to be requested via the contact person. The information can be obtained even in a few minutes.

381. The Estonian **Tax and Customs Board (TCB)** deals *inter alia* with tax and customs duties, implementation of the tax and customs arrangements based on the national tax and customs policy, ensuring compliance with tax legislation, customs regulations, permits for gambling and for organisers of lotteries, supervision of gambling and the activities of organisers of lotteries. It is divided in various divisions. Concerning AML/CFT issues, the most relevant one is the Enforcement and Investigation Division which consists of:

- Intelligence Department
- Audit Department
- Customs Control Department and
- Investigation Department.

382. The *Intelligence Department* analyses information received from other authorities and foreign countries. There is a special agreement in place between this department and the FIU on information exchange concerning money laundering. This agreement was concluded in August

2007. The department also conducts an information exchange on the international level, and analyses cross border cash declarations, which are exchanged with the FIU. The *Customs control Department* coordinates, organises and analyses the work of customs control, including cash control and different restrictions. The *Investigation Department* of the Tax and Customs Board as well as the structural unit of the Tax and Customs Board engaged in pre-trial procedure is an independent unit, which reports directly to the Director General of the Tax and Customs Board and his/her Deputy.

383. Money laundering cases are investigated by the *Investigation Department*. Money laundering as a crime *per se* does not belong to the competence of the TCB but in the case of a tax offence the investigation is carried out by customs. Should TCB discover that the crime is drug related, the case is forwarded to the police for investigation. In the case of the non declaration of cash at the border, the investigation falls into the competence of customs. Nonetheless, the prosecutor can make an *ad hoc* decision which authority will be the designated body to investigate a case. Representatives from the Prosecution service told the evaluation team that they were satisfied with the quality of money laundering investigations done by the TCB.

384. There is a cooperation agreement in place between the FIU and the TCB since August 2007, but this cooperation is based only in "case of need" (see above para 382). While representatives of the FIU and representatives of the Tax Department of the TCB meet weekly, there are less frequent contacts between the FIU and customs representatives of the TCB. Representatives from the TCB explained that they would be interested in more closer and more regular cooperation with the FIU. The FIU has direct access to the tax register of the Tax and Customs Board (which includes tax declarations), but it does not have direct access to the customs database (customs related data can be reached only upon request).

385. To search persons or premises, to seize transaction records and other data related to an account, an order from the prosecutor's office is needed. It takes usually a week to get an order, but if urgent it can be done within the same day. Further details on seizing have been described above (para 234 ff). In the context of criterion 27.2 it is worth mentioning here that the prosecutor has the discretion to postpone or waive arrests in money laundering cases in order to gather evidence and identify suspects. According to § 40 MLTFPA "*in the event of suspicion of money laundering or terrorist financing, the Financial Intelligence Unit may issue a precept to suspend a transaction or to impose restrictions on the disposal of an account or other property constituting the object of the transaction for up to thirty days as of the delivery of the precept*". The FIU forwards information about suspicion of terrorist financing to the SPB. If the SBP initiates a criminal procedure, the property will be seized according to § 142 (1) CCP.

Additional elements

386. The CCP provides for the following special investigative techniques for all offences which are punishable with a minimum term of imprisonment of 3 or more years, and thus also in money laundering, terrorist financing and a number of predicate crime cases:

§ 115. Covert surveillance and covert examination and replacement of object
§ 116. Covert examination of postal or telegraphic items
§ 117. Collection of information concerning messages transmitted through commonly used technical communication channels
§ 118. Wire tapping or covert observation of information transmitted through technical communication channels or other information
§ 119. Staging of a criminal offence
§ 120. Police agent (i.e. "undercover agent").

387. The surveillance activities are also used in practice for money laundering offences. For money laundering investigations, wire tapping is the most common technique.

388. In order to use special investigative techniques, it is necessary to get authorisation from the prosecutor's office. In the case of wire tapping, authorisation is given by the preliminary investigation judge. An authorisation can be given in 1 day or sometimes even on the same day. During night time, the authorisation could be given by the director of the security police, but it needs to be approved by a judge the next day. The authorisation is usually done for 30 days, which can be extended for another 30 days.

389. Also the Tax and Customs Board uses special investigative techniques when conducting investigations. The TCB may use all the special investigative techniques as described above (para 386) autonomously; but when it comes to wire tapping it requests assistance from the Central Criminal Police as it does not have the necessary facilities for these measures.

390. Reference should also be made here to the *Asset Recovery Unit* within the FIU which is responsible for identifying possible assets belonging to criminals and also assists investigators and prosecutors to identify criminal assets (for further details see above para 311).

391. The evaluators were informed that both the Estonian Police and the FIU have experience in cooperative investigations with the appropriate competent authorities, including special investigative techniques. Employees of the FIU have participated in operations of the Police (interrogations and searches of premises) as experts. Furthermore, staff of the FIU have participated in the staging of crimes (*agent provocateur*). The Estonian authorities emphasised that in all these cases the criminals were convicted later. There are approximately 3-5 cooperative investigations each year.

392. The SPB also cooperates with partner services of foreign countries, in order to collect information about potential terrorists or persons related to them, who may arrive in Estonia.

393. In 2007, the Estonian FIU employed a strategic analyst who regularly reviews money laundering and terrorist financing trends, methods and techniques. These findings are published in the FIU's annual report (as of 2007). The annual report is made publicly available through the FIU public website. Additionally, the Estonian FIU presents the findings on money laundering and terrorist financing trends, methods and techniques regularly in training sessions organised for law enforcement authorities and reporting bodies. Moreover, those findings are reported annually to the Money Laundering and Terrorist Financing Prevention Committee where all competent authorities are represented.

Recommendation 28

394. § 26 (3) MLTFPA prescribes that the obligated persons under the Act have to preserve the relevant identification documents to be able "*for an exhaustive and immediate reply to enquiries received from the Financial Intelligence Unit or other investigative bodies or a court pursuant to legislation*". Failure to do so can be sanctioned with a fine up to 18 000 EEK for a natural person and up to 500 000 EEK for a legal person (§ 58 MLTFPA). § 41 (4) MLTFPA entitles the FIU also "*to receive from third parties information for identification of circumstances which are of relevance in the prevention of money laundering or terrorist financing, including to receive accounting documents on any data medium from a third party whose connection to the investigated transactions became evident in the course of the inspection or analysis*".

395. Furthermore, the Code of Criminal Procedure also contains a number of provisions addressing the requirements of criterion 28.1. The competent authorities responsible for conducting investigations of money laundering and financing of terrorism and other underlying predicate offences are authorised to inspect *inter alia* documents, any other object or physical evidence, and in the case of physical examination, also the person as well as postal or telegraphic items (§ 83 CCP).

396. For the prosecution service and investigative bodies, § 215 (1) CCP provides a general "*obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices*". It stipulates 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*". Furthermore, the Estonian authorities referred to several provisions of the CCP which cover a number of the elements of criterion 28.1 and can be enforced via the regime of § 215 CCP:

- § 83 Objective of inspection and objects of inspection
- § 86 Inspection of document, other object or physical evidence
- § 89 Seizure and examination of postal or telegraphic items
- § 91 Search ("*The objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, property to be seized for the purposes of compensation for damage caused by a criminal offence or of confiscation, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area*")
- § 123 Document
- § 124 Physical evidence
- § 125 Storage of physical evidence
- § 126 Measures applicable to physical evidence and confiscated property

The other elements of criterion 28.1 can be enforced via the regime of § 215 CCP in conjunction with provisions of other sectoral laws: e.g. the Credit Institutions Act (§ 88 (5) 2) – disclosure of facts related to banking secrecy).

Power to take witness statements

397. The witnesses' obligation to give testimony both in pre-trial procedure and court procedure arises from § 66 (3) CCP: "*A witness shall give truthful testimony unless there are lawful grounds specified in §§ 71–73 of this Code for refusal to give testimony*". § 468 CCP also provides the possibility of hearing witnesses via video-conference or telephone.

398. §§ 71 – 73 CCP provide the only grounds for refusing to give testimony. This list covers the usual reasons under which witnesses are released from their testimony obligations (close relationship to the suspect or accused; counsels and notaries, health care professionals, protection of a state secret etc.). The unlawful refusal to give testimony is punishable based on Art 318 PC.

399. The described general provisions concerning the powers to take witness statements apply also for investigations and prosecutions related to money laundering, terrorist financing and other underlying predicate offences. Depending on the "*gravity of a criminal offence or the exceptional circumstances relating thereto*", § 67 CCP allows the use of certain safety measures for witnesses (fictitious name, using voice distortion equipment, long distance hearing etc.). The Estonian authorities explained that these measures may also applied in proceedings concerning money laundering, terrorist financing and other underlying predicate offences.

Recommendation 30

Law enforcement and prosecution

400. The Estonian **Police** appears to be modern equipped: each employee has the opportunity of using a computer and the internet; each police agency has also an internal web page for providing its employees with necessary organisational information. However, representatives of the police were of the opinion that the Police do not have enough resources (human and technical) to deal satisfactorily with economic crimes (though the rate of public trust in the Police was 80 % in 2008)

401. The Estonian **Prosecutor's Office** has two levels: the Public Prosecutor's Office/superior prosecutor's office and four District Prosecutor's Offices (Northern District Prosecutor's Office, Southern District Prosecutor's Office, Western District Prosecutor's Office and Viru District Prosecutor's Office). The total number of prosecutors is 198 (for further details and the number of prosecutors specialised in financial crimes, including money laundering see above para 374).

402. Representatives from the Prosecutor's Office stated that they are satisfied concerning funding and staffing and that they are provided with sufficient technical and other resources. Currently, the salary of prosecutors amounts to approx. 70% of that of judges and in the coming 2 years it will be raised to the same level as that of judges. A system of additional performance-based payment has been established.

403. At least 3 times per year, prosecutors dealing with financial and money laundering offences have a round table meeting where problems concerning investigations are discussed and analysed.

404. Representatives from the **SPB** stated that their staff numbering is sufficient, but the evaluators cannot assess this statement as the exact number of staff was considered to be confidential (§ 9 para 6 of the State Secrets and Classified Information of Foreign States Act). The employees frequently participate in various seminars and conferences in Estonia and abroad in order to keep up with numerous national and international legislations that regulate the attitude, behaviour and every day work of officials.

405. The staff of the **Tax and Customs Board** (TCB) consists mainly of officials with a police background. Upon recruitment, special attention is paid to the reliability of the person, which means that background checks of the candidates are obligatory. The Intelligence Department is staffed with 37 officials at the TCB headquarters and 63 officials at regional level. The number of staff at the border is 120.

406. Representatives of the TCB expressed that they do not have enough resources (human and technical); it was explained that the TCB can manage its daily work sufficiently, but there is a need for additional resources (particularly for investigations)., It should be noted that the IT system of the TCB is old and should be renewed.

407. One of the duties of the Customs Control is to secure the effective fight against illicit trafficking – which, as a criminal activity, may be related to money laundering and terrorist financing. Therefore, the training related to customs control has been focused on securing the border control.

Professional standards (confidentiality, integrity and other skills)

408. **Police education** in Estonia consists of 3 levels:
- Police school (2 years)
- Police School of a higher education (another 2 years)
- Public Service Academy
- Master's studies (another 2 years; in co-operation with state universities).

409. Candidates have to undergo a background check, which usually takes several weeks; this also includes the checking of criminal records. Candidates also have to make a declaration concerning the economic situation (property, income etc.) of themselves and their close relatives. This is also an annual obligation for all police officers.

410. There are a number of provisions regulating professional standards for Police officials. § 8 of the Police Service Act stipulates

§ 8. Requirements for police officers

(1) An Estonian citizen who has attained 19 years of age, has at least secondary education, is proficient in Estonian to the extent established by law or legislation issued on the basis of an Act and meets the professional requirements for police officers may be employed in the service as a police officer.

(2) The professional requirements for police officers, including requirements for their physical training, educational background and health shall be established by a regulation of the Government of the Republic.

The Regulation mentioned under § 8 Police Service Act was issued on 22 June 2006 (no 141). According to this Regulation, the police officer must have the qualities to be able to fulfil the obligations and respond to the requirements of police service as follows:

- loyalty to the Republic of Estonia, honest and law-abiding;
- Ability to work, including the ability to work sustainably and be achievement-orientated also in tense situations and the ability to do teamwork;
- A sense of duty, the ability to make decisions and *Sui juris,* including the ability to make decisions according to the competence of position, the ability to see the consequence of the decisions and take the consequences;
- intellectual abilities, including the ability to differentiate the importance and the ability to analyse and synthesise, the ability to own the information that is ready to use and react to changes in a timely manner;
- good ability to socialise;
- different requirements to the education (depending on the position), including the requirement to take part in complementary training, physical preparation and health.

411. In this context it is also worth referring to § 9 of the Police Service Act which provides a list of grounds that persons shall not be employed in the police service:

a) a person with restricted active legal capacity;
b) a person who has not undergone compulsory military service;
c) a person who has been punished for an intentionally committed criminal offence;
d) a person who has been convicted with a sentence of imprisonment;
e) a person who is a suspect, the accused or accused at trial in a criminal case;
f) a person deprived of the right to work in the position of police officer by a court judgment entered into force;
g) persons closely related by blood (parents, brothers, sisters, children) or by marriage (spouse, spouse's parents, brothers, sisters, children) to an officer or the immediate superior who has direct control over the corresponding position;
h) persons who receive a pension, remuneration or other regular benefits from a foreign state.

412. Police officers shall take the police oath as well. For those who are not police officers (which is approx. one third of all Police staff), the Public Service Act is applicable, stating:

§ 14. Requirements for state or local government officials

(1) An Estonian citizen who has attained eighteen years of age, has at least a secondary education, has active legal capacity and is proficient in Estonian to the extent provided by or pursuant to law may be employed in the service as a state or local government official.

(2) A person who has attained 21 years of age and complies at least with the requirements provided for in subsection (1) of this Act may be appointed to a position of higher or senior official in the state public service.

(3) A citizen of a Member State of the European Union who conforms to the requirements established by law and on the basis of law may also be appointed to a position. Only Estonian citizens shall be appointed to positions which involve exercise of public authority and protection of public interest. Such positions are, for example, the positions related to the directing of the administrative agencies specified in subsections 2 (2) and (3) of this Act, exercise of state supervision, national defence and judicial power, processing of state secrets, representing of public prosecution and diplomatic representation of the state, and the positions in

which an official has the right, in order to guarantee public order and security, to restrict the basic rights and freedoms of persons.
§ 16. Persons who shall not be employed in service
The following shall not be employed in the service:
1) a person under punishment for an intentionally committed criminal offence;
2) a person under preliminary investigation for or a person accused of a criminal offence for which the law prescribes imprisonment;
3) a person deprived of the right to work in a particular position or to operate in a particular area of activity by a court judgment which has entered into force, in such office or area of activity;
4) persons who are in a close relationship (grandparents, parents, brothers, sisters, children, grandchildren) or in a close relationship by marriage (spouse, spouse's parents, brothers, sisters, children) with an official or the immediate superior who has direct control over the corresponding position;
5) a person who has been punished for an act of corruption under administrative or criminal procedure.

413. On the basis of the Taxation Act, the Personal Data Protection Act, the Public Information Act and other legal acts, the **Tax and Customs Board** developed and implemented internal requirements for handling professional secrecy. The Director General of the TCB issued several Ordinances ensuring the protection of information including:
- TCB List of Documents (28 December 2006, Ordinance No 477-p);
- TCB operations procedure (1 July 2005, Ordinance No 250-p);
- Information Security Policy (27 July 2005, Ordinance No 322-P), which is mostly based on ISO/IEC TR 13335 standards and on ISKE (i.e. an Estonian standard for the protection of information systems, issued by the Government of the Republic of Estonia);
- TCB information systems regulation and liability for due usage of the information systems.

414. The Director General of the TCB also issued (8 April 2005; order No 169-P, amended on 21 June 2006, No 299-P) the "General Principles of Ethical Behaviour of TCB Officials". Furthermore, there are several guidance papers governing the integrity of officials and protection information:
- General Principles of Ethical Behaviour of TCB Officials;
- The case definition of corrupt behaviour;
- Guidance for behaviour in the case of bribing and gratuities;
- Notification of the relationships involving the risk of corruption and acts of corruption;
- Procedure for Submission of the declaration of economic interests.

Training

415. The FIU provides a lot of training to other governmental authorities: the Head of the FIU and the Heads of Units are actively engaged in providing various law enforcement agencies, prosecutors, judges etc. with AML/CFT training. In 2006, 6 training seminars (to 166 officials), in 2007, 6 seminars (194 officials) and in 2008, 5 seminars (to 150 officials) were provided to law enforcement officers (Police, Tax and Customs Board, Security Police) by the FIU.

416. Through 2005 to 2006, an AML/CFT twinning programme was implemented in cooperation with the Netherlands which included various courses for prosecutors, Police, Tax and Customs Board, Security Police, the FIU and judges.

417. So far, the **Police** were not provided with training concerning the new MLTFPA. In the past there was some training on AML/CFT issues. Since 2002 there has been a special training course (8 hours) on money laundering and since 2004 also on terrorist financing issues for the students of the Police College of *Sisekaitseakadeemia* (Estonian Public Service Academy). The lecturers are from the FIU. The course is a part of the second stage of the police education.

418. Also the **Security Police Board** pays great attention to the training of its employees which is done as "in-house training", carried out by more experienced employees.

419. **Prosecutors** are provided with in-service training. Prosecutors described that there are even more possibilities for training than they could attend. In addition to national training courses, prosecutors also participated in a number of training courses abroad.

420. The FIU made available the teaching materials on money laundering to the **Tax and Customs Board**. According to the information exchange agreement between the TCB and the FIU, a common training for the officials of both authorities took place on 6 March 2008. The officials of the *Investigation Department* of the Tax and Customs Board 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 money laundering and financing of terrorism. However, some officials have undergone training related to proceeds of crime (seizure and confiscation of proceeds of crime).

Additional elements

421. According to the list provided by the FIU about training courses and seminars held in 2006 and 2007, judges were only provided during this period with one special training course on AML issues by the FIU. In February 2008, the FIU provided an AML/CFT training for judges (30 participants).

Recommendation 32

Statistics – investigations, prosecutions and convictions

422. The competent authorities keep a wide range of statistics on AML matters and in this way they review the effectiveness of their systems for combating money laundering and terrorist financing.

423. The **FIU** maintains comprehensive annual statistics on the:
- number of STRs received. This includes also the breakdown of the type of financial institutions or DNFBP or other businesses or persons filing the STR;
- number of STRs analysed and disseminated;
- number of cases disseminated. Each case may include several STRs.

424. The FIU maintains comprehensive statistics concerning STRs which were forwarded to the Police or Prosecutor's Office for further proceedings. 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. The relevant statistics and figures have already been described above (Section 2.5; para 329 ff).

425. The TCB keeps statistics in general, but there are no statistics available on individual cases. The following statistical data was provided during the on-site visit by the authorities:

Pre-trial Criminal Proceedings at the Investigation Department of the Tax and Customs Board
2005-2008

No	Statistical Data	2005	2006	2007
1.	**Procedures in criminal matters forwarded to the prosecutor's office**	131	134	166
1.1	… tax offences	31	39	59
1.2	… customs offences / unlawful handling	86	78	81
1.3	… drug offences	14	10	25
1.4	… other offences	0	7	1
1.5	… seizure of illegal assets	13	33	28
1.5.1	… estimated value of seized illegal assets (in EEK)	26 000 000	52 000 000	69 000 000
2.	**Cases related to suspicion in money laundering forwarded to the prosecutor's office**	0	1	1
2.1	… suspicion in money laundering	0	1	5
2.2	… damage caused (by tax offence) (in EEK)	0	16 000 000	16 000 000
2.3	… seizure of illegal assets	0	1	1
2.4	… estimated value of seized illegal assets (in EEK)	0	6 000 000	5 000 000

2008		
3.	**Ongoing proceedings in** cases related to suspicion in money laundering	3 cases/ 9 persons
3.1	… tentative damage caused by these cases (in EEK)	83 000 000
3.2	… seizure of illegal assets in these cases	3
3.3	… estimated value of seized illegal assets (in EEK)	28 000 000

2.6.2 Recommendations and comments

426. Estonia is in compliance with Recommendations 27 and 28.

2.6.3 Compliance with FATF Recommendations 27 and 28

	Rating	Summary of factors underlying rating
R.27	**C**	
R.28	**C**	

2.7 Cross Border Declaration or Disclosure (SR IX)

2.7.1 Description and analysis

427. In Estonia, being an EU member country, the *Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community* is directly applicable; it entered into force on 15 June 2007. According to Article 3, any natural persons entering or leaving the European Community (but not between Estonia and another EU member country) must *declare* any cash that they are carrying if it amounts to 10 000 EUR or more (or the equivalent in other currencies). This Regulation provides for the declaration to be made either orally, electronically or in writing. In Estonia, the competent authority in accordance with Art. 2 of Regulation (EC) No 1889/2005 is the Tax and Customs Board (TCB). Since 21 December 2007, Estonia has been part of the Schengen zone, i.e. it has abolished border controls on persons travelling between Schengen countries. Before the above mentioned Regulation (EC) No 1889/2005 came into force, there was no legal provision requiring that persons have to declare any physical cross-border transportation of cash (the Estonian authorities advised that before Estonia's access to the European Union in 2004, there was an obligation to declare cross-border transportation of cash exceeding 100 000 EEK).

428. Based on several different laws and regulations, the main tasks of the customs control on the borders are:

a) Drug detection controls;
b) Alcohol and tobacco controls;
c) Cash controls;
d) strategic goods and dual-use goods controls;
e) other controls which enhance the safety of society;
f) controls of products under the EU Common Agricultural Policy.

429. So far, the TCB received the following declarations:

	III. Quarter 2007		IV. Quarter 2007	
	export	import	export	import
Number of declarations	189	6	234	13
Total	195		247	
Value (EUR)	94 996 984	1 123 212	155 237 241	826 935
Total	96 120 196		156 064 176	

430. The evaluators were informed that most of the cash *imports* are from Russia and Latvia. The Estonian authorities also explained that the large amount of cash *exported* from Estonia (and also the discrepancy between import and export as well as the very high average amount of a single declaration which is nearly 600 000 EUR) is caused by the fact that a lot of Russian individuals and companies change their money in Estonia as there are better exchange rates (no commissions added): the procedure is as follows: that the money (in RUB) is sent via wire transfers to Estonia, there it is withdrawn, changed into USD or EUR and brought physically back to Russia. With regard to this procedure which follows a very usual money laundering scheme, Estonian authorities informed that the FIU has performed on-site inspections to all major currency exchange offices exchanging RUB to EUR or USD (which also resulted in fines and misdemeanour proceedings); it was said that these service providers cooperate with the FIU and report suspicious transactions as a result of this supervision activity. Also the Customs are said to be aware of this situation and to cooperate effectively with the FIU. So far, these declarations caused one money laundering investigation which was started in 2007 and where more than 10 Million EUR were seized (the investigation is still pending).

431. In the case of a suspicion of money laundering or terrorist financing, the declaration is forwarded to the FIU. The FIU provided the following statistics concerning STRs (one STR may cover multiple declarations) sent by the TCB:

STR sent by the TCB										
Year	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**TOTAL**
STR	4	7	68	71	21	70	129	73	54	**497**

432. According to Article 3(2)(e) of Regulation No. 1889/2005, the declaration must contain details of the provenance and intended use of the cash. The evaluators were provided with an English version of the declaration form (Annex IV of Regulation No 91, 23 April 2004 of the Minister of Finance on travellers customs formalities, traveller's declaration form and its performance). It is separated into several sections and requests *inter alia* information on the person, a description of the cash or monetary instruments transported, the provenance and destination of it. It also contains instructions on how to fill it in.

433. The border checkpoints are equipped with examination halls and storage premises; mobile x-ray sets; an automatic number detection system; radiation monitors; x-ray sets for pallets and single packages; constant video surveillance; endoscopes, dosimeters, tools, photo and video cameras etc.

434. According to Article 4(2) in conjunction with Art. 3 of EC Regulation No. 1889/2005, in case of a false declaration or failure of declaration "*cash may be detained by administrative decision in accordance with the conditions laid down under national legislation*". According to § 91^1 of the Customs Act, failure to perform the obligation to declare cash, as defined by EC Regulation No. 1889/2005/EC is punishable by a fine of up to 100 fine units (as one fine unit is defined with 60 EEK, this amounts to 6 000 EEK, i.e. 383.46 EUR). To identify the elements of the misdemeanour specified in § 91^1 of the Customs Act, cash may be deposited as evidence upon identification of the circumstances of the subject of proof in accordance with §§ 62 and 124 of the CCP. However, there are no provisions authorising Customs to seize and also confiscate cash simply in the case of a suspicion of money laundering or terrorist financing. The Estonian authorities explained that Customs would have in such a situation only two possibilities: either they could inform the FIU which could immediately issue a precept that the money has to be frozen (§ 40 paragraphs 1 and 3 MLTFPA); furthermore, they could also initiate criminal proceedings, inform prosecutors to get an order from the investigative judge to seize the cash. However, the evaluators consider this a shortcoming as the system involving the FIU or courts may work to a certain extent during working hours when there are no difficulties to reach responsible persons at the FIU or at courts. However, when it comes to nighttimes, weekends and public holidays, this system is not fully operational.

435. In the case of the failure to declare cash and the submission of a false declaration a person is detained at the border along with the cash (§ 91^1 Customs Act). A false declaration is forwarded to the Investigation Department of the TCB. The evaluators were not informed of a legal basis authorising Customs to stop or restrain currency or bearer negotiable instruments when there is a suspicion of money laundering or terrorist financing (criterion IX.3 a).

436. The Information Department of the TCB keeps all the necessary data concerning cash declarations (above threshold; false declarations; failure of declarations). However, Customs do not keep data on cases when there is a suspicion of money laundering or terrorist financing; instead, Customs forward such information to the FIU which stores this information.

437. According to a Memorandum of Understanding between the TCB and the FIU, the TCB sends all cash declarations which indicate a suspicion of money laundering or terrorist financing to the

FIU. The exchange of information and cooperation in cash declaration matters is based on this agreement. Furthermore, this Memorandum of Understanding determines 5 officials of the Intelligence Department of the TCB as contact persons, who are responsible for exchanging information with the FIU and answering information requests from the FIU. The FIU also has direct access to the Tax database (excluding the internal data base of the Customs).

438. The Tax and Customs Board also has cooperation agreements with other state authorities (Police Board, Border Guard, Security Police) and customs assistance agreements with all the neighbouring states and many other states. These agreements also cover joint operations as well. However, so far, cash information has not yet been exchanged on the basis of customs assistance agreements. In this respect it is also necessary to mention Art. 6 of EC Regulation No. 1889/2005 which stipulates that "*where there are indications that the sums of cash are related to any illegal activity associated with the movement of cash, as referred to in Directive 91/308/EEC*[27]*, the information obtained through the declaration provided for in Article 3 or the controls provided for in Article 4 may be transmitted to competent authorities in other Member States*". In practice, there is good cooperation between the TCB and border police, at both central and regional level. Work is divided between the authorities in the areas of responsibility, training, joint investigations and information exchange. If there should be no agreement with a country, the TCB is trying to establish contacts with both, in a direct and indirect way.

439. In the context of criterion IX.9, reference has to be made to the general sanction regime of the Penal Code, particularly to the money laundering offence and to the provisions covering financing of terrorism. This reference to the sanction regime of the Criminal Code (and the criminalisation of money laundering and terrorist financing) in conjunction with the aiding and abetting provisions covers the conducts envisaged by criterion IX.9, though it should be noted that it suffers from the same deficiencies as described above under Sections 2.1 and 2.2.

440. In the case of discovering an unusual cross-border movement of gold, precious metals or precious stones, Customs can contact third countries (countries of destination or origin and others) and notify them or request additional information from them. Gold, precious stones, etc. are considered as goods and therefore the exchange of information falls under the customs assistance agreements. As mentioned above (para 438), Customs assistance agreements have been concluded with a number of countries.

441. Concerning safeguards for the systems for reporting cross border transactions, it has to be noted that this data is maintained by the TCB in a computerised data base (Excel sheet). In order to use them, one needs proper authorisation, which is only granted on the basis of a reasonable application.

2.7.2 Recommendations and comments

442. Estonia should establish an effective regime to stop or restrain currency or bearer negotiable instruments when there is a suspicion of money laundering or terrorist financing at the border (criterion IX.3 a).

443. There are no provisions authorising Customs to seize cash simply in the case of a suspicion of money laundering or terrorist financing. In such a situation Customs have only two possibilities: either they could inform the FIU which could immediately issue a precept that the money has to be frozen or they could initiate criminal proceedings and inform prosecutors to get an order from the investigative judge to seize the cash. This system may work to a certain extent during working hours when there are no difficulties to reach responsible persons at the FIU or at courts. However,

[27] so called First EU AML Directive.

when it comes to nighttimes, weekends and public holidays, this system is not fully operational. Estonia should establish an effective system which allows that at any time there is the possibility to seize cash when there is a suspicion of money laundering or terrorist financing (in the evaluators view the easiest way to do so would be to authorise Customs to seize cash in the case of a suspicion of money laundering or terrorist financing).

444. Estonia has a new declaration system in place (following EC Regulation No. 1889/2005). This covers only the transfer of cash or bearer negotiable instruments when entering or leaving the European Union territory and not between Estonia and another EU member-state, which is a requirement of Special Recommendation IX[28].

2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors underlying rating
SR.IX	**PC**	• There are no legal provisions ensuring that there is under the circumstances of Special Recommendation IX at any time a designated competent authority which is authorised to stop or restrain currency or bearer negotiable instruments when there is a suspicion of money laundering or terrorist financing. • There are no legal provisions ensuring that there is under the circumstances of Special Recommendation IX at any time a designated competent authority to seize cash when there is a suspicion of money laundering or terrorist financing. • As the disclosure system has been established only in mid 2007, there are not yet comprehensive statistics available. Thus, it is not yet possible to assess the effectiveness of the system. • EC regulation No. 1889/2005 and relevant national legislation do not cover the transfer of cash or bearer negotiable instruments between Estonia and another EU member state[29].

[28] It has to be noted that the European Commission proposed amendments to the FATF Methodology and to consider in the context of Special Recommendation IX the European Community as one jurisdiction. As a consequence this would not be considered a shortcoming any more. This issue is currently under consideration by the FATF and was at the time of the adoption of this report not yet solved.

[29] see FN 28.

3 PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

445. The preventive measures required of operators in the Estonian financial sector are primarily set out in the new Money Laundering and Financing of Terrorism Prevention Act ("MLTFPA"). This law came into effect on 28 January 2008, which is one week before the on-site visit. § 3 of the MLTFPA defines the "obligated persons" under the Act, to which the requirements set out in the MLTFPA apply. The MLTFPA sets out a number of provisions which apply equally to DNFBP and financial institutions. Where applicable, the MLTFPA makes specific mention of "credit and financial institutions" when measures are required only for these entities.

446. Since the new law came into force on 28 January 2008, the evaluation team could not fully assess the effectiveness of the new provisions and obligations. The evaluation team however noted a high level of awareness by the industry concerning the new obligations. Consequently, and in the light that implementation decrees had still to be issued by the Ministry of Finance, the ratings are based on the new legal provisions and effectiveness is evaluated with regard to the provisions of the previous MLTFPA.

447. § 6 (1) of the MLTFPA refers for the definition of a *credit institution* to the definition as provided for by the Credit Institutions Act (CrIA); § 3 CrIA defines credit institutions as "*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*". Furthermore, the MLTFPA understands credit institutions as the branch of a foreign credit institution registered in the Estonian commercial register (§ 6 (1) 2) MLTFPA).

448. In a similar way of cross-referencing as the definition of credit institutions, § 6 (2) MLTFPA refers also for the definition of *financial institutions* to the definition as provided for by the Credit Institutions Act. § 5 CrIA defines financial institutions as "*a company other than a credit institution, the principal and permanent activity of which is to acquire holdings or conclude one or more of the transactions specified in clauses 6 (1) 2)-12) of this Act*"; the activities as described in § 6 (1)2)-12) CrIA cover "*borrowing and lending operations, including consumer credit, mortgage credit, factoring and other transactions for financing business transactions; leasing transactions; settlement, cash transfer and other money transmission transactions; issue and administration of non-cash means of payment (e-g. electronic payment instruments, traveller's cheques, bills of exchange); guarantees and commitments and other transactions creating binding obligations to persons; transactions for their own account or for the account of clients in traded securities provided in § 2 of the Securities Market Act [...] and in foreign exchange and other money market instruments, including transactions in cheques, exchange instruments, certificates of deposit and other such instruments; transactions and acts related to the issue and sale of securities; provision of advice to clients on issues concerning economic activities, and transactions and acts related to the merger or division of companies or participation therein; money broking; portfolio management and consultation on investment issues; safekeeping and administration of securities"*.

449. Furthermore, § 6 (2) MLTFPA considers the following services also as *financial institutions* for the purposes of the MLTFPA: providers of currency exchange services; providers of payment services; providers of services of alternative means of payment; an insurer engaged in life assurance within the meaning of the Insurance Activities Act (insurer); an insurance broker engaged in mediation of life assurance within the meaning of the Insurance Activities Act (insurance broker); a management company and an investment fund established as a public limited company within the meaning of the Investment Funds Act; an investment firm within the meaning of the Securities Market Act; a savings and loan association within the meaning of the Savings and Loan Associations Act; an electronic money institution within the meaning of the Electronic Money Institutions Act; or a branch of a foreign service provider registered in the Estonian commercial register providing one of the above services.

450. It is obvious that the law drafters of the MLTFPA were anxious to cover all kind of financial activities as described by the FATF Methodology. As a consequence there are some financial activities which are covered both by § 6 (2) 1) MLTFPA (which refers to the definition as provided for by § 5 CrIA) and by the list of § 6 (2) 2) - 11) MLTFPA: e.g. currency exchange services, providers of payment services, companies trading in securities etc. Though these overlaps could cause some theoretical discussions under which particular provision a specific entity may be covered, it seems that the MLTFPA's definition of financial institutions is wider than the activities described in the FATF Methodology and 3rd AML Directive.

451. The most pertinent primary legislation in the AML/CFT field is the Money Laundering and Terrorist Financing Prevention Act (MLFTPA). Additionally, relevant primary legislation to which the MLTFPA makes reference and which supplies additional abilities to government authorities, for example regarding their sanctioning power, exists, e.g. the Credit Institutions Act (CrIA), Insurance Activities Act, Securities Market Act, etc. Primary legislation in many cases gives the authority to create secondary legislation regarding specific subsets of the subject matter of the primary legislation. The MLFTPA has specified that the Minister of Finance shall issue secondary law for areas with low money laundering or terrorist financing risks according to (§ 18 (5) MLTFPA) and regarding AML/CFT-specific internal rules of procedure for credit and financial institutions (§ 31 (6). Such secondary law was created with the Minister of Finance Regulations 11 and 10, respectively, on 3 April 2008. As both came into force only on 11 April 2008 (date of the publication in the Official Gazette) and moreover the Minister of Finance Regulation No 10 stipulates in its § 30 that "*Credit and financial institutions must bring their activities and documents into compliance with the provisions of this Regulation by no later than 1 November 2008*", it was not taken into account in the descriptive part and for rating purposes; where appropriate it was referred to it with a footnote (para 36 of the FATF Handbook for countries and Assessors).

Customer Due Diligence and Record Keeping

3.1 Risk of money laundering / financing of terrorism

452. A country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is low or little risk of money laundering or terrorist financing. In Estonia, there was no such decision not to apply certain measures recommended in the FATF 40+9 Recommendations just because of low or little risk of money laundering or terrorist financing. However, Estonian law allows the use of simplified CDD in specified instances of low risk (see below, para 487).

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to R.8)

3.2.1 Description and analysis

Recommendation 5

453. The obligations arising under Recommendation 5 are mainly addressed by provisions of the new MLTFPA, which reflect the intent of the Estonian lawmaker to introduce legal provisions covering the requirements set out both in the FATF 40+9 Recommendations as well as those set out in the third EU AML Directive (2005/60/EC). The MLTFPA sets out obligations which must be complied with. The law, according to its § 3, applies to: credit institutions; financial institutions, organisers of games of chance; persons who carry out or act as intermediaries in transactions with real estate; traders for the purposes of the Estonian Trading Act, if a cash payment of no less than 200,000 EEK (12756.32 EUR) or an equal amount in another currency is

made to the trader, regardless of whether the financial obligation is performed in a single transaction or in several related payments (unless otherwise provided for by law); pawnbrokers; auditors and providers of accounting services; providers of accounting or tax advice services; providers of trust and company services. These entities are described by the MLTFPA also as "obligated persons" (§ 10).

454. Some of the provisions of the law refer specifically only to "credit and financial institutions".

Anonymous accounts and accounts in fictitious names

455. § 15 (2) MLTFPA forbids financial institutions from providing services which can be used without prior identification and verification of the customer; this provision expressly requires such institutions "*to open an account and keep an account only in the name of the account holder*". In addition, the language of the law also does not make an allowance for previously established relationships. Indeed, a provision requiring such institutions to hold accounts only in the name of the account holder also existed in the law existing previously to the MLTFPA, in § 6 (3) of the MLTFPA. Under the current law, unnamed accounts are not only illegal, all transactions relating to them are also void *ipso iure* should they occur (according to § 15 (3), 2nd sentence). The private sector representatives met by the evaluators were well aware of this restriction. § 6 (3) and (4) of the previous MLTFPA similarly required accounts to be in the name of the account holder.

Customer due diligence

When CDD is required

456. § 12 (2) 1) MLTFPA requires all obligated persons to undertake CDD at least when establishing a business relationship. § 11 (1) 2) MLTFPA provides for a definition of "business relationship" and makes it clear that this "*is not based on a contract for an indefinite period, but which may reasonably be expected to last for a certain term and during which an obligated person repeatedly enters into separate transactions in the framework of its economic or professional activities or professional practice*". Thus, this definition covers also repeated one-off transactions with the same customer when undertaken as part of a economic relationship which can be expected "*to last over a certain term*".

457. According to § 12 (2) 1) MLTFPA, all obligated persons are also required to undertake CDD when carrying out occasional transactions above the designated threshold of 200 000 EEK (12 782.33 EUR). The language specifically also includes situations where the transaction is carried out in several operations that appear to be linked. Furthermore, § 14 (2) clarifies that if the total amount of related payments is not known, the requirement for CDD arises as soon as an exceeding of the threshold becomes evident.

458. § 25 (7) and (8) MLTFPA require financial institutions (but not DNFBP) to include with payment mediation services information compulsory under Regulation (EC) 1781/2006, which is directly applicable in Estonia. The law also requires to include with any alternative means of payment information regarding the names of payer and recipient, as well as "*... the [Estonian] Personal Identification Code, and upon absence thereof, the date and place of birth or a unique feature on the basis of which the payer can be identified*" (§ 25 (8) MLTFPA). § 25 (1) MLTFPA makes it clear that such information has to be based upon a previous identification and verification of the customer.

459. § 12 (2) 3) MLTFPA requires all obligated persons to carry out CDD whenever there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds provided elsewhere in law.

460. § 12 (2) 4) MLTFPA requires financial institutions to undertake CDD whenever it has doubts about the veracity or adequacy of previously obtained customer identification data.

461. The representatives of the private sector with whom the evaluators met were well aware of the CDD requirements. Given that the MLTFPA was introduced very short before the on-site visit, they were not always aware of the exact criteria of the new law, but indicated that training sessions were under way and that new procedure manuals were being prepared or had already been provided which took the new provisions of the MLTFPA into account. These training sessions could leverage off the procedures already in place, as the previous Estonian MLTFPA, in its §§ 6 ff also contained identifications and verification requirements for, e.g. cash transactions beyond a certain threshold (lower than the one provided by the Directive), instances of smurfing, suspicious transactions and upon opening an account.

Required CDD measures

462. While § 12 MLTFPA lays out the general requirement for CDD measures and when CDD has to be undertaken, § 13 MLTFPA describes the necessary steps of the CDD process. Furthermore, §§ 23 and 24 MLTFPA describe the information which must be gathered in relation to both natural (§ 23 MLTFPA) and legal (§ 24 MLTFPA) persons.

463. § 13 (1) 1) MLTFPA states that while *identification* of a customer will be made according to documents provided by the customer, *verification* of the information provided is required "*on the basis of information obtained from a reliable and independent source*". § 23 (1) MLTFPA states that information pertaining to the person's name, [Estonian] personal identification code or date and place of birth needs to be verified according to a document specified in §§ 2 (2) or 2 (4) of the Identity Documents Act. Apart from Estonian identity documents, these also allow using a valid foreign travel document or a driving license which contains comparable data to an Estonian identity document as per § 2 (4) of the Identity Documents Act. A similar requirement was included in the previous Estonian MLTFPA under § 7 (1).

464. § 23 (2) MLTFPA further requires that 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 specified in subsection (1), an obligated person shall register the following personal data:*

1) the name and the representative's name;

2) the personal identification code or, upon absence of a personal identification code, the date and place of birth;

3) the name and number of the document used for identification and verification, its date of issue and the name of the agency that issued the document;

4) the name of the document, used for identification and verification of the right of representation, its date of issue and the name of the issuer."

A similar requirement existed in § 11 of the previous Estonian MLTFPA (listing the information to be gathered) and § 9 (1), second sentence, requiring a photocopy of the identifying document(s).

465. The law also, in § 23 (4), provides that at the request of an obligated person, a person or customer participating in a transaction performed in economic or professional activities shall submit documents and provide relevant information required for application of the due diligence measures.

466. If such documents cannot be provided, documents certified or authenticated by a notary public or authenticated officially may be used for verification of the identity of a person (§ 23 (6) MLTFPA). According to § 23 (7) MLTFPA, a "*person or customer participating in an economic or professional transaction or official act shall, at the request of an obligated person, certify the correctness of the submitted information and documents in hand or by signature*".

467. Obligated Persons are allowed to rely on information received from credit institutions licensed in Estonia or such other nations as have requirements in place equal to those contained in the MLTFPA. While the law indicates that member states of the European Economic Area are considered to be in line with this criterion, no further guidance is available regarding the question of which countries satisfy this requirement (§ 14 (4) MLTFPA).[30]

468. The required CDD measures as described above under para 456 to 467 are also sanctionable as § 57 MLTFPA provides sanctions both for natural persons and legal persons if they "*fail to comply with identification requirements*". The sanction for natural persons is a fine up to 300 "fine units"; as 1 fine unit was defined with 60 EEK at the time of the on-site visit, the maximum fine for natural persons is 18 000 EEK (approx. 1 150 EUR). The sanction for legal persons is a fine up to 500 000 EEK (approx. 31 955 EUR). These fines cannot be cumulated in case of several breaches.

469. § 13 (1) 2) and 3) MLTFPA require the identification of both the natural person acting as agent for a legal person as well as identification of the legal person. Further details are set out as follows:

470. Regarding the person purporting to act on behalf of a legal person, where the legal entity is supposed to become the customer of the obligated person, § 13 (1) 2) MLTFPA requires "*identification and verification of the representative of a natural or a legal person and the identification and verification of the right of representation*". The legal requirements regarding the identification of the acting representative are therefore identical to the requirements pertaining to natural persons as customers outlined above.

471. Regarding the power of representation, § 23 (5) MLTFPA provides that "*a representative of a legal person of a foreign country 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 replacing legalisation (apostille), unless otherwise prescribed by an international agreement*". § 23 (1) MLTFPA spells out that "*the representative of a person participating in a transaction shall submit in the required format a document certifying the right of representation*". The required format is further defined in §§ 23 and 24 MLTFPA.

472. § 24 MLTFPA requires financial institutions to gather and verify information regarding the formation and legal power of any legal entity in regard to which it is required to undertake CDD, as well as the powers to bind such an entity. According to the "Explanatory Memorandum to the Draft Money Laundering and Terrorist Financing Prevention Act", one of the purposes underlying the creation of § 24 MLTFPA was to comply with criterion 5.4b of Recommendation 5. § 24 MLTFPA specifically requires: „*(1) An obligated person shall identify a legal person and its passive legal capacity and verify it. A legal person registered in Estonia or a branch of a foreign company registered in Estonia shall be identified on the basis of an extract of a registry card of the relevant register and a foreign legal person is identified on the basis of an extract of the*

[30] The list of equivalent third countries was adopted in the EU Committee on the Prevention of Money Laundering and Terrorist Financing on 18 April 2008 (*Common Understanding Between Member States on Third Country Equivalence Under the Anti-Money Laundering Directive (Directive 2005/60/EC*)). The list and Estonian translation has been made available on the web-pages of the Ministry of Finance, FSA and FIU.

relevant register or a transcript of the registration certificate or an equal document, which has been issued by the competent authority or body not earlier than six months before submission thereof. (2) The document submitted in order to enable identification shall set out 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. (3) On the basis of the documents specified in subsection (1) 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 replacing it and their authorisation in representing the legal person; 2) the area of activity of the legal person; 3) means of communications' numbers; 4) the data of the beneficial owners of the legal person."

473. § 13 (1) 2) and 3) MLTFPA require obligated persons to identify and verify the identity of natural persons acting on their own behalf as well as acting upon a legal person's behalf, as well as identifying the legal person for whom a natural person may be acting and the natural persons who are the ultimate beneficiaries of a legal person.

474. However, the language in the law (at least according to the English translation provided) does not spell out specifically that an instance of beneficial ownership can also occur when a natural person acts for another natural person (for the language of § 8 MLTFPA defining "beneficial owner" for the purpose of this Act, see below para 478). While the applicable legal provisions can be interpreted to cover this situation, they do not specifically mandate this interpretation – it would be also possible to interpret the law in a way that the concept of "beneficial ownership" only applies to the ultimate owners and controllers of legal persons. Also the applicable part of the "Explanatory Memorandum to the Draft Money Laundering and Terrorist Financing Prevention Act" seems to allow both readings.

475. The drafters of the law and, indeed, all Estonian authorities met by the evaluators, clearly understood the law's provisions on beneficial ownership to also cover instances of a natural person exerting control over another natural person. The representatives of the financial sector met by the evaluators clearly did not have the same understanding. Rather, it appeared that "beneficial ownership" as a concept was widely understood to refer to ultimate control over legal entities (only). The representatives did state unanimously that they would consider any indication of a natural person being somehow controlled by another natural person without having so declared (as in the case of accounts held by attorneys or notaries) a suspicious action which they would notify to the FIU.

476. The Estonian authorities advised that this is likely due to the fact that the on-site visit occurred immediately after the new MLTFPA came into force. Under the previous MLTFPA (which was in force until 28 January 2008 when the new MLTFPA came into force), the concept of "beneficial ownership" was not covered. Nevertheless, § 10 of the previous MLTFPA specified that if "*upon identification, there is good reason to suspect that a person is acting on behalf of or for the account of someone else, the credit or financial institution … shall obtain information as to the real identity of the person on whose behalf or for whose account the person is acting*", as well as a legal requirement to terminate the business relationship and inform the FIU if CDD on the beneficial owner cannot be carried out. So while the term of "beneficial owner" was clearly not well understood, it appears that the underlying requirements were being met.

477. § 13 (1) 3) MLTFPA, *inter alia*, requires "*gathering information on the ownership and control structure of a legal person, trust, civil law partnership or other contractual legal arrangement on the basis of the information provided in pre-contractual negotiations or obtained from another reliable and independent source*"; in conjunction with § 8 MLTFPA it can be concluded that this requires coming to an understanding of the ownership and control structure of the legal entity in order to comply with this legal requirement. § 24(3) 4) MLTFPA also requires to register the data

of the beneficial owners of a legal entity when identifying that entity. However, though this covers some elements of understanding of the ownership and control structure of a legal person, it is not the same as establishing the beneficial owner is a more linear process while understanding the ownership and control structure of a legal person requires a more broad approach.

478. § 13 (1) 3) MLTFPA also requires identifying the beneficial owner of a legal entity. § 8 MLTFPA defines the beneficial owner as:

> *"(1) A beneficial owner is a natural person who, taking advantage of his or her influence, exercises final control and in whose interests or favour or on whose account a transaction or act is performed. A beneficial owner is a natural person who ultimately owns the company or exercises ultimate control over the management of a company: 1) by having over 25 percent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares; 2) by 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, 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 in whose interests a legal person, civil law partnership or another contractual legal arrangement is set up or operates."*

§ 24 MLTFPA requires that such data be properly verified.

479. § 13 (1) 4) MLTFPA requires "*acquisition of information about a business relationship and the purpose of a transaction*". According to the "Explanatory Memorandum to the Draft Money Laundering and Terrorist Financing Prevention Act", § 13 (1) 4) requires that "*an obligated person under the MLTFPA must understand why and for what purpose the other party wants to enter into a contractual relationship*". There is no specific sanction for infringements of this provision but as a legal requirement under the MLTFPA, one could say that this requirement is sanctionable in that failure to observe these requirements indicate a failure of the institution's internal controls. Such internal measures are required under § 59 (2) of the Credit Institution Act and similar provisions in the Acts regarding securities and insurance institutions. According to § 103 of the Credit Institution Act, failure to have proper measures in place will be met with a "precept", i.e. an administrative measure requiring compliance with a stated request within a given time. Failure to obey such a precept can be fined according to § 104 of the Credit Institution Act. Parallel provisions exist in §§ 172, 173 and 181 of the Insurance Activities Act, §§ 234 and 235 of the Securities Market Act and §§ 289, 290 and 301 of the Investment Fund Act. However, this way of sanctioning appears very indirect and would not work, if the institution's internal controls would be satisfactory and an infringement would have other reasons (e.g. an employee circumventing sophistically internal control mechanisms).

480. § 13 (5) MLTFPA requires ongoing due diligence through "*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*". Failure to comply with these provisions can be sanctioned as described above in para 468. In addition to regular updates of the information so gathered and verification of this information stipulated in the above provision, § 26 MLTFPA requires storing such data in a form which allows for "full and immediate" answers to information requests by the FIU. The provisions concerning registration and keeping records are sanctionable (§ 58 MLTFPA) in the same way as the sanctions provided for by § 57 MLTFPA in case of CDD infringements.

481. The measures described in the last three paragraphs above (para 478 to 480) contain elements in which the new MLFTPA, having come into force on 28 January 2008, goes substantially beyond the more formal requirements of the previous MLTFPA. However, the private sector representatives met were well aware that the new MLTFPA required a deeper understanding of their customers and their customers' business, and that they had been preparing for the new requirements for some time.

Risk

482. § 19 MLTFPA requires financial institutions and DNFBP to conduct enhanced due diligence in cases of "*high risk of money laundering or terrorist financing*". The law indicates as criteria in which enhanced due diligence measures have to be applied:

- customers who have not been identified face-to-face (either because they are not customers of a financial institution or existing customers who were taken without a face-to-face identification before the coming into effect of the current law, forbidding financial institutions from doing so);
- instances when upon identification or verification of a person suspicion arises concerning the accuracy of the data or authenticity of the documents submitted or that the beneficial owner has not or that the beneficial owners have not been identified; or
- a person or customer participating in a transaction or official act performed in economic or professional activities is a politically exposed person.

483. There is currently no further guidance for obligated persons on what circumstances may pose "*high risk of money laundering or terrorist financing*". § 30 (3) 2) MLTFPA sets out that an institution's internal rules of procedure should set out transactions of a higher risk level and subsection (6) of the same provision states that the requirements in this regard will be set by the Minister of Finance. According to the Ministry of Finance, a minister's decree (secondary, enforceable and sanctionable law) is being drafted which is intended to address this and other issues in which the MLTFPA calls for additional guidance from the Minister of Finance. A draft of this decree was not available for inspection by the evaluators.

484. The MLTFPA contains a difference between categories of (a) "*high* risk" situations of money laundering or terrorist financing, which according to § 19 MLTFPA require enhanced due diligence and (b) "transactions of a *higher* risk level" according to § 30 MLTFPA. Though the difference in language seems small, it has to be highlighted that there is a difference between "high risk" and "higher risk" (a differentiation which is also defined e.g. by Art. 13 of the 3rd EU AML Directive): while "high risk" is at the upper end of a level of risk, "higher risk" refers only to a situation more risky than average. Moreover, it is interesting to note that non-resident customers and private banking (examples given by the Methodology under criterion 5.8) do not appear in the categories of § 19 MLTFPA as higher risk situations for money laundering or terrorist financing which would require enhanced due diligence measures; this is particularly surprising concerning the geopolitical position of Estonia and its number of non-resident accounts (for an overview see para 82). The remainder are, in part, addressed by the requirement in § 30 (3) 2) MLTFPA, which states that obligated persons must have rules of procedure in place which, amongst other things "*describe transactions of a higher risk level and establish the appropriate requirements and procedure for entering into and monitoring such transactions*". However, as the law addresses transaction monitoring rather than customer due diligence, this does not entirely close the gap between the methodology's categories of "higher risk" and the "high risk"-situations specified in § 19 of the MLTFPA.

485. § 18 MLTFPA sets out criteria for low risk, which include instances in which the subject of CDD is a legal person governed by public law founded in Estonia; a governmental authority or another authority performing public functions in Estonia or in another contracting state of the European Economic Area; an authority of the European Community; a company of a contracting state of the European Economic Area or a third country, which is subject to requirements equal to

those provided for in this Act and whose securities are traded in a regulated securities market in one or several contracting state of the European Economic Area; a credit or financial institution, a credit or financial institution located in a contracting state of the European Economic Area or a third country, which in the country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision.

486. According to § 18 (5) MLTFPA, the Minister of Finance will set out further criteria in this regard. Again, according to the Ministry of Finance, a minister's decree (secondary, enforceable and sanctionable law) is being drafted which is intended to address this issue[31].

487. § 17 of the MLTFPA leaves it to the financial institutions in question how and to what extent to apply customer due diligence measures in situations of low risk. However, it requires at a minimum to ascertain the bases upon which a situation of low risk is founded and prohibits using simplified CDD in situations of high risk of money laundering or terrorist financing.

488. Regarding the application of simplified CDD, § 18 MLTFPA provides, regarding each instance of application of simplified CDD, that it may be applied to national entities, similar entities from within the European Economic Area, or from third countries which impose "*requirements equal to those provided for in this act*". At present, no guidance from the Estonian supervisory bodies exists regarding the identity of such countries[32].

489. § 17 (2) MLTFPA states that "Simplified due diligence measures shall not be applied if there is suspicion of money laundering or terrorist financing". This provision applies to both financial institutions and DNFBP.

490. According to § 18 (5) MLTFPA, the Minister of Finance shall establish "*the criteria of the low risk of money laundering or terrorist financing with regard to certain persons or transactions in the case of which simplified due diligence measures may be applied shall be established*". There was no such regulation at the time of the on-site visit, but the evaluation team was informed that a minister's decree (secondary, enforceable and sanctionable law) was being drafted which was intended to address this issue[33].

491. The previous Estonian MLTFPA did not include risk-oriented provisions. The private sector representatives indicated that it was understood that the additional information gathered under the new CDD requirements would have to lead to more in-depth scrutiny where such appeared to be warranted. In particular, the team was advised that the larger internationally owned banks had been using risk-graded client take-on procedures for some time.

492. The lack of guidance available at the time of the on-site visit creates a concern that legal requirements of the new law may not be optimally put into practice.

Timing of verification

493. § 12 (2) MLTFPA states that "An obligated person shall apply due diligence measures at least: 1) upon establishment of a business relationship", where the legal definition for a business relationship is given in § 11 and includes repeated one-off transactions as described above. A similar requirement existed under § 6 (3) of the previous MLTFPA.

494. The MLTFPA makes two exceptions to the rule stated above: Firstly, according to § 15 (4) MLTFPA, a credit or financial institution may exceptionally, at the request of a person participating in a transaction, open an account before full application of due diligence measures on

[31] The Regulation of Minister of Finance was published in the State Gazette and became effective on April 11, 2008; see para 451.

[32] See FN 30.

[33] This was done in the meanwhile; see para 451.

the condition that the account is only debited after full application of the due diligence measures required by law and the first payment relating to the transaction is made through an account of the same person, which has been opened in a credit institution that operates in a contracting state of the European Economic Area or in a state where requirements equal to those provided for in this Act are in force. Secondly, according to § 15 (5), an insurer or insurance broker may verify the identity of a beneficiary under a life assurance contract after establishment of the 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.

495. As a general requirement, § 30 MLTFPA requires all obligated persons to have rules of procedure which ensure that the legal CDD requirements as set out in § 13 MLTFPA are followed, and to have appropriate measures vis-à-vis high risk and low risk transactions in place. Though not explicitly mentioned, the Estonian authorities considered this language to cover also all instances in which a business relationship begins prior to full CDD, which Estonian law allows only in the circumstances as described in § 15 (4) and (5) of the MLFTPA. The financial sector representatives met by the evaluators indicated that they considered business relationships upon which full CDD had not yet been conducted to be an instance of high risk. According to § 30 (6) MLTFPA, further requirements for such rules of procedure shall be established by the Minister of Finance. Such guidance was not yet in existence at the time of the on-site visit. However, the Estonian Ministry of Finance indicated that such guidance (in the form of secondary, enforceable and sanctionable law) was being drafted. § 13 (3) of the previous MLTFPA similarly required financial institutions to have internal procedures in place which safeguarded the performance of duties arising from it.

Failure to satisfactorily complete CDD

496. According to § 27 MLTFPA, obligated persons are legally prohibited from entering into or maintaining business relationships, or engaging in one-off transactions, with persons or entities who fail to furnish information or documents required for the completion of CDD measures required by law. The financial sector representatives met by the evaluators were well aware of this requirement. § 9 (4) of the previous MLTFPA had a similar requirement, although it allowed to carry out a transaction in the exceptional circumstance "*only if there is no reason to doubt the identity of the counterparty*".

497. In instances where a full CDD fails due to the other party's failure to provide sufficient information or documentation, all obligated persons in Estonia are required to file a report to the FIU according to §§ 32 (2); 27 (1) and (2) MLTFPA. The financial sector representatives met by the evaluators indicated that they were aware of this requirement and indicated that they had filed notices with the FIU based on insufficient documentation in the past. Indeed, also the previous MLTFPA contained in its § 10 (2) such a requirement: "*If it is impossible to identify the person on whose behalf or for whose account another person is acting, the credit or financial institution […] is prohibited from carrying out the transaction. The credit or financial institution […] is also required to inform the Financial Intelligence Unit immediately of an expression of intention by the person to carry out a transaction or of a transaction which has already been carried out by the person.*"

498. § 27 (3) MLTFPA provides that an existing business relationship can be terminated without regard to the usual periods pertaining thereto in circumstances where the business partner cannot furnish sufficient information or documentation upon request through an obligated person. This provision applies to circumstances in the remit of criteria 5.2(e) or 5.17, i.e. where a business relationship has already existed for some time and the request for information comes in the course of ongoing due diligence or due to subsequent doubts regarding the veracity of the information provided. The law does not explicitly require termination in these instances (in instances of criterion 5.14, § 27 (2) MLTFPA requires termination of the relationship). Should additional due

diligence have been required because of a particular transaction the long-term customer was trying to undertake, § 32 requires notification to the FIU. However, the law does not seem to require either termination of the business relationship or notification of the FIU in instances in which a request for additional documentation arising only from ongoing due diligence remains unfulfilled. The financial sector representatives met by the evaluators indicated, however, that they would consider such a circumstance suspicious and therefore notify the FIU and then terminate the business relationship depending on the feedback from the FIU.

Existing customers

499. Estonian law, in § 13 (1) 5) MLTFPA, requires all obligated persons to "constantly" monitor their business relationships and any transactions entered into during their course, and includes in this provision the regular verification of data used for identification as well as updating relevant documents, data or information and, if necessary, identification of the source and origin of funds used in transactions. According to § 14 (3) MLTFPA, such due diligence measures may be varied in their scope according to the risk involved. No examples are given in law or guidance regarding the particulars of when to apply due diligence to existing customers. However, a transaction of significance, i.e. in excess of 200 000 EEK (12 782.33 EUR) as well as instances in which there is doubt concerning the veracity of data gathered so far, § 12 (2) and (4) MLTFPA mandate the application of customer due diligence. Also, § 19 (4) MLTFPA states, that in the events specified in paragraphs (1) and (2) an obligated person shall apply the due diligence measures specified in § 13 (1) 5) more frequently than usually.

500. Estonian law, under both the current and former AML law, affirmatively prescribes that accounts may only be held in the proper name of the owner. The Estonian authorities as well as the financial sector representatives met by the evaluators affirmed that anonymous or numbered accounts have never been legal in Estonia.

Recommendation 6

501. As part of their general due diligence measures, obligated persons under the MLTFPA are required, under § 23 (3), to register the address of the place of residence and the profession or area of activity of the person to be identified on the basis of the information received from the person. If a person or customer participating in a transaction entered into in economic or professional activities is a natural person of another contracting state of the European Economic Area or a third country, the obligated person is required to register the information about whether the person performs or has performed any prominent public functions or is a close associate or a family member of a person performing prominent public functions.

502. Such functions are defined in §§ 20 and 21 MLTFPA, stating that 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, or the family members or close associates of such person are not considered a politically exposed person. This time limit of one year is in line with the 3rd EU AML Directive; however, the FATF Recommendations do not provide for such an exception.

503. § 20 (2) MLTFPA provides an exhaustive list of persons who fall for the purposes of this Act under the category "person performing prominent public functions": a head of state, head of government, minister, and deputy or assistant minister; a member of parliament; a justice of a supreme, constitutional or another court the judgments of which can be appealed to only in exceptional circumstances; a member of the supervisory board of a state audit institution or central bank; an ambassador, chargé d'affaires and senior officer of the Defence Forces; a member of a directing, supervisory or administrative body of a state company. Positions within the European Union and other international organisations are also covered by this list (§ 20 (3) MLTFPA).

504. § 20 (4) MLTFPA defines the term "family member of a person performing prominent public functions" as his or her spouse; a partner equal to a spouse under the law of the person's country of residence or a person who as of the date of entry into the transaction had shared the household with the person for no less than a year; his or her children and their spouses or partners, his or her parents.

505. § 30 (4) 1) MLTFPA mandates that an obligated person's rules of procedure shall contain instructions for how to effectively and quickly identify whether or not a customer is a politically exposed person as defined above. § 21 (2) 1) MLTFPA requires that obligated persons, when entering into business relationships with politically exposed persons, shall apply appropriate risk-based internal procedures for making a decision on establishment of a business relationship or entry into a transaction. § 19 (2) 3) MLTFPA also states that such business relationships require enhanced due diligence measures.

506. § 30 (6) indicates that further guidance on this subject shall be issued by the Minister of Finance. Such guidance has not yet been issued, though the Estonian Ministry of Finance has declared it is working on a draft[34].

507. § 21 (2) 2) MLTFPA states that the management board of the obligated person or a person or persons authorised by the management board shall decide on the establishment of business relationships with politically exposed persons as discussed above.

508. § 21 (2) 3) MLTFPA requires obligated persons, upon establishment of a business relationship or entry into a transaction, to take appropriate measures for identification of the origin of the money or other property used.

509. § 21 (2) 4) in connection with § 13 (1) 5) MLTFPA require obligated persons to conduct ongoing monitoring of the business relationship with a politically exposed person.

510. It must be noted that on the implementation side, 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. The larger, internationally active banks generally check one or more of the relevant private-sector databases during their client take-on procedures, which should generate information indicating whether a customer is a politically exposed person.

Additional elements

511. There was initially some confusion regarding the exact wording of the law and whether the requirements of R.6 extended to PEPS who hold prominent public functions domestically. After double-checking the translation, it appears that while the definition of a politically exposed person found in § 20 MLTFPA is worded so as to include domestic politically exposed persons, the special requirements pertaining to politically exposed persons found in § 21 of the law relate only to foreign politically exposed persons. Indeed, it was the clear understanding both of the Estonian authorities and financial sector representatives that domestic politically exposed persons are not covered by the special legal requirements relating to politically exposed persons under the MLTFPA.

512. Estonia did not sign the 2003 United Nations Convention against Corruption[35]. However, the Council of Europe Criminal Law Convention on Corruption (CETS 173) was signed on 8 June 2000, ratified on 6 December 2001 and entered into force on 1 July 2002.

[34] See para 451.

Recommendation 7

513. The banking representatives met by the evaluators stated that due to the highly concentrated banking market in Estonia, there are generally only few correspondent banking relationships directly from Estonian banks, as many of the banks rely on their foreign parent banks for such services, but that the business model of the correspondent banks which do exist were well understood.

514. § 87 (6) of the Credit Institutions Act (CrIA) provides that a correspondent relationship is a legal relationship arising from a contract entered into by credit institutions on the basis of which a credit institution uses an account (correspondent account) at another credit institution (correspondent bank) and in addition to the services offered by the correspondent bank, such account is used by the credit institution for providing services to its customers in its name.

515. Financial institutions in Estonia are required under § 22 (1) MLTFPA to assess, based on public information, the trustworthiness and reputation of the credit institution of the third country and the effectiveness of supervision exercised over the credit institution. This section also stipulates that correspondent banking relationships require the exercise of enhanced due diligence. Estonian authorities explained that § 22 MLTFPA (correspondent banking) is the *lex specialis* to § 18 MLTFPA (simplified CDD). Thus it can be concluded, that § 22 of the MLFTPA limits the application of Enhanced Customer Due Diligence (ECDD) to correspondent banking relationships with institutions from non-EU member countries. § 18 MLTFPA allows to apply simplified CDD in relation to correspondent banking relationships with institutions from EEA member countries (this system of enhanced/simplified CDD for the various situations of correspondent banking was introduced to cover the requirements of the 3rd EU AML Directive[36]). Concerning criterion 7.1 and the requirement to understand the respondent bank's business, Estonian authorities pointed out that it is a general requirement of all obligated persons to acquire information about a business relationship according to § 13 (1) 4) MLTFPA. In addition, it was said that according to § 13 (3) MLTFPA the intensity of such information gathering has to correspond with the risk level of the customer. It was also explained that § 22 (1) MLTFPA requires enhanced due diligence for correspondent banking, which means that an understanding of the correspondent bank's business would be a minimum requirement under the law. However, it has to be noted that these are some elements but overall there is no specific provision in Estonian law which clearly requires understanding the respondent bank's business.

516. § 22 (1) 2) MLTFPA requires that Estonian financial institutions regularly assess the control systems for prevention of money laundering and terrorist financing of the credit institution of the third country.

517. There is no clear legal requirement in Estonian law which mandates prior approval by senior management before establishing new correspondent relationships. It was pointed out by the Estonian authorities that according to Estonian law, legal entities entering into contracts are anyway legally represented by the management board or by a body substituting for same, and that approval is always required if the transaction is made by a person who is not a member of the board. However, from a systemic point of view it has to be noted that § 21 (2) 2) MLTFPA contains a specific provision requiring a decision of the management board in the case of establishing a business relationship with a politically exposed person, which means that the law drafters were aware that certain situations require such an approval. As there is no analogous

[35] The Estonian authorities advised that during 2008 the Ministry of Justice plans to prepare the ratification law to the 2003 United Nations Convention against Corruption.

[36] The shortcomings with regard to the coverage of the these particular requirements are explained in section 7 of the Addendum to this report (MONEYVAL (2008) 32 ADD 1).

provision for correspondent banking relationships in the MLTFPA, this has to be considered as a shortcoming.

518. § 22 (2) 1) MLTFPA requires that the contract for a correspondent banking relationship detail the banks' respective obligations in the "*application of due diligence measures for prevention of money laundering and terrorist financing*". As this clause only addresses AML/CFT with regard to due diligence, other responsibilities of the corresponding institutions, such as notification obligations etc., are not covered. Thus, this provision does not rise to the level at which it would affirmatively require correspondent banks to lay out all of their respective AML/CFT obligations and how and by whom they are to be carried out.

519. Where "payable-through" accounts are being maintained in correspondent banking relationships, § 22 (2) 1) MLTFPA requires that the appropriate due diligence measures have been conducted by the correspondent bank.

520. § 22 (2) 2) MLTFPA requires that the contract for the correspondent banking relationship requires a correspondent bank to be able to submit the data gathered in the course of identification and verification of the customer based on an enquiry.

521. The previous MLTFPA, in § 7 (3), stated that "*in order to establish a correspondent relationship with a foreign credit institution, a credit institution is required to obtain confirmation from the competent body of the host country of the counterparty concerning the legal capacity of and implementation of money laundering prevention measures by the foreign credit institution.*" Due to this previous requirement and the fact that correspondent banking relationships appear to be the exception rather than the norm in Estonia, it appeared that the business models of existing correspondent banks were well understood.

Recommendation 8

522. There are no specific provision in the law which address financial institutions to have policies in place or take such measures as may by needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Estonian authorities are of the opinion that this is indirectly covered by the MLTFPA which requires the obligated entities to establish rules of procedure – § 30 (1) MLTFPA requires that these rules of procedure shall correspond to the sort, scope and complexity of the economic or professional activities of the obligated person. It was pointed out by the Estonian authorities that the degree to which technological means are used in the activities of the obligated person would therefore be one such factor which the rules of procedure would have to address. Again, these rules of procedure, according to § 30 (6) MLTFPA, are supposed to be the subject of guidance from the Minister of Finance in the near future. Apart from the fact, that there is not yet such guidance by the Ministry of Finance, it has to be noted that the presented construction does not clearly cover the requirements of criterion 8.1.

523. § 15 (1) MLTFPA prohibits Estonian financial institutions to open new accounts or first use of another service without a face-to-face identification. § 19 (2) 1) MLTFPA establishes that enhanced due diligence shall be required in regard to business relationships entered into by financial institutions without a face-to-face identification prior to this law coming into effect.

524. § 30 (4) 5) MLTFPA provides that a financial institution's procedure rules have to give guidance on how to effectively and quickly identify whether or not the person is "*a person with whom a transaction is concluded via using means of communications*". Specifics of such requirements will supposedly be set out in guidance from the Minister of Finance provided for in § 30 (6) MLTFPA (see previous paragraph). The financial sector representatives met by the

evaluators seemed generally aware that non-face-to-face business relationships were of high risk. Rather than setting up a particular procedure for handling such a situation, however, most indicated they would much rather require the customer to be present for a face-to-face identification. As far as due diligence subsequent to the initial identification step was concerned, they seemed confident that the measures taken to combat fraud were sufficient to make sure that the counterparty is the person claimed to be. Transactions ordered without face-to-face contact were generally considered as not to be materially different from those ordered in person as far as transaction monitoring was concerned. In addition, § 19 (2) 1) of the MLFTPA says that an obligated person must apply enhanced due diligence measures (further laid out in § 19 (3) MLTPA) if a person or customer participating in a transaction or official act performed in economic or professional activities has been identified and verified without being present at the same place as the person or customer.

525. Overall it needs to be noted that the predominant part of banking and a very large number of other financial transactions in Estonia are apparently conducted electronically. This is apparently considered the norm in the Estonian financial sector.

526. § 62 MLTFPA provides sanctions for financial institution in case of failure to establish rules of procedure for application of due diligence measures.

Sanctioning concerning Recommendations 5 to 8

527. As described below under Rec. 17 in more details (para 678 ff), the MLTFPA does not provide a direct sanctioning regime with administrative sanctions for all of its obligations. Several provisions need to become enforceable via precepts (issued either by the FSA or FIU). While the obligations under Recommendation 8 are fully covered by the (direct) sanctioning regime of § 62 MLTFPA, there remain with regard to Recommendations 5 to 7 a number of criteria of the Methodology which are only covered by an indirect sanctioning regime via precepts:

a) Concerning Recommendation 5, only an indirect sanctioning regime is in place with regard to constant monitoring of a business relationship, regular verification of data, opening anonymous accounts or saving books and some elements of enhanced CDD.
b) With regard to Recommendation 6, it has to be noted that criteria 6.2 to 6.4 (in other words, those elements which are not related to the identification process of PEPs) are only covered via such an indirect sanctioning regime.
c) Recommendation 7 is in its entirety only indirectly sanctioned via precepts.

528. This means of enforcing provisions of the MLTFPA via indirect sanctioning does not amount to a fully dissuasive and effective sanctioning regime as it is not possible to sanction violations which already have happened; it only allows the issuance of precepts (which can be regarded from a practical point of view as being equivalent to warning letters) to sanction future infringements or failure to comply with the demands made in the precept. Moreover, the amount of the sanctions (a fine of up to 50 000 EEK, i.e. 3 195.58 EUR, for the first occasion and 750 000 EEK, i.e. 47 878.53 EUR, for each subsequent occasion) is not proportionate, effective and dissuasive when it comes to the sanctioning of legal persons.

3.2.2 Recommendations and comments

529. The obliged entities are allowed to rely on CDD information received *inter alia* from a credit institution which 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 the MLTFPA are in force. In the absence of further guidance on this issue, the Estonian authorities should at least issue guidance regarding the question of which countries satisfactorily fulfil these requirements.

530. Concerning beneficial ownership, the law leaves some discretion in interpretation as to whether it also covers instances when a natural person acts for another natural person. The Estonian authorities should make it clear in the law that beneficial ownership does not only refer to the first natural person in the chain but that it (also) covers natural persons who ultimately control other natural persons.

531. Concerning criterion 5.6, § 13 (1) 4) MLTFPA requires "*acquisition of information about a business relationship and the purpose of a transaction*". This provision could only indirectly be sanctioned (in that failure to observe these requirements indicates a failure of the institution's internal controls). Estonia should introduce a direct sanctioning regime for this provision.

532. The Estonian approach to address "*high risk of money laundering or terrorist financing*" sets the level to apply enhanced CDD to a higher level than "*higher risk*" in terms of the Methodology. While "high risk" is at the upper end of a level of risk, "higher risk" refers only to a situation more risky than average. Furthermore, in the categories of § 19 MLTFPA non-resident customers and private banking do not appear as higher risk situations which would require enhanced CDD measures. Considering the geopolitical position of Estonia and having a high number of non-resident accounts, Estonia should above all change the term of "high risk" to "higher risk" and consider to add non-resident customers and private banking to the categories which require enhanced CDD measures. Furthermore, the authorities should provide financial institutions with guidance on the existing categories of high risk.

533. § 18 MLTFPA allows for the application of simplified CDD measures in the case of credit or financial institutions located in a contracting state of the European Economic Area or a third country, which in the country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision. At present, no guidance from the Estonian supervisory bodies exists specifying which third countries fulfil these criteria. Though simplified CDD is not mandatory under the Methodology, nonetheless, in applying such a system, the requirements of criterion 5.10 have to be met, which is not the case in Estonia [37].

534. The MLTFPA requires all obligated persons to have rules of procedure which ensure that the legal CDD requirements, as set out in the MLTFPA, are followed. Though not explicitly mentioned, the Estonian authorities are of the opinion that this language also covers all instances in which a business relationship begins prior to full CDD. The Minister of Finance is obliged to issue a decree specifying further requirements for such rules of procedure. Such guidance was not yet in existence at the time of the on-site visit and should be introduced as soon as possible[38].

535. The MLTFPA should clearly require financial institutions to terminate a business relationship and notify the FIU in instances in which a request for additional documentation arising only from ongoing due diligence remains unfulfilled (part of criterion 5.16).

536. The exemption concerning politically exposed persons that "*a person who, by the date of entry into a transaction, has not performed any prominent public functions for at least a year, or the family members or close associates of such person are not considered a politically exposed person*" (§ 20 (1) MLTFPA) is not in line with the Methodology and should be removed.

537. Concerning effective implementation of Rec. 6, at least one of the smaller local banks did not, at the time of the on-site visit, conduct independent background checks on their customer's possible role as a politically exposed person (in contrast to the larger, internationally active banks

[37] A list of equivalent third countries has subsequently been established; see para 451.

[38] The relevant Regulation of Minister of Finance was published in the State Gazette and became effective on April 11, 2008; see para 451.

which seem to follow their obligations). The Estonian authorities should address this shortcoming by focused supervision on these issues and consider issuing guidance in this regard.

538. While § 22 (1) MLTFPA requires the application of enhanced due diligence vis-à-vis correspondent banks, there should be a clear requirement in the law which obliges financial institution to understand the respondent bank's business.

539. Estonia should introduce a clear legal requirement for financial institutions to obtain approval from senior management before establishing new correspondent relationships.

540. In case of correspondent banking, financial institutions should be required to document not only the respective CDD responsibilities of each institution but the whole range of AML/CFT responsibilities (e.g. notification).

541. Estonia should introduce specific provisions in the law which address the risk of misuse of technological developments in money laundering or terrorist financing schemes.

542. Regarding effectiveness, it should be noted that a substantial part of the legal requirements of the MLFTPA were already in force under the previous AML Act and that the private sector representatives met were well aware of where the new requirements went beyond the old ones. It therefore appeared that the new requirements were being effectively addressed.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**LC**	• The obliged entities are allowed to rely on CDD information received *inter alia* from a credit institution which has been registered or whose place of business is in a country (outside the European Economic Area) where requirements equal to those provided in the MLTFPA are in force. There is no guidance available for financial institutions on which countries satisfactorily fulfil these requirements. • Concerning beneficial ownership, the language in the law is not clear as to whether it also covers instances when a natural person acts for another natural person. • The Estonian approach to address "*high risk of money laundering or terrorist financing*" sets the level to apply enhanced CDD measures to a higher level than "*higher risk*" in terms of the Methodology. The categories which require enhanced CDD measures seem insufficient and there is also no guidance on the existing categories. • The MLTFPA allows for the application of simplified CDD measures in case of credit or financial institutions located in a contracting state of the European Economic Area or a third country, which in the country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision. At present, no guidance from the Estonian supervisory bodies exists specifying which third countries fulfil these criteria. • There is not yet guidance from the Minister of Finance specifying the requirements for rules of procedure of the obliged entities dealing with situations in which a business relationship begins prior to full CDD. • The MLTFPA does not require termination of the business relationship in instances in which a request for additional documentation arising only from ongoing due diligence remains unfulfilled.

R.6	**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. • 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).
R.7	**PC**	• There is no specific provision in Estonian law which explicitly requires understanding the respondent bank's business. • There is no clear legal requirement to obtain approval from senior management before establishing new correspondent relationships. • 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.
R.8	**PC**	• There are no specific provision in the law which address financial institutions to have policies in place or take such measures as may by needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

3.3 Third Parties and introduced business (R.9)

3.3.1 Description and analysis

543. § 7 (1) of the previous MLTFPA allowed Estonian financial institutions to rely on certain, exhaustively listed third parties, consisting of other financial institutions, law offices, notary offices and auditing firms, provided the other party was listed in the commercial register of Estonia or operating in another member state of the European Union or in a country where equivalent requirements apply for the prevention of money laundering and the identification of clients.

544. Under the current law, the obligated persons are entitled to rely on "*information received by the obligated person in a format which can be reproduced in writing from a credit institution or from a branch of a foreign credit institution registered in the Estonian commercial register or from a credit institution who 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*" (§ 14 (4) MLTFPA). This provision follows the requirements of Art. 15 ff of the 3rd EU AML Directive (2005/60/EC).

545. Estonian obligated persons are not entitled to rely on another parties' statement of having gathered information to a particular effect. Rather, § 14 (4) MLTFPA entitles only to rely on information already received. It was clearly understood by representatives of the Estonian financial sector that being told that a potential customer had been identified by such a third party was insufficient and that rather it was legal to rely on the particular identification information received as long as the additional requirements of § 14 (4) were met.

546. § 14 (4) MLTFPA allows reliance only on such information which "*can be reproduced in writing*". However, there is no clear requirement for obligated persons to ensure that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay. It was pointed out in discussions with

Estonian authorities that the reliance is based on the mutual recognition duty arising from Art. 15 of the 3rd EU AML Directive (2005/60/EC), which should also apply to the institution relied upon and, in Art. 18 para 1 of the Directive, requires that such information be made "*immediately available*" upon request. As the 3rd EU AML Directive is not directly applicable in Estonian law, this construction cannot be considered as covering this issue. Estonia pointed out that in practice credit institutions exchange information electronically as scanned attachments of the original documents; it makes it possible to make different documents available immediately and reproduce them in writing.

547. To be complete in the context of criterion 9.2, it is also worth referring to § 28 (2) 6) MLTFPA which requires that "*the documents and data collected for fulfilment of the requirements arising from this Act are preserved pursuant to the procedure provided for in this Act*" by the person to whom activities are outsourced. However, as this provision deals with outsourcing activities, it does not fall under Recommendation 9.

548. § 14 (4) MLFTPA states that an obligated person has the right to rely on information received, from a credit institution as long as it is satisfied that the other person has fulfilled similar requirements as are necessary under the MLFTPA.

549. In the same way as the requirements of the MLFTPA regarding Recommendations 5 and 10 fall short of the recommendations, criterion 9.3 also falls short of the recommendations. This only has an effect regarding Rec. 10 (in the context of Rec. 9), as Estonian obligated persons' reliance is limited to the ability to produce the documents in question. As far as reliance on a third party for the identifying information is concerned, that information must actually be received by the obligated person in question, as according to § 14 (4) MLTFPA it can only then rely on the documentation gathered by the third party.

550. Concerning criterion 9.4 and reading § 14 (4) MLTFPA (see para 544 above), it can be concluded that the law drafters considered that all contracting states of the European Economic Area met the requirements of Recommendation 9. There is no mechanism to exclude certain states from this blanket assessment, and indeed Art. 15 of the 3rd EU AML Directive (2005/60/EC) appears to prevent Estonia from implementing one. Regarding other countries which may have established sufficient controls, the MLTFPA does not indicate which countries these could be, and there has been no guidance on this question to date. Financial sector representatives met by the evaluators were waiting for guidance on this issue[39]. The lack of guidance available at the time of the on-site visit creates a concern that legal requirements of the new law may not be optimally put into practice.

551. The Estonian authorities explained that the financial institutions' obligation to identify and verify a customer is based on public law and that the obligations based on public law can be delegated only if expressly provided in law. Thus, they consider that a financial institution is always responsible for fulfilling its obligations provided in public law. However, it appears as though § 14 (4) MLTFPA creates a situation in which an obligated person is entitled to rely on a third party, thereby removing the relying person's ultimate responsibility, though only to the degree in which its own duties under the legal due diligence requirements were met.

552. The MLTFPA does not provide a direct sanctioning regime with administrative sanctions for all of its obligations. This is also the case for those provisions of the MLTFPA covering Recommendation 9. This way of enforcing provisions of the MLTFPA via indirect sanctioning does not amount to a dissuasive, proportionate and effective sanctioning (for details see below under Rec. 17 where this indirect sanctioning regime and its shortcomings are described in more details; para 678 ff).

[39] See FN 30.

3.3.2 Recommendation and comments

553. § 28 MLTFPA provides for the ability of obligated persons to outsource some of their activities. Inasmuch as parts of the identification or customer due diligence procedure are outsourced, the above requirements do not apply (nor does Recommendation 9, see Fn 15 of the Methodology). Several representatives of financial institutions met by the evaluators indicated that where they had often relied on particular third parties in the past, they would now enter into an outsourcing agreement with these parties. The Estonian authorities, when questioned on this strategy, indicated that this was considered acceptable, as the respective financial institutions would shift the immediate responsibility for satisfying CDD requirements onto themselves in exchange for a reduced requirement regarding oversight of the third party.

554. Concerning criterion 9.2, the MLTFPA only allows reliance on such information which "*can be reproduced in writing*". However, there is no clear requirement for obligated persons to ensure that timely reproduction is possible (the construction via obligations arising of the 3rd EU AML Directive cannot be regarded as covering this issue). Financial institutions should be required to produce the necessary documentation without delay.

555. Concerning criterion 9.4, all contracting states of the European Economic Area are considered under the MLTFPA to meet the requirements of Recommendation 9. The same applies for third countries where requirements equal to those provided in the MLTFPA are in force. The Estonian authorities should issue guidance to clarify which countries meet these criteria.

556. 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. The Estonian authorities should clarify that also in the circumstances of § 14 (4) MLTFPA the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

557. The MLTFPA does not provide a direct sanctioning regime with administrative sanctions for all of its obligations. This is also the case for those provisions of the MLTFPA covering Recommendation 9. This method of enforcing provisions of the MLTFPA via indirect sanctioning does not amount to a dissuasive, proportionate and effective sanctioning Estonia should also provide for the provisions of the MLTFPA addressing Recommendation 9 a direct sanctioning regime (the easiest way to do so would be to provide in the MLTFPA sanctions for these requirements of the Act itself).

558. Due to the very limited nature of allowed reliance on third parties according to § 7 (1) of the previous MLTFPA, it appears as though the private sector practice in this regard at the time of the on-site visit does not create an additional effectiveness problem beyond the findings outlined above.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**LC**	• There is no clear requirement for obligated persons to ensure that timely reproduction of the necessary documentation from third parties is possible. • Concerning criterion 9.4, there has been no guidance issued by the Estonian authorities to advise financial institutions on 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. • 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 a third party.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and analysis

559. § 88 (1) Credit Institutions Act (CrIA) requires the Estonian credit institutions to guarantee the confidentiality of customers' data; all data and assessments which are known to a credit institution concerning the customers of the credit institution are deemed to be information subject to banking secrecy. § 3 of the CrIA defines a credit institution as "*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*". According to its § 2 (1) and (2), the CrIA applies to all credit institutions founded or operating in Estonia and to parent companies, subsidiaries, branches and representative offices thereof which are located in Estonia; it also applies to subsidiaries, branches and representative offices of Estonian credit institutions in foreign states, unless otherwise prescribed by the legislation of the state where they are registered, and to subsidiaries, branches and representative offices of foreign credit institutions in Estonia, unless otherwise provided by international agreements entered into by Estonia. This means in practice that the CrIA applies to seven locally licensed credit institutions, eight branches of foreign credit institutions and a number of providers of cross-border banking services.

560. Unauthorised disclosure of information which is subject to banking secrecy may entail criminal sanctions (§ 157 PC) or misdemeanour sanctions (§ 134^{10}CrIA). § 157 PC ("Violation of obligation to maintain confidentiality of secrets which have become known in course of professional activities") reads as follows:

> *Disclosure of information obtained in the course of professional activities and relating to the health, private life or commercial activities of another person by a person who is required by law to maintain the confidentiality of such information is punishable by a pecuniary punishment.*

561. § 134^{10}CrIA ("Violation of obligation to maintain confidentiality of information subject to banking secrecy") stipulates:

> *(1) A head or employee of a credit institution, or any other person acting in the interests of a credit institution, who unlawfully discloses information subject to banking secrecy shall be punished by a fine of up to 300 fine units.*
> *(2) The same act, if committed by a legal person, is punishable by a fine of up to 50 000 EEK.*

562. There are some circumstances in which confidentiality obligations may be lifted. § 88 (5) CrIA requires a credit institution to disclose information subject to banking secrecy to the Bank of Estonia and the FSA for the performance of their duties; this provision obliges a credit institution to disclose information subject to banking secrecy amongst others also to

- a court or, in the cases prescribed by law, a person specified in a court ruling;
- a pre-trial investigation authority and the Prosecutor's Office if a criminal proceeding is commenced, and on the basis of a request for legal assistance received from a foreign state pursuant to the procedure provided for in an international agreement;

- a foreign financial supervision authority or other financial supervision authority through the Financial Supervision Authority if the obligation to maintain the confidentiality of information subject to banking secrecy extends to such authority;
- a depositary of declarations of economic interests for the verification of the correctness of the data submitted in a declaration of economic interests of a person specified in § 4 of the Anti-corruption Act in the case of suspicion of corruption.

563. Credit institutions are required to provide their information in a format which can be reproduced in writing. A request for information should set out the legal grounds for it and has to be proportional with the objectives of the inquiry. Persons to whom information subject to banking secrecy has been disclosed may use such information only for the purpose specified in the request; the obligation to maintain the confidentiality of such information is indefinite.

564. In accordance with § 88 (8) CrIA, credit institutions have the right and obligation to disclose information subject to banking secrecy to the FIU and the Security Police Board in the cases and to the extent prescribed in the MLTFPA.

565. Similar confidentiality requirements apply to *insurance companies*. Managers and employees of insurance undertakings, persons acting on the authorisation or orders of such persons are required to maintain, during and after their employment or operation and for an unspecified term, the confidentiality of all information which becomes known to them and which concerns the economic status, state of health, personal data or the business or other professional secrets of policyholders, insured persons or beneficiaries, unless otherwise prescribed by law (§ 54 (3) Insurance Activities Act). § 207 of the Insurance Activities Act ("*Violation of confidentiality requirement*") provides administrative liability of insurers in case of breaches of confidentiality obligations:

> *(1) Violation of the confidentiality requirement provided for in this Act by the manager or an employee of an insurance undertaking or intermediary or other person acting in their interests is punishable by a fine of up to 300 fine units.*
> *(2) The same act, if committed by a legal person, is punishable by a fine of up to 50 000 EEK.*

566. In order to exercise supervision, the Financial Supervision Authority has the right to demand information, documents and oral or written explanations without charge concerning facts which are relevant in the exercise of supervision from insurance undertakings (§ 170 IAA).

567. Apart from the exemptions from financial secrecy stipulated by § 88 CrIA (see above para 562 ff), the MLTFPA contains a more general provision for the FIU to access information subject to financial secrecy: According to § 41 MLTFPA, the FIU has the right to receive information from the FSA or state and local government authorities and - on the basis of precepts – also from obligated persons regarding the circumstances, transactions or persons related to suspicion of money laundering or terrorist financing. The addressee of a precept is required to comply with the precept and to submit the requested information "*including any information subject to banking or business secrecy"* during the term prescribed in the precept. The information has to be submitted orally, in writing or in a format which can be reproduced in writing (§ 41 (2) MLTFPA).

568. Concerning provisions for other bodies, e.g. courts, prosecutors, police etc., which allow them to access information subject to financial secrecy, the Estonian authorities explained that there are also provisions for these authorities to access directly such information. It was said that these bodies have the same powers as the FIU when criminal investigations have been started and that in practice they do not use the FIU to access this information indirectly (which would in principle be possible, see below para 573). Concerning the powers of the prosecutors and investigative bodies, Estonian authorities referred to § 215 CCP which reads as follows:

§ 215. Obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices
(1) 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.
(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.
(3) A preliminary investigation judge may impose a fine of up to sixty minimum daily rates on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a Prosecutor's Office. The suspect and the accused shall not be fined.

569. The Estonian authorities referred also to § 32 (2) CCP, which stipulates that an investigative body has the right to demand submission of a document necessary for the adjudication of a criminal matter. In cases where the demanded information or documents are not presented, the investigative bodies and Prosecutors' Office have according to § 91 CCP the right to conduct a Search (§ 91(1): *The objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, property to be seized for the purposes of compensation for damage caused by a criminal offence, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area*).

570. The Estonian authorities told the evaluation team that these provisions can be and are used in practice for all kind of orders of investigative bodies, courts and prosecution services unless it is against legal provisions. It was also mentioned that § 215 CCP to be applicable in the context of Recommendations 3 and 28, and, thus, should also provide a legal basis to request information which is subject to financial institution's secrecy from financial institutions. Reportedly, so far no problems have occurred with these provisions and obliged entities follow these orders. However, the evaluation team has some doubts concerning the overall applicability of these provisions as they seem to be only enforcement provisions for powers of prosecutors, courts and investigative bodies concerning their powers which have to be determined in other provisions. Without authorisation in specific provisions, there seems to be no applicability for these provisions. To sum up, it may be possible to enforce an existing obligation with these provision but they cannot provide per se a legal basis for something which is not regulated somewhere else (particularly when there are even provisions which do not allow for such a procedure, such as financial institution's secrecy provisions). However, considering that there is apparently no problem in practice and, moreover, the (legal well grounded) possibility for these bodies to access this information in an indirect way via the FIU, this legal uncertainty can be left aside in the context of this report.

571. The FIU has also the right to receive *from third parties* information for identification of circumstances which are of relevance in the prevention of money laundering or financing of terrorism (§ 41 (4) MLTFPA). The explanatory memorandum of the MLTFPA explains in this regard that "*the FIU has the right to obtain information from third parties with regard to whose activities there is no suspicion of illegality, but who have information about the circumstances which have a meaning for the purpose of prevention of money laundering or terrorist financing. Among other things, the FIU has the right to demand accounting documents on any data medium from a third party whose connection with the transactions under investigation becomes evident in the course of the checks*".

572. In order to perform its functions, the FIU also has the right to make enquiries to and to receive data from state and local government databases and databases maintained by persons in public

law, pursuant to the procedure provided by legislation (§ 42 MLTFPA). For further details and the access of the FIU to various databases see above section 2.5 of the report.

573. The MLTFPA provides that only officials of the FIU shall have access to and the right to process the information in the FIU database. In order to prevent or identify money laundering, financing of terrorism or other criminal offences related thereto and in order to facilitate pre-trial investigation thereof, the FIU is obligated to forward significant information, *including information subject to tax and banking secrecy* to the prosecutor, the investigative body and the court. This can be done upon a written request by the respective body or on the initiative of the FIU (§ 43 (2) MLTFPA).

574. § 34 (3) MLTFPA stipulates that the duty of confidentiality may be lifted between financial institutions solely for the purpose of prevention of money laundering and financing of terrorism (Para 4) in the following 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 or management or internal control system as the obligated person in 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 who 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."*

575. Though arguably § 34 (3) MLTFPA allows, in a number of situations, the sharing of information between financial institutions where this is required by R. 7 (correspondent banking), R. 9 (third parties and introducers) and SR VII (wire transfers), one has to say that the provision itself is drafted in a complicated way and also leaves some discretion and uncertainty in interpretation: e.g. § 34 (3) item 1 requires that the financial institution has to belong to the "*same consolidation group or financial conglomerate*" but nowhere is it described what is covered by this expression; furthermore, there is also no specification in the law and no guidance has been issued about which countries can be considered as equivalent to "*a contracting state of the European Economic Area"*[40]. Furthermore, the phrase "*joint owners and management*" may be difficult to interpret when this requirement is fulfilled with regard to stock companies. The Estonian authorities advised in the course of the pre-meeting that the phrase "*joint owners and management*" is not the best translation. Instead § 34 (3) 1) MLTFPA should be translated "*the third party acts in the same legal person or structure, which has joint same owners and management or internal control system as the obligated person in the profession of a notary public, attorney or auditor*". Nonetheless, it has also to be noted that this amended translation causes the same concerns. To sum up, it has to be noted that this provision is drafted in a complicated way which will make it difficult for practitioners to establish whether all

[40] See FN 30

requirements are fulfilled and it is allowed to exchange information. Concerning the language of this provision, the Estonian authorities referred to § 28 of the 3rd EU AML Directive which was said to require these elements. However, it has to be noted that § 28 of the 3rd EU AML Directive is more clear in this respect (particularly what has to be understood under "*belonging to the same group*" by cross-referencing to Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002[41]) and (as far as the Estonian legal provisions can be interpreted) also seems to provide different (less) restrictions concerning information sharing between financial institutions.

576. Regarding the exchange of information among financial supervisors, see Chapter 6.1 (domestic exchange of information) and Chapter 6.5 (international exchange of information).

3.4.2 Recommendations and comments

577. 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 access information which is subject to financial secrecy.

578. The provisions allowing the sharing of information between financial institutions, where this is required by R. 7, R. 9 and SR VII, should be revised: the language should be simplified to facilitate their application in practice and further guidance should be provided[42].

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**LC**	• The provisions allowing the sharing of information between financial institutions where this is required by R. 7, R. 9 and SR VII are drafted in a complicated way and leave some discretion and uncertainty in interpretation which may hamper their practical application.

[41] i.e. "*'group' shall mean a group of undertakings, which consists of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 12(1) of Directive 83/349/EEC*".

[42] This has already been done to a certain extent concerning countries which can be considered as equivalent to "*a contracting state of the European Economic Area*"; see FN 30.

3.5 Record keeping and wire transfer rules (R.10 and SR.VII)

3.5.1 Description and analysis

Recommendation 10

579. Recommendation 10 has numerous criteria under the Methodology which are asterisked, and thus need to be required by law or regulation. Financial institutions should be required by law or regulation:

- to maintain all necessary records on transactions, both domestic and international, for at least five years following the completion of the transaction (or longer if properly required to do so) regardless of whether the business relationship is ongoing or has been terminated;
- to maintain all records of the identification data, account files and business correspondence for at least five years following the termination of the account or business relationship (or longer if necessary) and the customer and transaction records and information;
- to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority.

580. According to § 26 (2) MLTFPA, an obligated person shall preserve the documents prepared with regard to any transaction (domestic or international) on any data medium and the documents and data serving as the basis for the notification obligations for no less than five years after entry into the transaction or performance of the notification obligation. The law does not require longer storage if requested by a competent authority. However, the financial sector representatives met by the evaluators indicated that they would certainly comply with any such requests made by the FIU. § 12 of the previous MLTFPA also required that "*Credit and financial institutions and persons specified in subsection 5 (1) of this Act shall preserve data specified in § 11 for at least five years after the end of a contractual relationship with a client*".

581. Transaction record documentation obligations, according to § 26 (2) in connection with § 32 (1) and (2) MLTFPA, extend only to the documentation required to notify the FIU or transactions the obligated person finds which are possibly indicative of money laundering or terrorist financing. According to Guidance Notes, such information may include the beneficial owner of the account, the volume of funds flowing through the account, the origin of the funds (if known), the form in which the funds were placed or withdrawn, i.e. cash, cheques etc., the identity of the person undertaking the transaction, the destination of the funds and the form of instruction and authority. In addition, the required information under EC Regulation 1781/2006 also falls under the documentation obligation, as this regulation is directly applicable in Estonia.

582. The financial sector representatives met by the evaluators indicated that their institutions generally keep *all* their available data for a minimum of five years, without regard to the likelihood of any particular data being of interest at some point in the future. This was widely considered to be a legal requirement.

583. The MLTFPA requires in § 26 (1) that an "*obligated person shall preserve the original copies or copies of the documents specified in §§ 23 and 24, which serve as the basis for identification and verification of a person, and the documents serving as the basis for establishment of a business relationship no less than five years after termination of the business relationship*". § 26 (2) of the law extends that requirement to storing such data "for no less than five years after entry into the transaction or performance of the notification obligation". This indicates that any information given to the FIU by the obligated person will have to be stored for an additional five years after the notice was made, irrespective of the date on which the obligated person first documented the information therein.

584. According to § 26 (3) MLTFPA, an "*obligated person shall preserve the documents and data specified in sections (1) and (2) in a manner which allows for an exhaustive and immediate reply to enquiries received from the Financial Intelligence Unit or other investigative bodies or a court pursuant to legislation*".

Special Recommendation VII

585. The Methodology concerning SR VII requires for all wire transfers, that financial institutions obtain and maintain so-called "full originator information" (i.e. name of the originator; originator's account number; or unique reference number if no account number exists) and the originator's address (though countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth) and to verify that such information is meaningful and accurate. Full originator information should accompany cross-border wire transfers, though it is permissible for only the account number to accompany the message in domestic wire transfers.

586. As a member of the European Union, Estonia is bound by EC Regulation 1781/2006 of the European Parliament and the Council on information on the payer accompanying transfers of funds which was adopted on 15 November 2006 and came into force on 1 January 2007. This EC Regulation meets all the requirements of SR VII (as described above in para 585): obtaining and verifying originator information; maintaining full originator information for cross-border transfers; accompanying domestic wire transfers with more limited originator information and making full originator information available within three days; adopting specific procedures for identifying and handling wire transfers not accompanied by full originator information; compliance monitoring; and sanctions. There is one particularity of this EC Regulation as it classifies wire transfers within the EU as domestic and therefore requires only limited originator information on wire transfers within the European Community. While this was a while under consideration, the revised Interpretative Note to SRVII issued by the FATF on 29 February 2008 makes it now clear that the term "*domestic transfer*" also refers to any chain of wire transfers that takes place entirely within the borders of the European Union (revised IN to SR VII paragraph 2, letter c).

587. However, for the EU Regulation to become effective, an appropriate domestic monitoring enforcement and penalties regime needs to be implemented and the competent authorities should be given the power to impose penalties for its infringement as from 15 December 2007 (see Articles 15 and 20 of the Regulation). In addressing these requirements, § 63 of the MLTFPA provides for sanctions in the case of a violation of Regulation (EC) No. 1781/2006 by a manager or employee of a payment service provider: a violation of the obligations imposed by the Regulation by a payment service provider is punishable with a fine up to 300 fine units à 60 EEK (i.e. 18 000 EEK; 1150.40 EUR) and, if the infringement is committed by a legal person, then the fine goes up to 500 000 EEK. It is noted that § 63 MLTFPA speaks about infringements only by "*payment service providers*", but not of credit institutions and currency exchange bureaux; though, Estonian authorities advised that, according to the licensing requirements, credit institutions are considered as "payment service providers" and therefore subject to the regulation of § 63 MLTFPA (and of the Regulation (EC) No. 1781/2006).

588. With regard to the level of awareness and implementation of Regulation (EC) No. 1781/2006, credit institutions have been informed of its existence by the Estonian Banking Association (EBA). The FSA and FIU published the regulation on their websites, but did not issue a circular to inform credit institutions and payment service providers of their obligations arising from the Regulation. It seems that current supervisory tools used by the FSA and the FIU do not encompass the monitoring of compliance with the Regulation by both credit institutions and other financial business entities involved in money remittances. Estonian authorities advised that the EBA has been actively involved both during the consultation process of the draft Regulation and in the process of preparation of implementation of Regulation (EC) No. 1781/2006 and that the draft

Regulation and the approved Regulation were distributed by the EBA to all the member banks in due course. Additionally, representatives of the EBA (members of Estonian Committee at EBA responsible for clearing and settlement issues) were involved in discussions in the European Payments Council (EPC) on 7 March 2007 and 4 June 2007. The Guidance Notes of implementation of the regulation issued by the EPC were distributed to all the member banks in due course by the EBA. Estonian authorities also advised that the problems arisen in connection of implementation have been discussed in the EBA AML Committee (which consists of the AML compliance officers of all credit institutions and the representatives from FSA and FIU) on 11 October 2007 and 9 January 2008[43].

589. Additionally, the EBA has asked the Ministry of Finance for written guidance for implementation of the regulation and the adequate instructions were given to EBA on 10 September 2007 and on 11 December 2007.

3.5.2 Recommendation and comments

590. The MLTFPA (particularly § 63) needs to be amended
- that sanctions also apply to credit institutions and currency exchange bureaux when they breach the provisions of the said Regulation.

591. Further measures need to be taken to ensure full awareness of by credit institutions and payment service providers of the requirements of Regulation (EC) No 1781/2006. Moreover, both the FSA and the FIU should elaborate an appropriate monitoring mechanism to ensure its proper implementation.

592. Neither the FSA nor the FIU have informed credit institutions and payment service providers of their obligations arising from Regulation (EC) No. 1781/2006. For the sake of a proper implementation of this EU Regulation (and consequently SR VII), it is necessary to raise awareness with its requirements concerning fund transfers. Furthermore on-site inspections and other off-site monitoring techniques should aim at ascertaining and evaluating implementation of this EU Regulation by credit institutions and payment service providers. The supervisory tools used by the FSA and the FIU should encompass the monitoring of compliance with the EU Regulation by both credit institutions and other financial business entities involved in money remittances.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**LC**	• There is no requirement in law or regulation to keep documents longer than five years if requested by a competent authority.
SR.VII	**LC**	• There is no proper monitoring of Regulation (EC) No. 1781/2006 which is aimed to cover the requirements of SR VII.

[43] The Estonian authorities advised that after the on-site visit, further meetings have taken place (on 30 April 2008 and 12 June 2008).

Unusual and Suspicious Transactions

3.6 Monitoring of transactions and relationships (R.11 and 21)

3.6.1 Description and analysis

Recommendation 11

593. § 12 (1) MLTFPA stipulates that "*in economic or professional activities or professional practice an obligated person shall pay special attention to [...] complex, high value and unusual transactions which do not have reasonable economic purpose*".

594. The FSA has also issued guidance on these issues to be implemented from 1 August 2002 onwards. This guidance indicated that particular attention should be paid to suspicious or unusual transactions. It is planned that additional guidance by the Minister of Finance in the form of secondary, binding and sanctionable law will address the internal procedures required of financial institutions regarding their AML/CFT obligations. It was indicated that such guidance was being drafted by the Ministry of Finance, though no draft was available for the inspection of the evaluators.

595. The FIU had undertaken training lessons with financial sector representatives who indicated to the evaluators that such measures are routinely in place in Estonian financial institutions, particularly in the larger, foreign-owned banks.

596. Concerning criterion 11.2, the Estonian authorities pointed to § 25 MLTFPA of which certain elements should cover this issue:

> *"(2) A credit and financial institution shall register the following data about a transaction: […]*
> *7) in the case of the payment mediation service, the data the communication of which is compulsory under Regulation (EC) No. 1781/2006 of the European Parliament and Council on information on the payer accompanying transfers of funds; 8) in the case of provision of services of alternative means of payment, the name of the payer and recipient, the personal identification code, and upon absence thereof, the date and place of birth or a unique feature on the basis of which the payer can be identified; 9) in the case of another transaction, the transaction amount, the currency and the account number.*

597. The Estonian authorities also referred in this context to § 30 MLTFPA which specifies the requirements of the rules of procedure which the obligated persons have to establish: § 30(1) MILTFPA requires obligated person to establish internal rules of procedures for the application of due diligence measures at least in the events specified in § 13(1) MLTFPA (which deals with due diligence measures). Furthermore § 30 (1) MILTFPA requires that the internal rules of procedure shall correspond to the sort, scope and complexity of the economic or professional activities of the obligated person. § 30(4) MILTFPA requires that the rules of procedure shall contain instructions on how to effectively and quickly identify whether or not the person is, among others, a person whose place of residence or seat is in a country where no sufficient measures for prevention of money laundering and terrorist financing have been applied. Furthermore, § 30 (3) (3) requires that the rules of procedures shall describe transactions of a higher risk level and establish the appropriate requirement for entering into and monitoring such transactions. Finally, § 30(6) provides that the Minister of Finance shall issue a regulation setting the requirements for the rules of procedure established by credit and financial institutions. This regulation (Minister of Finance Regulation No 10 of 3 April 2008), sets out in § 3 (2) that internal codes of conduct must contain "*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, and procedures for ongoing monitoring of business relationships".

598. However, it needs to be noted that the obligations stipulated by § 25 MLTFPA describe what obliged entities have to do in case of certain transactions. This is not necessarily the same as required under criterion 11.2, which prescribes that financial institutions should be required to examine "*as far as possible the background and purpose of such transactions and to set forth their findings in writing*". None of the provisions mentioned above stipulate such examination requirements as set out by Recommendation 11. As a consequence there are no corresponding requirements to set forth these findings in writing and to keep them for a certain period. The only provision, which could be considered to address this issue can be found in § 26 (1) of the MLTFPA, which stipulates that an "*...obligated person shall preserve the original copies or copies of the documents ... which serve as the basis for identification and verification of a person, and the documents serving as the basis for establishment of a business relationship no less than five years after termination of the business relationship*". However, this provision relates only to the usual record keeping provisions with regard to the CDD obligations of the obligated entities but has nothing to do with the special requirements of Recommendation 11 dealing with complex, unusual large transactions of which the background and purpose should be examined in as much detail as possible.

Recommendation 21

599. Recommendation 21 requires financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not, or insufficiently apply the FATF Recommendations. This should be required by law, regulation or by other enforceable means. It places an obligation on financial institutions to pay close attention to transactions with persons from or in any country that fails or insufficiently applies FATF Recommendations and not just countries designated by FATF as non-co-operative (NCCT countries).

600. The legal situation concerning the coverage of Recommendation 21 is that there are some general provisions on record keeping and customer due diligence but no provisions specifically addressing the requirements of Recommendation 21[44]. Estonia has indicated that § 13 (2) of the MLFTPA requires foreign branches of Estonian banks to apply measures at least equal to those required under the MLFTPA and also seeks to rely on its rules on correspondent banking. Rec. 21 focuses on customer relationships, however. There is no requirement in law, regulation or other enforceable means to be particularly security-conscious when dealing with business from certain countries, nor is there guidance which countries should be treated with particular care.

[44] In addition it has to be noted that the Minister of Finance proceeded, under § 30(6) MLTFPA, with the issue of Regulation No.10 on 3 April 2008 setting out the "Requirements for the rules of procedure established by credit and financial institutions and for their implementation and verification of compliance". This Regulation requires credit and financial institutions to establish written rules of AML/CFT procedures which should include *inter alia* a code of conduct for the application of CDD measures. The said code of conduct must contain the credit or financial institution's requirements, for the identification and verification of its customers, including "*business relationships with persons whose place of residence or registered office is in a country where the application of AML/CFT measures is insufficient*". The Regulation also specifies (§§ 8 and 9) that for the identification and verification of legal persons, a credit or financial institution's CDD measures must provide requirements for business relationships with customers "*whose registered office is in a third country that has not implemented sufficient AML/CFT measures or where this country has not engaged in international cooperation for AML/CFT purposes*". However, as noted above (para 451), this Regulation was not taken into account in the descriptive part and for rating purposes as financial institutions have to comply with it not before 1 November 2008.

3.6.2 Recommendations and comments

601. Financial institutions should be required by law, regulation or other enforceable means to investigate the background and purpose of complex/unusual large transactions and to keep a record of the written findings which will be then accessible for competent authorities and auditors.

602. The existing legal provisions do not adequately address the requirements of Recommendation 21. Credit and financial institutions are not explicitly required to give special attention to business relationships and transactions with persons from countries which do not or insufficiently apply FATF recommendations. The existing legal and regulatory framework contains general requirements regarding business relationships and transactions with persons from countries which insufficiently apply FATF recommendations and does not adequately cover the essential criteria of R.21. Furthermore, there are no requirements with regard to possible measures for advising credit and financial institutions of concerns and weaknesses in the AML/CFT systems of other countries (criterion 21.1.1), the investigation of unusual transactions (criterion 21.2) and the application of counter measures against countries with deficient AML/CFT systems (criterion 21.3).

3.6.3 Compliance with Recommendations 11 and 21

	Rating	Summary of factors underlying rating
R.11	**PC**	• Financial institutions are not required to examine the background and the purpose of complex/unusual large transactions and thus to keep a record of the written findings which will be accessible for competent authorities/auditors.

R.21	**NC**	• There are no obligations in law or regulation or other enforceable means requiring financial institutions to
		  • give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations.
		  • to examine and monitor such transactions, if they do not have an apparent economic or visible lawful purpose, and have written findings available to assist competent authorities and auditors.
		• There are no specific provisions on application of counter-measures where a country continues not to apply or insufficiently applies the FATF Recommendations.

3.7 Suspicious transaction reports and other reporting (R. 13, 14, 19, 25 and SR.IV)

3.7.1 Description and analysis

Recommendation 13

603. § 32 MLTFPA sets out the reporting requirements for financial institutions when a suspicion of money laundering or terrorist financing arises: "*If, upon performance of economic or professional activities or when carrying out an official act, an obligated person identifies an activity or circumstances which might be an indication of money laundering or terrorist financing 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 notify the Financial Intelligence Unit thereof*" (para 1). This clause makes it clear, that the reporting requirement is

triggered either by a suspicion of money laundering or when there is a suspicion of terrorist financing (subject to the concerns set out in para 619 below); furthermore, all offences required to be included as predicate offences under Recommendation 1 are covered. All suspicious transactions, regardless of the amount of the transaction, are required to be reported.

604. According to § 32 (5) MLTFPA, an obligated person has the right to postpone a transaction or official act when there is a requirement to file an STR. However, if the postponement of a transaction may cause considerable harm, the transaction has to be executed. The transaction or official act shall also be carried out if postponing the transaction may impede catching the person who is possibly committing money laundering or terrorist financing; in such a case, the FIU shall be notified thereafter.

605. § 60 MLTFPA provides for sanctions both for natural and legal persons in the case of failure to report an STR to the FIU:

> *"Violation of the obligation to notify the Financial Intelligence Unit of suspicion of money laundering or terrorist financing, currency exchange transaction or another transactions whereby the financial obligation exceeding 500 000 EEK or an equal amount in another currency is performed in cash or submission of incorrect information by the manager, contact person or another employee of an obligated person is punishable by a fine of up to 300 fine units or detention.*
> *(2) The same act, if committed by a legal person, is punishable by a fine of up to 500 000 EEK."*

606. It is remarkable that, in addition to this (administrative) sanction in the MLTFPA, § 396 of the Penal Code contains a criminal sanction for repeated non-reporting:

> *§ 396. Failure to report suspicious transaction, submission of incorrect information*
> *(1) Failure to report a suspicious transaction or a suspicion of terrorist financing or submission of incorrect information to the Financial Intelligence Unit, if a punishment for a misdemeanour has been imposed on the offender for the same act, is punishable by a pecuniary punishment or up to one year of imprisonment.*
> *(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.*

607. To avoid a person being sanctioned twice (administrative and criminal) for the same offense (which would be in contradiction to Art. 4 of Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 117; "right not to be punished twice", *ne bis in idem*, which Estonia has signed, ratified and is part of the Constitution of Estonia), Art 29 (1) 4) of the Code of Misdemeanour Procedure stipulates that:

> *(1) Misdemeanour procedure shall not be commenced and the proceedings commenced shall be terminated if:[...]*
> *4) the act in question contains elements of a criminal offence.*

This means that the criminal sanction will be given priority where conduct could be penalized both with a criminal and administrative sanction. In order to ensure consistent treatment of persons under indictment (i.e. one person receives a criminal sanction while another person only receives an administrative sanction) just because of a lack of communication between the sanctioning authorities, the Estonian authorities advised that a register of punishments contains all (administrative and criminal) sanctions imposed. In the course of indictment proceedings there is a requirement for the authorities to check previous sanctions which provides a safeguard that criminal proceedings are only initiated where appropriate.

608. As the language of § 32 (1) MLTFPA is rather broad and does not specifically link the reporting requirement simply to transactions (which are defined in § 67 (1) of the Civil Code Act as an act or a set of interrelated acts which contains a declaration of intention directed at bringing about a certain legal consequence) but with suspicious "activity or circumstances", it can be concluded that *funds* suspected to be linked with terrorist financing are also covered.

609. The law does not explicitly address attempted transactions. However, the language of § 32 (1) MLTFPA is not restricted to transactions; instead it relates to "*activity or circumstances which might be an indication of money laundering or terrorist financing*". Thus, one interpretation is that attempted transactions are covered as they can be considered as a kind of "*activity or circumstances*". An alternative interpretation is that an attempted transaction is the exact opposite of "*activity*" as one of the characteristics of an attempt is that the intended action does not take place. Also "*circumstances*" do not necessarily cover attempted transactions, as it could be interpreted in a way that this covers only the concomitant circumstances of an action and not of an attempted action.

610. Some attempted transactions may be covered by the regime of § 32 (2) MLTFPA which stipulates a reporting obligation in the circumstances provided for by § 27 (1) to (3) MLTFPA: this covers *inter alia* situations when an obligated person is required to refuse a transaction and/or terminate a business relationship where full CDD fails due to the other party's failure to provide sufficient information or documentation. This does not, however, cover situations involving attempted transactions when the customer (and not the obligated entity) declines to enter into the transaction.

611. In conclusion, some attempted transactions are covered via § 32 (2) MLTFPA but to cover all kind of attempted transactions clearer language is required. In practice, the Estonian authorities advised that the FIU does receive STRs concerning attempted transactions but does not keep statistics about attempted transactions. The Estonian reporting form for STRs does not contain a specific field to indicate that it was an attempted transaction; the reporting entities can indicate this only by way of a supplementary remark on the form.

612. In Estonia predicate offences involve also tax offences, thus, the reporting obligation covers also tax matters, which is also addressed in the FSA's AML guidelines.

613. Figures on STRs are provided in Section 2.5 of the report. The highest number of reports still comes from banks (in 2007 more than 40% of all STRs), from providers of cash transfer services and organisers of gambling and lotteries. The accumulated value of assets related to the reported transactions was in 2005 EUR 4,15 billions, in 2006 EUR 1,92 billions and in 2007 EUR 7,16 billions.

614. Concerning STRs related to financing of terrorism, the Estonian authorities could only provide the overall figure (73) but no breakdown concerning the reporting entities. The reason for this was that the FIU did not keep such detailed statistics until 2007 due to the deficiencies of the old FIU database. From 1 January 2008 the new FIU information system has been able to provide such additional statistics.

615. The FIU is satisfied with the level of STRs received from the obligated entities. Reportedly, notaries submit the best quality reports. Most of these reports concern real estate businesses/operations and are under criminal investigation.

616. On the negative side it was noted that savings and loan associations as well as the insurance sector had not submitted any reports to date. The evaluators were advised by the Estonian authorities, that all such transactions go through the banking sector, and as banks are obliged to report any money laundering or terrorist financing suspicions, there is no need to duplicate reporting (a view not shared by the evaluation team as all obliged entities should follow their reporting obligations and not rely on others).

Additional Elements

617. The money laundering offence and corresponding reporting obligation are based on an "all crimes" approach. Financial institutions are required to report to the FIU when they suspect that funds are the proceeds of criminal acts that would constitute a predicate offence for money laundering domestically.

Special Recommendation IV

618. As described above (para 603), § 32 MLTFPA also covers the obligation to notify the FIU in cases of suspicion of terrorist financing.

619. The MLTFPA does not provide a separate definition of financing of terrorism in its § 5, instead it makes a cross-reference to § 237[3] PC: *"Terrorist financing means financing terrorism crimes as provided in § 237[3] of the Penal Code."* Thus, the reporting obligation as provided for in § 32 is limited to this extent and suffers from the same shortcomings as the terrorist financing offence (see above section 2.2). This means that there is no reporting obligation concerning terrorist financing in the following circumstances:

a) Financing of an individual terrorist;
b) when it comes to "collecting of funds" by any means, directly or indirectly, and their use in full or in part for terrorist financing purposes;
c) the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist;
d) Some conducts as referred to in Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions are not covered

However, it has to be noted that in the opinion of the evaluation team these shortcomings in the reporting obligation have only a minor impact in practice because it is considered that the obligated persons under the law will not do a detailed analysis of the shortcomings of the terrorist financing offence. Instead it is assumed that they will consider their obligations under the MLTFPA (which basically states that there is a reporting obligation when it comes to terrorist financing) and in addition rely on guidance by the FIU and the FSA explaining the concept of terrorist financing in more detail.

Recommendation 14

Safe Harbour Provisions

620. The waiver of official, banking or commercial secrecy, and protected private information, is addressed by § 35 MLTFPA ("Relief from liability"):

> *(1) An obliged person, its employee, representative or a person who acted in its name shall not, upon performance of the obligations arising from this Act, be liable for damage arising from failure to enter into a transaction or failure to enter into a transaction by the due date if the damage was caused to the person participating in the transaction made in economic or professional activities in connection with notification of the Financial Intelligence Unit of the suspicion of money laundering or terrorist financing in good faith, or for damage caused to a person or customer participating in a transaction entered into in economic or professional activities in connection with cancellation of a contract entered into for an indefinite period on the basis provided in subsection 27 (3).*
> *(2) The performance in good faith of the notification obligation arising from § 32 and communication of relevant data by an obligated person is not deemed infringement of the confidentiality requirement provided by law or contract and no liability provided by legislation or contract is imputed with regard to the person*

who performed the notification obligation for disclosure of the information. An agreement derogating from this provision is void.

621. It can be concluded that the language of § 35 provides a comprehensive protection of financial institutions, their directors, officers and employees concerning civil (arg. e "*not [...] be liable for damage*") and criminal (arg. e "*not deemed infringement of the confidentiality requirement provided by law or contract*") liability for breaches of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU.

Tipping off

622. § 34 of the MLTFPA establishes the confidentiality requirements of persons with a notification obligation: "*An obligated person, a structural unit and 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 or initiation of criminal proceedings under § 40 or 41. 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 after fulfilment of the precept made by the Financial Intelligence Unit*." This provision comprehensively covers the requirements of criterion 14.2. § 61 MLTFPA provides for sanctions in case of violations of § 34 MLTFPA: a natural person is publishable by a fine up to 300 fine units à 60 EEK (1150.40 EUR) or detention; a legal person is punishable by a fine of up to 500 000 EEK (31 955.82 EUR).

Additional elements

623. § 43 (5) of the MLTFPA establishes restrictions on the use of information and states that "*the Financial Intelligence Unit shall not disclose the personal data of the person performing the notification obligation or a member or employee of the directing body of the obliged person*". Furthermore, § 44 (2) of the MLTFPA stipulates that "*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.*" Moreover, also the contact person at the Security Police Board is similarly restricted under (§ 45 (3) MLTFPA). In practice, when forwarding an analytical report to law enforcement authorities for further investigation, the FIU does not include in its report any data or other details of the persons filing the STR.

Recommendation 19

624. With the new MLTFPA, Estonian authorities introduced a CTR reporting system which has been mandatory since 28 January 2008: according to § 32 (2) MLTFPA, all obligated persons have to notify the FIU "*of any transaction where the financial obligation exceeding 500,000 EEK or an equal amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments*". It is worth noting that this obligation is not applicable for credit institutions; for the credit institutions such an obligation exists only in cases of a *currency exchange transaction* exceeding 500 000 EEK in cash and only if the credit institution has not established a business relationship with the person participating in the transaction. Estonian authorities explained that the reasons for allowing this exemption for credit institutions were that credit institutions have a good understanding of their reporting obligations and the FIU is satisfied with the quality and amount of STRs received by CTRs. Thus, to include credit institutions in the CTR reporting obligations would only overload the work of the FIU without providing any additional value.

625. The Estonian authorities explained the reasons for introducing such a CTR reporting system with the high technological level of banking in Estonia, which allows for quick and secure non-cash settlements; thus, there is no reason to make large cash transactions in commerce. According to the information provided by the Bank of Estonia, the number of payments initiated in cash in credit institutions accounts for 0.26% of all initiated payments.

626. The FIU has a computerised system for all STRs and CTRs. (**19.3)** Only officials of the FIU have access to and the right to process the information of this database (for further details see above para 356).

Recommendation 25

627. § 37 MLTFPA defines the functions of the FIU. One of these functions is "*to inform the persons who submit information to the Financial Intelligence Unit of the use of the information submitted for the purposes specified in clause 1) of this section in order to improve the performance of the notification obligation*". As this provision only describes the functions of the FIU, one has to conclude that this does not stipulate an obligation for the FIU; instead, this has to be considered as a competence (authorisation) of the FIU.

628. In practice, the Estonian FIU provides financial institutions and DNFBP with:

- **General feedback**. This emanates from the Annual Report released by the Unit. Annual reports are made publicly available through the FIU's official website on the internet. The annual report includes:
  - statistics on the number of disclosures with appropriate breakdowns and the results of the disclosures;
  - information on current techniques, methods and trends;
  - sanitised sample cases.
- **Specific feedback** in written form on the case-by-case basis. This means that the FIU annually sends a written notice to every reporting entity if the STR they submitted has been forwarded to a law enforcement authority or a Prosecutor's Office for further investigation. The FIU also informs the reporting entity about further results of the investigation (whether the case is closed or completed) and possible convictions/acquittals.
- **Feedback upon request** by a financial institution or DNFBP.

3.7.2 Recommendations and comments

629. In general, Estonia has a comprehensive system for reporting suspected money laundering and terrorist financing. The necessary legal provisions are in place and the system seems to be implemented effectively. However, some shortcomings exist which should be remedied:

630. It should be clarified in the MLTFPA, that all attempted transactions have to be reported.

631. The definition of financing of terrorism as provided for by § 5 of the MLTFPA is linked with the definition as provided for by § 237^3 PC (the terrorist financing offence) and thus it has the same limitations as the terrorist financing offence and there is no reporting obligation in case of:

a) financing of an individual terrorist;
b) collecting of funds for the purpose of terrorist financing;
c) the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist;
d) those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC).

Though these shortcomings are supposed not to be of significant practical influence, it is recommended that the reporting obligation is broadened and brought into line with SR IV.

632. Savings and loan associations as well as the insurance sector have not submitted any STRs to date. Estonian authorities are of the opinion that the money laundering risks in these sectors are quite low. However, the total absence of any reports sent by these entities cannot be justified with an assessment of low risks as the indicators for money laundering (issued by the FIU) contain a number of situations which should also trigger some reports from these entities. This shows that there is presumably either a lack of understanding or awareness of anti-money laundering obligations within these entities. The FIU should provide more guidance and training to these entities so that they better understand their reporting obligations.

633. In the absence of detailed statistics concerning STRs related to financing of terrorism before 2008 it is difficult to evaluate the effectiveness of the system in this regard.

3.7.3 Compliance with Recommendations 13, 14, 19, 25 (criterion 25.2 only) and Special Recommendation SR.IV

	Rating	Summary of factors underlying rating
R.13	**LC**	• Not all kinds of attempted transactions are clearly covered by the reporting obligations. • There is no reporting obligation in case of: – financing of an individual terrorist; – collecting of funds for the purpose of terrorist financing; – the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist; – those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC). • Savings and loan associations as well as the insurance sector sent no STRs so far which is presumably caused by a lack of understanding or awareness of their reporting obligations.
R.14	**C**	
R.19	**C**	
R.25	**C**	
SR.IV	**LC**	• There is no reporting obligation in cases of: – financing of an individual terrorist; – collecting of funds for the purpose of terrorist financing; – the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist; – those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC). • Not all kinds of attempted transactions are clearly covered by the reporting obligations. • In the absence of detailed statistics before 2008 it is difficult to evaluate the effectiveness of the system.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 and 22)

3.8.1 Description and analysis

Recommendation 15

Generally

634. § 29 (1) of the MLTFPA requires obligated persons to establish written rules of procedure for the application of due diligence measures, including assessment and management of the money laundering and terrorist financing risk, collection of information and storage of data, reporting of suspicious transactions as well as rules for checking adherence thereto. This provision is complemented by § 63(2) (6) of the Credit Institutions Act which requires credit institutions to establish internal rules of procedure which, among others, should set out the procedures for the application of international sanctions on the basis of the International Sanctions Act and the code of conduct and the internal audit rules to monitor compliance with the MLTFPA. § 30(1) MLTFPA requires that the rules of procedure established by an obligated person shall correspond to the sort, scope and complexity of the economic or professional activities of the obligated person and set out the rules for the application of the due diligence measures.

635. § 30 (2) of the MLTFPA requires obligated persons to regularly check the established rules of procedures and update them by introducing new rules of procedures where deemed necessary.

636. § 30 (3) MLTFPA sets out the contents of the internal rules of procedures requiring that these should deal with the following:

- Low risk transactions
- High risk transactions
- On-going monitoring of business relationships and transactions and verification of identification data
- Collection and presentation of documents and data.

637. § 30 (6) assigns to the Minister of Finance the duty to prescribe in a regulation the requirements for the rules of procedures established by credit and financial institutions as well as the rules for the internal audit arrangements. At the time of the on-site visit, no such regulation was in existence[45]. Consequently, the necessary content of these internal rules of procedure for the

[45] Subsequent to the on-site visit, the Minister of Finance issued Regulation No 10 "Requirements for the rules of procedure established by credit and financial institutions and for their implementation and verification of compliance". However, as this Regulation came only into force more than 2 months after the on-site visit, it was not taken into account in the descriptive part and for rating purposes. By virtue of this Regulation, credit and financial institutions must establish written rules of procedures which must at least, comprise the following:

- Code of conduct for the application of CDD measures, on a risk sensitive basis, as per section 14(3) of the MLTFPA
- Code of conduct for the collection and preservation of data (record keeping)
- Code of conduct for performing the notification obligation and management information
- Internal control procedures for monitoring adherence to the above.

The Regulation specifies that the responsibility for the establishment of the written rules of procedures in one or more documents lies with the Head of a credit or financial institution (§ 2 (2)). Article 10 of the Regulation imposes an obligation on credit or financial institutions to communicate to their employees engaged in the establishment of business relationships or the carrying out of transactions the current rules of procedures and internal control rules. Article 22 of the Regulation requires that the Rules of Procedure establish procedures for the detection of unusual or suspicious transactions, operations or circumstances. In this context, it is also required that the rules of procedures provide for the obligation of employees to analyse the circumstances of

obligated entities was not determined at the time of the on-site visit. As another consequence, it is questionable whether financial institutions were already obliged by the provisions of the MLTFPA to issue internal rules of procedure concerning AML/CFT issues. Though the law determines some of the elements, it clearly states that the requirements have to be established by the Ministry of Finance (§ 30 para 6). At the time of the on-site visit representatives of the financial institutions were also waiting for these specifications. However, it should to be taken into account that § 13 of the previous MLTFPA established the obligation for credit institutions and financial institutions "*to establish a code of conduct for employees to prevent money laundering and terrorist financing, and to establish internal audit rules to monitor compliance with the code of conduct*"; similar like the new MLTFPA, also § 13 para 6 of the previous MLTFPA required the Ministry of Finance to establish the requirements for this code of conduct and for the internal audit rules to monitor compliance with the code of conduct. This had been done with Regulation No 61 of 5 September 2005 of the Ministry of Finance, which was in force until 28 January 2008. This Regulation No 61 stated in its § 1 that "*(2) A code of conduct shall set out at least the following information: 1) bases for identification, including requirements for the data and documents which are the basis for identification; 2) the procedure for verification and preservation of data and documents used for identification and the procedure for updating the data; 3) bases for monitoring of customer relationships; 4) measures used by an employee of a credit or financial institution (hereinafter employee) in the event of suspicion of money laundering or terrorist financing*".

638. Leaving aside the legal uncertainty whether at the time of the on-site visit obligated persons were already obliged to establish such internal rules of procedure and only taking into account the respective requirements of the MLTFPA, one can conclude that the MLTFPA does not require financial institutions to include guidance concerning the detection of unusual and suspicious transactions in their internal rules of procedure. This will need to be determined by the Regulation of the Minister of Finance[46].

639. § 59 Credit Institutions Act requires credit institutions to establish an independent internal audit unit as part of the internal control system of a credit institution which shall monitor the activities of the whole credit institution. The internal audit unit shall assess the ordinary business of the credit institution and the suitability and sufficiency of the internal rules and rules of procedure for the activities of the credit institution, regularly monitor compliance with the requirements, rules of procedure, limitations and other rules established by the supervisory board or the management board, and monitor compliance with precepts issued by the Financial Supervision Authority. Art. 58 of the Investment Funds Act, Art. 83 of the Insurance Activities Act and Art. 83 of the Securities Market Act provide similar provisions.

640. § 29 (3) MLTFPA explicitly requires credit and financial institutions to appoint a person as the "contact person" of the FIU. § 29 (5) MLTFPA permits the functions of a contact person to be performed either by an employee or a structural unit of the obligated person. In the event that a structural unit is appointed to perform the functions of the contact person, the Head of the structural unit is considered to be directly responsible for the performance of the functions assigned to the contact person under the MLTFPA. Furthermore, the said provision requires the notification by the obligated person of the appointment of a contact person.

641. § 31 MLTFPA requires the "contact person" of a credit and financial institution to report directly to the Management Board of the credit or financial institution. The Management Board is responsible for ensuring that the contact person has the competences, means and access to relevant information needed for the performance of his functions. The MLTFPA (§ 30(3)(4)) defines the functions of the contact person as follows:

---

suspicious transactions and verify the origin of property before a transaction is carried out when a transaction is considered to be unusual and unexplainable.

[46] see FN 45.

- Organisation and analysis of information related to unusual and suspicious transactions,
- Notifying the FIU on suspicious transactions,
- Reporting to the Management Board on the implementation of the rules of procedures together with proposals for amendments or modification,
- Ensuring that the credit or financial institution complies with the requirements of the MLTFPA, and
- Demand from the structural units of the credit or financial institution to take measures to eliminate deficiencies in AML/CFT requirements.

642. With regard to training, § 29 (2) MLTFPA requires obligated persons to "*ensure the provision of regular training in the performance of obligations arising from [the MLTFPA] for employees whose duties include establishment of business relationships or entry into transactions*".

643. Credit and financial institutions have their own procedures and requirements when hiring new employees. The MLTFPA contains no provision on this and there is no other regulation from supervisors dealing with the matter. Hence, criterion 15.4 is not met.

Recommendation 22

644. § 13(2) of the MLTFPA, in line with Article 31 (1) of the 3rd EU AML Directive, requires that credit and financial institutions apply due diligence measures in an agency, branch or subsidiary situated in a third country and follow requirements for collection and storage of data, which are at least equivalent to the provisions of the MLTFPA. It is noted, however, that criterion 22.1 refers to AML/CFT measures in general and not only to customer due diligence and record keeping. The said provision further states that in the event that the legislation of a third country does not permit the application of equivalent measures, the credit or financial institution concerned is required to notify its competent supervisory authority and moreover, apply additional measures for the prevention of ML/TF risks.

645. The MLTFPA does not explicitly require branches and subsidiaries in host countries to apply, when the AML/CFT requirements of the home and host countries differ, the higher standard to the extent that local laws or regulations differ, as required by criterion 22.1.2. This can be deduced from the language of § 13 (2) MLTFPA which reads as follows: "*Credit and financial institutions apply the due diligence measures in an agency, branch or subsidiary where they have a majority shareholding located in a third country and follow the requirements for collection and storage of data, which are <u>at least equal</u> to the provisions of this Act.*"[47] This means that if the foreign provisions are worse, they should follow the Estonian provisions. But if the foreign provisions provide better standards, it would still be sufficient to follow the Estonian regulations (*arg. ex* "*...and follow the requirements for collection and storage of data, which are <u>at least equal</u> to the provisions of this Act*"). If they were required to follow the higher standards, the language would have to be like "*follow the higher standards*" but "*at least*" refers only to a minimum standard, but not that the higher standard has to be applied.

646. Furthermore, criterion 22.1.1 requires that financial institutions should be required to pay particular attention to the application of the principles laid down in R.22 to branches and subsidiaries located in countries which do not or insufficiently apply the FATF Recommendations. The MLTFPA does not address this particular issue.

647. The Estonian authorities advised that in total, Estonian financial institutions maintained 17 subsidiaries and branches in foreign countries:
- 3 Subsidiaries of credit institutions (in Latvia, Lithuania and Russia);
- 2 Branches of credit institutions (in Latvia & Lithuania);

[47] Emphasis added.

- 12 Branches of financial institutions:
  - 4 Investment companies (in Latvia, Lithuania, UK & Cyprus);
  - 8 insurance companies (in Latvia & Lithuania).

3.8.2 Recommendation and comments

Recommendation 15

648. The MLTFPA requires obligated persons to establish written rules of procedure for the application of due diligence measures, including assessment and management of the money laundering and terrorist financing risk, collection of information and storage of data, reporting of suspicious transactions as well as rules for checking adherence thereto. However, the MLTFPA follows a system that further details of these internal rules have to be established by the Minister of Finance; at the time of the on-site visit and two months subsequently, no such regulation had come into force and effect[48].

649. Financial institutions should be required to have guidance in their internal rules of procedure concerning the detection of unusual and suspicious transactions.

650. It is recommended that the legal requirements for regular training of employees extend to cover new developments in AML/CFT matters, including information on current ML/TF techniques, methods and trends.

651. The Estonian authorities should introduce requirements imposing an obligation on credit and financial institutions to put in place screening procedures when hiring employees beyond the ones established regarding audit employees and members of management as per the relevant articles of CrIA, IAA, Investment Funds Act and the Securities Market Act.

Recommendation 22

652. The MLTFPA requirements for the implementation of AML/CFT measures by foreign branches and subsidiaries of credit and financial institutions should extend beyond customer due diligence and record keeping measures.

653. Credit and financial institutions should be required to pay particular attention to foreign branches and subsidiaries operating in countries which do not or insufficiently apply FATF Recommendations.

654. Provision should be made that where minimum requirements of the host and home countries differ, branches and subsidiaries in host countries should be required to apply the higher standard to the extent that local (i.e. host country) laws and regulations permit.

3.8.3 Compliance with Recommendations 15 and 22

	Rating	Summary of factors underlying rating
R.15	**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

[48] see FN 45.

		AML/CFT issues which, at the time of the on site visit, were based on a Regulation of the Minister of Finance issued under the previous law. • Financial institutions are not required to have guidance in their internal rules concerning the detection of unusual and suspicious transactions. • Limited requirements concerning screening procedures for new employees. • Financial institutions are not required to include in their training of employees current AML/CFT techniques methods and trends.
R.22	**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. • 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. • 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.

3.9 Shell banks (R.18)

3.9.1 Description and analysis

655. According to § 3(2) of the Credit Institutions Act (CrIA), credit institutions may operate as public limited companies or savings and loans associations. Credit institutions must be authorised by the Estonian FSA (§ 13(1) CrIA). The Credit Institutions Act requires applicants to submit a written application which has to provide amongst other things the following information:

a) "*information on the information and other technological means and systems, security systems, control mechanisms and systems needed for provision of the planned financial services*" (§ 13^1 (1) item 6 CrIA).

656. Apart from this, the CrIA does not require applicants to submit information on the premises of the place of operation (e.g. a vault and other equipment to run a banking business; furniture; clients rooms etc.). However, the FSA is also empowered to refuse authorisation if "*the information submitted by the applicant indicates that the applicant mainly plans to operate in another contracting state*" (§ 15(1) 6) CrIA). This seems to provide a useful tool to avoid the establishment of shell banks and is more comprehensive than the requirements of § 131 CrIA. However, the term "*contracting state*" used in this provision refers only to "*states which are contracting parties to the EEA agreement*" (§ 4 (4) 1 CrIA). This reference to EEA contracting states reduces significantly the coverage of criterion 18.1, as it would allow the establishment or continuous operation of shell banks if applicants were interested in running such a business from outside of the European Economic Area (EEA).

657. § 22(3) MLTFPA prohibits credit or financial institutions from opening or holding a correspondent account with a credit institution whose actual place of management or business 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 or financial institution which is subject to sufficient supervision. This legal requirement effectively prevents credit or financial institutions from entering or maintaining a correspondent banking relationship with a credit institution, whose

characteristics as set out in the MLTFPA, correspond to a shell bank as defined in the methodology. Effectively, Estonian requirements go beyond the requirements of Recommendation 18 as they also prohibit relationships with banks whose business is outside their country of location (i.e. offshore banks). Hence, essential criterion 18.2 is considered to be satisfied.

658. Furthermore, § 22(3) 2) MLTFPA prohibits the opening or holding of correspondent bank accounts with credit institutions which open accounts for credit institutions which have the characteristics defined in § 22(3) (1) MLTFPA (mentioned in the previous paragraph). In this regard, essential criterion 18.3 is also considered to be satisfied.

3.9.2 Recommendations and comments

659. The CrIA only provides safeguards concerning the establishment or continuous operation of shell banks which are operated from the European Economic Area (EEA). This restriction to the EEA should be removed and the CrIA should prohibit the establishment or continuous operation of shell banks regardless of the country from which they are operated (though it is clear that the Estonian FSA's practice and policy is not to license shell banks).

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**LC**	• The CrIA does not clearly prohibit the establishment or continuous operation of shell banks in Estonia which are operated from outside of the European Economic Area (EEA).

Regulation, supervision, guidance, monitoring and sanctions

3.10 The supervisory and oversight system - competent authorities and SROs / Role, functions, duties and powers (including sanctions) (R. 23, 29, 17 and 25)

3.10.1 Description and analysis

Recommendation 23

660. § 6(1)7 of the FSA Act stipulates that one of the functions of the FSA is to perform the functions arising from the MLTFPA. § 47(2) of the MLTFPA empowers the Estonian FSA to supervise credit and financial institution which fall under its supervision by virtue of the FSA Act with regard to the fulfilment of their obligations arising from the MLTFPA. Under the FSA Act, supervised entities comprise credit institutions (including foreign banks' branches) investment firms, fund management companies, life and non-life insurance companies, insurance brokers (but not insurance agents), the Traffic Insurance Fund and the Tallin Stock Exchange.

661. According to §§ 37 and 47 (1) of the MLTFPA, the Estonian FIU exercises supervision over all other obligated persons engaged in financial activities, as set out in § 2 of the MLTFPA, who do not fall under the supervision of the Estonian FSA. This means that the Estonian FIU is responsible for the AML/CFT supervision of a very large number of undertakings spread all over the country which are engaged in financial and non-financial activities. At the time of the on-site visit, the activities and number of undertakings, falling under the FIU's supervision were the following:

Type of undertaking	No
Savings and loans associations	14
Leasing companies	29
Pawnshops	81
Loaning	146
Providers of alternative means of payment	6
Money transmitters	8
Currency exchange (including money transmission)	135
Non-classified financial intermediation (companies that provide financial intermediation as a secondary activity; e.g. hotels or travel companies that provide currency exchange.)	648

Source: Estonian FIU (taken from the Estonian Commercial Register)

662. § 48 of the MLTFPA lays down the rights of supervisory authorities for the performance of their supervisory duties and responsibilities. By virtue of the said paragraph, supervisory authorities have the right to carry out on-site inspections at the offices of obligated persons in the presence of a representative of the inspected person, obtain documents and information, including copies thereof, and receive oral and written explanations from its employees and directors.

663. With regard to criterion 23.3, it is noted that the Estonian FSA has the legal power to prevent, to a certain extent, the criminal infiltration of credit and financial institutions. § 15 (1) 4) Credit Institutions Act states: "*The Financial Supervision Authority shall refuse to grant authorisation to the applicant if the managers, auditor or shareholders of the applicant do not meet the requirements provided for in this Act or legislation established on the basis thereof*". Therefore, the FSA shall refuse to grant authorisation if the person who will be appointed as a manager is not fit and proper. According to § 48 (2) Credit Institutions Act, only persons who have the education, experience and professional appropriateness necessary to manage a credit institution and who have an impeccable business reputation may be elected or appointed managers of credit institutions or financial holding companies. According to § 15 (1) 8) and § 17 (1) 5) of the Credit Institutions Act, the FSA may refuse to grant authorisation or revoke authorisation if the applicant or the credit institution or its managers have been punished for an economic offence, official misconduct, offence against property or offence against public trusts. As the money laundering offence (§ 394 PC) is in chapter 21 of the Penal Code which has the title "Economic Offences", one can conclude that prior convictions for money laundering are a reason to refuse or revoke an authorisation according to the Credit Institutions Act. On the other side a prior conviction for terrorist financing appears not to be an obstacle as the terrorist financing offence (§ 237^1 PC) is placed in chapter 15 of the Penal Code ("Offences against the state").

664. Similar legal requirements and procedures are in force in respect of market entry regarding insurance undertakings, investment firms and fund management companies, see:

a) § 23 (1) 3), 6), § 48 (2) 2) of the Insurance Activities Act;
b) § 56 (3), (4), § 58 (2) 2), § 79 (4) 4) of the Securities Market Act;
c) § 18 (1) 4), 8), § 51 (2) of the Investment Funds Act.

665. With regard to beneficial owners of a significant or controlling interest of a financial institution, according to § 30 of the Credit Institutions Act, a person who intends to acquire 10% or more of the share capital or votes of a credit institution or increases its holding to more than 20%, 33% or 50% is required to inform the FSA before proceeding with the acquisition. This person is required to provide to the FSA various information and documents, including data relating to its identity, information on the members of the management and supervisory bodies, and sources of funds. § 29(4) of the Credit Institutions Act requires that a qualifying holding in a bank may be held by anyone whose structure of ownership and business connections are transparent and do not prevent supervision or receipt of

information. Furthermore, the FSA is empowered (§ 30(4) CrIA) to request additional information or documents in order to specify of verify the information or documents submitted by applicants. Also, the FSA has the legal right (§ 31(3) CrIA) to prohibit the acquisition or increase of qualifying holdings in a bank if, inter-alia, the sources of funds to be used for the acquisition may be connected, in the opinion of the FSA, with a criminal offence. However, there are no provisions clearly stating that criminal records of beneficial owners of a significant or controlling interest would be an obstacle.

666. According to § 31 (3) 1) of the Credit Institutions Act, the FSA may prohibit, by a precept, the acquisition or increase of a qualifying holding or turning a bank into a controlled company if this is contrary to the principles of the sound and prudent management of the bank; this would be the case, if amongst other things the acquirer does not have an impeccable business reputation or does not meet the requirements provided for in § 29 of CrIA. There are similar provisions regarding other financial institutions (§ 60, §61 (3) 6), § 62 (3) 6 of the Insurance Activities Act; § 72, § 73, § 74 (1) 6), § 76 (1) 6) of the Securities Market Act; § 44, § 45, § 46 (1) 6) , § 48 (1) 6) of the Investment Funds Act).

667. Estonian authorities advised that, as a matter of practice, information is obtained directly from applicants on the criminal background of beneficial owners and controllers of banks and other financial institutions. This information is regularly checked with foreign supervisory authorities concerning non-resident applicants.

668. With regard to criterion 23.3.1, § 48 of the Credit Institutions Act requires managers of credit institutions to have the necessary education, experience and professional appropriateness necessary to manage a credit institution. Persons who have caused bankruptcy or liquidation of a company or if it becomes obvious from earlier activities that they are not capable of managing a company, are prohibited from taking over a managerial position of a credit institution. Credit institutions are required to notify the Estonian FSA of their intention to elect or appoint a manager, together with information on his work experience, education, and confirmation concerning the absence of facts provided for in the CrIA which preclude the right to be a manager of a credit institution (§ 48(7) CrIA). As a matter of practice, non-resident applicants must also present a police-issued excerpt of their criminal register, while the FSA, according to Art. 17 of the Punishment Registry Act, is empowered to check the criminal register of resident applicants.

669. According to § 50 (1) of the Credit Institution Act, the FSA has the right to issue a precept to demand the removal of a manager if it considers that the said person does not have the education, experience and professional qualifications necessary to manage a credit institution and an impeccable business reputation or the person has submitted misleading or inaccurate information or falsified documents in connection with his or her election or appointment. Similar provisions exist regarding the other financial institutions: § 173 (7) of the Insurance Activities Act, § 235 (6) of the Securities Market Act, § 290 (1) 7) of the Investment Funds Act.

670. Prudential supervision, including on-site examinations conducted by the Prudential Supervision Division of the FSA, also covers issues relevant to AML/CFT, especially in the context of management of operational risks. Regular reporting by supervised entities on operational risks includes e.g. the number of STRs submitted to the FIU and information on criminal offences (e.g. internal and external fraud) occurred.

671. § 52 MLTFPA requires currency exchange bureaux, providers of payment services (i.e. money remitters) as well as providers of alternative means of payment to register within the register of economic activities. § 55 of the MLFTPA provides that registration should be refused if the service provider, the directors or beneficial owners of the financial institution have committed a crime specified in §§ 237-237^3 or 394-396 of the Penal Code (this list includes the money laundering and the terrorist financing offence) or another intentionally committed criminal offence.

672. For financial institutions which are not supervised by the Estonian FSA pursuant to § 2 of the FSA Act (i.e. currency exchange bureaux, providers of payment services [i.e. money remitters] as well as providers of alternative means of payment, which are supervised by the FIU) no registration requirements apply[49]. According to § 24^1 of the previous MLTFPA (which was in force until 28 January 2008 from which day the new MLTFPA came into force), providers of currency exchange services were required to register in the Register of Economic Activities before commencing operations.

673. It is noted that under § 6 (4) 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 credit or a financial institution for the purposes of the Credit Institutions Act. At the time of the on-site visit, there were six entities providing the above type of payment services. The Estonian authorities anticipate that none of these entities will be able to meet the registration requirements of the MLTFPA and to comply with § 15 (8) of the MLTFPA which explicitly provides that alternative service providers have to identify their clients face to face for transactions in excess of 15 000 EEK (958.67 EUR). It is, therefore, expected by the Estonian authorities that they will cease operations and close.

Recommendation 29

674. Criterion 29.1 requires that supervisors should have adequate powers to monitor and ensure compliance by financial institutions with AML/CFT requirements. The Credit Institutions Act gives broad powers to the Estonian FSA to obtain information and carry out on-site inspections of supervised entities. § 99 of the Credit Institutions Act establishes the right of the Estonian FSA to demand and obtain information, documents and oral or written explanations for the performance of its supervisory functions. § 100 of the Credit Institutions Act empowers the FSA to perform on-site inspections of supervised entities.

675. In addition, both the Estonian FSA and FIU have the power under §§ 47 and 48 of the MLTFPA to exercise supervision over persons subject to their supervision for the purpose of checking compliance with the AML/CFT obligations stipulated in the Law. The supervisory powers of the FSA and FIU include the right of on-site inspections in the course of which they may request and obtain documents, information and explanations without a court order for those purposes. § 41 (1) MLTFPA provides that the FIU has the right to receive information from the FSA and state or local government authorities and, on the basis of precepts, from obligated persons regarding the circumstances, transactions or persons related to the suspicion of money laundering or terrorist financing to perform its functions arising from the law. It is noted, however, that there is no explicit provision empowering the FIU to request the production of information for other supervisory purposes. According to § 99 of the Credit Institutions Act, the FSA has the right to demand, free of charge, information, documents and oral or written explanations concerning facts relevant to the exercise of supervision.

676. With regard to sanctioning powers, the Estonian FSA is empowered by § 103 of the Credit Institutions Act to issue a precept to a supervised entity if violation of the requirements of the Credit Institutions Act or MLTFPA are discovered during supervision. By issuing a precept, § 104 of the Credit Institutions Act gives the right to the Estonian FSA to prohibit a credit institution from concluding transactions, demand amendment of internal rules and procedures or demand dismissal of employees. If a credit institution fails to comply with a precept, then the FSA is entitled to impose a penalty following the procedures given by the Substitutive Enforcement and

[49] It has to be noted that in principle § 52 MLTFPA also requires financial institutions which are not supervised by the Estonian FSA pursuant to § 2 of the FSA Act to register within the register of economic activities (as described in para 671). However, the requirement to register only came into force for these institutions on 15 June 2008 (§ 66 of the MLTFPA) which is outside the relevant period.

Penalty Payment Act. The upper limit for penalties is 18 000 EEK (i.e. 1 150.40 EUR) for the first violation and 75 000 EEK (i.e. 4 793.37 EUR) for each subsequent failure to comply in the case of natural persons, and 50 000 EEK (i.e. 3 195.58 EUR) and 750 000 EEK (i.e. 47 933.73 EUR) respectively in the case of legal persons. Under § 104 of the Credit Institutions Act, the FSA has the right by issuing a precept to demand, inter-alia, the removal of a member of the management board, suspension of an employee and propose to the general meeting of a credit institution the removal of a member of the supervisory board. Similar provisions exist in § 172, § 173 (precept), § 181 (penalty payment) of the Insurance Activities Act; 234 (precept), § 234^1 (penalty payment), § 235 of the Securities Market Act; § 289, § 290 (precept), § 301 (penalty payment) of the Investment Funds Act.

677. § 38 of the MLTFPA authorises the FIU to issue precepts and other administrative acts in order to perform the functions assigned to it by the Law. If a supervised entity fails to comply with an administrative act, the FIU is entitled to impose a coercive measure according to the Substitutive Enforcement and Penalty Payment Act (SEPPA) which amounts to a maximum penalty of 20 000 EEK (i.e. 1 278.23 EUR) for the first occasion and 80 000 EEK (i.e. 5 112.93 EUR) for each subsequent occasion. According to subsection (1) § 5 of the SEPPA the addressee of a coercive measure can be a natural person or a legal person in private law or in public law who is obligated, by a precept, to perform a required act or refrain from a prohibited act. If the addressee of a precept is a member of management board, director or senior management (it means natural person), then the addressee of the coercive measure (as translated into English: "penalty payment") is the same natural person.

Recommendation 17

678. Chapter 7 of the MLTFPA establishes the sanctions against obligated person for failure to comply with specified AML/CFT requirements. §§ 57 and 58 provide for a fine up to 300 fine units (as one fine unit amounts to 60 EEK the maximum sanction is 18 000 EEK; i.e. 1 150.40EUR) for a physical person, employee or agent of a credit or financial institution, and 500 000 EEK (i.e. 31 955.82 EUR) for a legal person for failure to comply with the identification and record keeping requirements. § 62 of the MLTFPA provides that failure by a manager of an obligated person to establish internal AML/CFT procedures for the application of due diligence measures, assessment and management of money laundering and terrorist financing risks, gathering and preservation of data and information, reporting of suspicions and appointment of a contact person is punishable by a fine of up to 300 fine units (i.e. 1 150.40EUR). According to § 48 (1) of the Credit Institutions Act, the "*members of the supervisory board and management board of a credit institution are deemed to be the managers of the credit institution*". Similar provisions exist in the laws governing the other types of financial institutions. If the said failure is committed by a legal person, then the fine reaches a maximum of 500 000 EEK (i.e. 31 955.82 EUR). § 65 of the MLTFPA provides that the extra-judicial proceedings of these misdemeanours shall be conducted by the police, the FSA and the FIU.

679. The FIU is empowered by § 38(1) MLTFPA to issue precepts and other administrative acts in order to perform the functions arising from the law. § 38(4) of the MLTFPA stipulates that in the event of failure to comply with an administrative act, the FIU may impose a coercive measure pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act which provides for a fine of up to 20 000 EEK (i.e. 3 195.58 EUR) for the first occasion and 80 000 EEK (i.e. 5 112.93 EUR) for each subsequent occasion. For sanctions imposed by the FIU see below para 702.

680. According to § 103 of the Credit Institutions Act, the FSA has the right to issue precepts for violations discovered during supervision of the requirements of the said Act or legislation specified in the FSA Act including the MLTFPA. The evaluators were informed that on three occasions the FSA issued a precept to credit institutions for insufficient implementation of AML/CFT requirements. According to § 104 of the Credit Institutions Act, the FSA has the

power, inter-alia, to prohibit a credit institution from conducting certain types of transactions, prohibit the payment of dividends and require restriction of operating expenses.

681. Apart from the specific AML/CFT-related sanctions provided in the MLTFPA, the general sanctioning mechanism for Estonian financial institutions relies on §§ 103 and 104 of the Credit Institutions Act. Under this regime, the Financial Supervisory Authority is empowered to issue a "precept" whenever it finds, as a result of supervision, that an institution has violated (any) requirements of the Credit Institution Act or legislation specified in § (2) 1) of the Financial Supervision Authority Act. Regarding the MLFTPA, § 47 (2) of the MLFTPA states that the "*Financial Supervision Authority exercises supervision over fulfilment of the requirements arising from this Act by credit and financial institutions which are subject to supervision by the Financial Supervision Authority under the Financial Supervision Authority Act*". These institutions are listed in § 2 (1) of the FSA Act which states that "*for the purposes of [the Credit Institutions Act], 'state financial supervision' […] means supervision over the subjects of state financial supervision […] and the activities provided for in […] the Credit Institutions Act*". § 6 (1) 7) of the FSA Act states that the "*functions of the Supervision Authority in fulfilling the objectives of financial supervision*" include performing "*the functions arising from […] the Money Laundering and Terrorist Financing Prevention Act*" (and others). § 6 (2) of the FSA Act states that in "*the performance of its functions, the Supervision Authority has all the rights provided for in [the FSA Act and] the Acts specified in subsection 2 (1) of [the FSA Act]*". As § 2 (1) of the FSA Act lists the Credit Institutions Act among the acts giving rise to supervisory powers, the FSA is entitled to issue precepts according to § 103 of the Credit Institutions Act. However, § 103 of the Credit Institutions Act empowers sanctioning (only) of "*violations of the requirements of [the Credit Institutions Act] or legislation specified in subsection (2) 1) of the Financial Supervision Authority Act*". The latter provision does not include the MLFTPA. This places violations of provisions of the MLFTPA other than the ones specifically made punishable through §§ 57 et seq. of the MLFTPA outside of the FSA's explicit sanctioning powers.

682. Instead, FSA relies on § 103 (1) 3) and § 104 (8) or (15) of the Credit Institutions Act, which empowers the FSA to issue a precept if "*the risks taken by a credit institution increase significantly or if other circumstances exist which endanger the activities of the credit institution, damage the interests or soundness of its depositors or the financial sector as a whole*". While this appears to be a less than clear legal basis for the issuance of a precept, the FSA has in fact issued precepts on this basis in the past. For example, precepts nr. 80 of 15 November 2006 and nr. 96 of 18 September 2007 required significant improvements of the recipients' internal rules of procedure and customer due diligence and were based on § 103 (3) and § 104 (8) and (15) of the Credit Institutions Act. Estonian authorities advised that these precepts were not challenged in court and complied with.

683. According to § 17 (12) CrIA, the FSA may revoke an authorisation if the credit institution engages in money laundering or violates the procedures established by legislation for the prevention of money laundering or terrorist financing. Similar provisions for other financial institutions exist in § 27 (9) Insurance Activities Act, § 58 (2) 8) Securities Market Act and § 22 (14) Investment Funds Act. For entities supervised by the FIU, deletion of the entry into the registry is possible only if a criminal conviction for a crime specified in §§ 237-237^3 or 394-396 of the Penal Code has entered into force regarding the service provider, the directors or beneficial owner.

684. Estonian authorities are of the opinion that the system of issuing precepts, either by the FIU (see para 679) or the FSA (see previous paragraph), makes the whole MLTFPA sanctionable. This "sanctioning system via precepts" is particularly relevant concerning provisions of the MLTFPA which are not covered by a specific sanctioning provision of the MLTFPA itself, as there is e.g. § 57 MLTFPA which refers to failure of obligated entities with "*identification obligations provided for in the [MLTFPA]*"; as "identification obligations" are not identical but only a part of customer due diligence measures, one has to conclude that a number of obligations outlined in Chapter 2 of

the MLTFPA (with the title "Due Diligence") do not fall under the sanctioning regime of § 57 MLTFPA. Thus, such non direct sanctionable parts would be constant monitoring of a business relationship, regular verification of data, opening anonymous accounts or saving books, some elements of enhanced CDD and treatment of PEPs which are not related to the identification process, correspondent banking provisions etc.

685. The approach of the Estonian authorities is apparently that though there are no sanctions provided by chapter 7 of the MLTFPA, all these provisions could be enforced by issuing a precept by the FIU or FSA and in case of a violation of this precept the obligated entity or an employee thereof could be sanctioned. However, it has to be noted that this system amounts only to an indirect sanctioning possibility. In first instance, the obligated entities could ignore all the provisions which are not directly sanctionable and wait till the FIU or the FSA discovers these violations. Only when a precept was then issued, th obligated entity would be required to stick to the obligations of the precept and, thus, also to the obligations of the MLTFPA which are mentioned in the precept.

686. A remarkable provision in the Estonian AML/CFT legal framework is § 395 PC which makes a repeated failure to comply with identification requirements a criminal offence and reads as follows:

> *(1) Failure to comply with the identification requirement, a punishment for a misdemeanour has been imposed on the offender for the same act, is punishable by a pecuniary punishment.*
>
> *(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.*

The Estonian legal system and practical measures to avoid that these two kinds of sanctions (administrative, criminal) for an identical conduct are in contradiction to Art. 4 of Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 117 ("right not to be punished twice", *ne bis in idem*) and the Estonian Constitution have been described above (para 607).

Recommendation 25 (criterion 25.1 only)

687. § 39 MLTFPA deals with guidelines to be issued by the FIU: its para 1 stipulates that the FIU "*has the right*" (i.e. non mandatory obligation) to issue advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing. The FIU has not yet proceeded with the issuance of such advisory guidelines.§ 39 (2) 3) of the MLTFPA imposes an obligation on the FIU to issue advisory guidelines related to "*the characteristics of suspicious transactions*" and "*the characteristics of terrorist financing*". The latter guidelines were developed by the FIU in cooperation with the Security Police Board and published on the FIU's website as requested by § 39 (3) and (4) of the MLTFPA.

688. In practice, the FIU issued in 2004 guidelines for the obligated entities on the characteristics of suspicious transactions including indicators, which were updated on 28 January 2008. The guidelines were divided for the various entities:

- guidelines for credit and financial institutions,
- guidelines for others.

689. Information on current techniques, methods and typologies is also given during the meetings of the Council of Obliged Entities at the AML/CFT Governmental Committee and the Banking Association at least two times a year, and also in various trainings and seminars.

690. The FSA is empowered by § 57 of the FSA Act to issue guidelines of advisory nature to explain legislation regulating the activities of supervised entities. The Law allows the FSA to involve experts and representatives of the supervised entities in the drafting of the advisory

guidelines[50]. On 1 August 2002, the Estonian FSA issued guidelines titled "Additional measures for preventing money laundering in credit and financial institutions" with the aim of assisting towards the building of common principles in the implementation of preventive measures. The guidelines, which are of non-binding nature and serve as recommendations to credit and financial institutions, deal with customer identification of natural and legal persons, non-face-to face relationships, internal control procedures, record keeping procedures and other preventive issues.

691. In view of the enactment of the new MLTFPA in early 2008, the FSA advised the evaluators that they will soon proceed with the issue of revised guidelines.

Recommendation 30

The Financial Supervision Authority

692. The Estonian Financial Supervision Authority (FSA) became operational on 1 January 2002 pursuant to the FSA Act which came into force on 9 May 2001. The FSA brought under its umbrella the Banking Supervision Department of the Bank of Estonia, the Securities Inspectorate and the Insurance Supervisory Agency. The latter two supervisory authorities used to be under the Ministry of Finance. According to the FSA Act, the FSA is an independent institution affiliated to the Bank of Estonia with a six-member Supervisory Council comprised of the Minister of Finance, the Governor of the Bank of Estonia, two members appointed by the Government and two members appointed by the Supervisory Board of the Bank of Estonia. The Supervisory Council decides on the strategy and budget of the FSA and appoints the four members of the Executive Management Board which takes all management and supervisory decisions.

693. The FSA is fully funded by supervised entities through a scheme of supervisory charges calculated on the basis of capital and volume of business.

694. At the time of the on-site visit, the FSA was staffed with 60 persons out of 70 positions. AML/CFT supervision is exercised by the Prudential Supervision Division, which is responsible for market entry, licensing and operational risk, and the Business Conduct Supervision Division which is responsible for the assessment of AML/CFT procedures, on-site inspections, as well as assessment of management information systems (MIS) and integrity issues. Within the Business Conduct Supervision Division, an AML Unit has been created staffed with two persons. Estonian authorities advised that the AML Unit of the FSA is supported by lawyers and supervisory specialists from the Business Conduct Supervision Division during the on-site examinations and assessment of internal procedures of supervised entities.

695. According to information provided, the FSA performed in the last three years (2005-2007) on-site inspections of 5 credit institutions and 2 investment firms while the AML/CFT procedures of 6 financial service providers were assessed in the course of licensing and assessing amendments to internal procedures notified to the FSA by the supervised entities according to § 108 (1) 3) Credit Institution Act.

696. § 30 of the FSA Act deals with the qualifying characteristics of persons employed by the FSA requiring that they should have the required education, sufficient experience and appropriateness to perform their duties and impeccable professional and business reputation. § 34 of the FSA Act

[50] FSA guidelines "Additional measures for prevention of money laundering and terrorist financing in credit and financial institutions" were adopted on 22 October 2008 and published on the web-site of the FSA. In course of drafting the guidelines, several meetings with supervised entities were held and, if justified, their comments and suggestions were taken into account. In the process of drafting the guidelines the experts from different ministries and from University of Tartu were involved. A similar procedure was followed when drafting the previous guidelines.

requires that Estonian FSA's employees have to maintain confidential for an indefinite time any information received in the course of performing their duties.

697. The Estonian FSA's staff comprises financial auditors, financial analysts, IT-specialists, IT-auditors, lawyers, an actuary and experts in financial services.

698. With regard to AML/CFT training, a number of the Estonian FSA's staff participated in courses offered by the UK FSA together with the IMF in the Joint Vienna Institute, the European Institute of Public Administration in collaboration with the Association of Anti Money Laundering Specialists and the Financial Technology Transfer Agency (ATTF) in Luxembourg. The Estonian FSA's staff has also participated in various training courses and seminars organised domestically.

The Financial Intelligence Unit

699. The Estonian FIU maintains a supervisory unit which, at the time of the on-site visit, was staffed with 6 persons out of 8 positions. Staff members involved in supervisory and regulatory work hold academic degrees or diplomas in accountancy, law or management. Starting in 2006, an AML Twinning project with the Dutch FIU took place in Estonia for 18 months during which all the employees of the FIU (including supervisors) were trained by Dutch experts. Moreover, each of the supervisors participates annually in at least 5 internal and external training modules. The staff involved in supervision have also received training about administrative proceedings, procedure of misdemeanours, money laundering etc.

700. § 44 of the MLTFPA sets out the integrity requirements for the staff of the Estonian FIU. According to this provision, only persons with impeccable reputation, the required experience and abilities and high moral qualities may be appointed as officials of the FIU. With regard to confidentiality, § 44(2) of the MLTFPA requires FIU officials to maintain confidential any information obtained in the course of their duties, even after the termination of their services (for further details see above section 2.5, particularly para 353 ff).

Recommendation 32

701. Estonia provided the following statistics concerning on-site visits of the Estonian FIU:

Subjects	2005	2006	2007
Providers of currency exchange services	39	19	18
Organisers of gambling or lotteries	11	19	24
Advocates	0	4	0
Notaries	0	10	48
Auditors	0	0	15
Intermediaries of high-value goods*	11	10	95
Banks**	0	0	5
Total	**62**	**62**	**205**

* Traders plus Real Estate Agencies

** concerning their compliance with the International Sanctions Act.

702. The following breakdown shows the activities of the Supervisory Unit (only) within the FIU:

2005 (2 supervisors)						
	On-site	Precepts	Misdemeanours	Closed	Warnings	Fines

	visits					
Money exchange	39	2	3	-	1	2
Casinos	11	-	2	-	1	1
Traders	9	-	1	1	-	-
Real Estate	2	-	-	-	-	-
Total	**61**	**2**	**6**	**1**	**2**	**3**

2006 (3 supervisors)						
	On-site visits	**Precepts**	**Misdemeanours**	**Closed**	**Warnings**	**Fines**
Money exchange	19	3	3	-	-	3
Casinos	19	4	-	-	-	-
Traders	10	6	-	-	-	-
Notaries	10	2	-	-	-	-
Advocates	4	1	-	-	-	-
Total	**62**	**16**	**3**	**-**	**-**	**3**

2007 (6 supervisors)						
	On-site visits	**Precepts**	**Misdemeanours**	**Closed**	**Warnings**	**Fines**
Money exchange	18	2	3	-	-	3
Casinos	24	4	2	-	-	1
Traders	77	27	-	-	-	-
Notaries	48	3	-	-	-	-
Real Estate	18	8	-	-	-	-
Auditors	15	-	-	-	-	-
Banks*	5	-	-	-	-	-
Total	**205**	**44**	**5**	**-**	**-**	**4**

* concerning their compliance with the International Sanctions Act.

	2005	**2006**	**2007**
No of supervisors	2	3	6
No of on-site visits	61	62	205
… number of proceedings conducted in matters of misdemeanours	6	3	5
… number of precepts	2	16	44
… number of off-site controls	0	0	0

703. The main reasons for sanctions imposed by the FIU were failure by supervised entities to observe identification requirements and to put in place internal controls to prevent money laundering and terrorist financing.

3.10.2 Recommendations and comments

Recommendation 23

704. Estonia should create legal provisions clearly stating that criminal records bar applicants from becoming beneficial owners of a significant or controlling interest in a financial institution.

705. Estonia should introduce an effective registration regime for financial institutions which are not supervised by the Estonian FSA pursuant to § 2 of the FSA Act[51].

Recommendation 29

706. The Estonian FIU should be empowered to compel the off-site production of records from supervised entities for supervisory purposes absent a suspicion of money laundering or terrorist financing.

Recommendation 17

707. The FIU does not have the power to withdraw or suspend the registration of a financial institution falling under its supervision in case it fails to comply with AML/CFT requirements.

708. The indirect sanctioning system of the MLTFPA via precepts of the FSA for provisions of the MLTFPA which are not covered by a specific sanctioning provision of the MLTFPA itself (which is the case for a number of important CDD measures) does not amount to a dissuasive and effective sanctioning regime as it is not possible to sanction violations which have already happened; it only allows to issue precepts to sanction future infringements or failure to comply with the demands made in the precept. Moreover, the amount of the sanctions (a fine of up to 50 000 EEK, i.e. 3 195.58 EUR, for the first occasion and 750 000 EEK, i.e. 47 878.53 EUR, for each subsequent occasion) is not proportionate, effective and dissuasive when it comes to the sanctioning of legal persons. This indirect sanctioning system should be revised and replaced by a direct sanctioning regime providing sanctions in the MLTFPA for all relevant AML/CFT obligations.

Recommendation 25

709. In the light of the changes of the Estonian AML/CFT system because of coming into force of the new MLTFPA, the guidelines issued by the FSA seem already out of date. The FSA should update its own guidelines in the light of the requirements of the new MLFTPA[52].

710. The FIU should issue guidelines explaining the legal requirements and preventive measures described therein to its supervised entities.

Recommendation 30

711. The FSA and the FIU should be provided with more manpower to carry out the supervisory tasks accorded to them by law, particularly regarding on-site supervision.

[51] see FN 49.

[52] The FSA advised that its guidelines "Additional measures for prevention of money laundering and terrorist financing in credit and financial institutions" were adopted on 22 October 2008 and published on its web-site.

3.10.3 Compliance with Recommendations 17, 23, 35 (criterion 25.1 only), 29 and 30

	Rating	Summary of factors underlying rating
R.17	**PC**	• The general provisions of the Credit Institution Act used by the FSA do not provide a clear basis to issue precepts regarding those violations of AML/CFT obligations which are not directly sanctionable by §§ 57 ff of the MLTFPA. • The sanctioning regime utilizing precepts according to §§ 103 ff of the Credit Institutions Act places sanctions at one remove, in that a precept first needs to be issued before formal sanctions, e.g. penalty payments or suspension of a license, can be imposed based on a finding of a violation of the precept. • The FIU does not have powers to withdraw or suspend registration of financial institutions in case they fail to comply with AML/CFT requirements.
R.23	**LC**	• There are no legal provisions to explicitly 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 function. • For financial institutions which are not supervised by the Estonian FSA pursuant to § 2 of the FSA Act no registration requirements apply[53].
R.25	**PC**	• In the light of the changes of the Estonian AML/CFT system because of coming into force of the new MLTFPA, the guidelines issued by the FSA seem already out of date. • The FIU has not yet issued guidelines explaining the legal requirements and preventive measures described therein to its supervised entities.
R.29	**LC**	• There is no explicit provision empowering the FIU to compel the off-site production of records from supervised entities for supervisory purposes absent a suspicion of money laundering or terrorist financing.

[53] see FN 49.

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and analysis

712. Money transfer services are provided, apart from banks, by the Estonian Post, which acts as an agent of Western Union, eight money transfer businesses which represent international payment networks (e.g. Western Union, MoneyGram and others), currency exchange bureaux (135 at the time of the site visit) and six providers of services of alternative means of payment.

713. With regard to the Estonian Post, a state owned entity, it is noted that the Postal Act which entered into force on 1 July 2006 (replacing the previous law which came into force on 8 January 2004) allows the provision of financial services through the postal network all over Estonia with regard to payments of pensions and benefits and cash transfers. According to the Postal Act, the Estonian Post has been licensed by the Estonian National Communications Board. The Estonian Post is also providing in cooperation and on the basis of an outsourcing agreement with the biggest bank in Estonia, a number of banking services, including account opening. The Estonian Post is part of the obligated entities under §§ 3 and 6 of the MLTFPA and subject to supervision by the Estonian FIU under § 47 of the MLTFPA. Until the time of the on-site visit, the FIU had not performed any on-site inspections of the Estonian Post. The Estonian authorities advised that in March 2008 the FIU performed 3 on-site inspections to Estonian Post; furthermore, it was explained that the FIU advised the Estonian Post in drafting their internal AML/CFT procedures and provided training for the staff.

714. With regard to other providers of payment services (i.e. money transfer businesses and currency exchange bureaux) as well as providers of services of alternative means of payment, § 52 of the MLTFPA requires that these should be registered in the Register of Economic Activities maintained by the Ministry of Economic Affairs. § 53 of the MLTFPA prescribes the contents of an application for registration. These include details on the service provider and its activities, the name and contact details of the persons providing the payments services (Estonian authorities advise that this includes agents of other payment service providers), the address or addresses of the place or places of provision of the service or the address of the website used for the provision of the service, and details on the directors and beneficial owners. According to § 25 (1) and 26 (1) of the Register of Commercial Activities Act, this information must be regularly updated (at least annually). The information in the Economic Activities Register is public. Failure to register or update registry information is punishable according to § 64 of the MLTFPA by a fine up to 300 fine units. § 55 MLTFPA stipulates that registration can be refused if the service providers, directors or beneficial owner(s) have been convicted for a crime under §§ 237-237[3], 394-396 of the Penal Code (this list includes the money laundering and the terrorist financing offence) or have committed another intentional crime and the terms arising from § 25(1) of the Penal Register Act have not expired. For the same reasons stated above, a registration should also be deleted if information to that effect is received for a registered service provider. Under § 47(1) of the MLTFPA, the FIU is responsible for the supervision of the payment service providers. As informed by the FIU, currency exchange bureaux have been subject to on-site inspections since 2005. To this end, the FIU provided the following statistical information:

	2005	2006	2007
On-site visits	39	19	18
Precepts	2	3	2
Misdemeanours	3	3	3

715. No on-site visits have been made by the FIU to money transmitters and providers of alternative means of payment other than the Estonian Post, and no system for monitoring their operations has been introduced.

716. Providers of services of alternative means of payment are defined under § 6(4) of the MLTFPA as "*a person who [...] through a communications, transfer or clearing system buys, sells, or mediates funds of monetary value*". Essentially, these payment service providers use unconventional methods outside traditional banking channels which allow for digital transfer of funds. Transactions are performed through the internet, other communication channels or smart cards which have a built-in microprocessor that records the monetary value. Transfers of money are made instantly, securely and anonymously. In Estonia, these payment service providers use the so-called electronic purses and digital precious metal based payments systems; e.g. E-Gold. E-Gold means an account based e-currency (electronic payment instrument) issued by the payment services providers (i.e. internet money). In view of the enhanced money laundering and terrorist financing risks, entities involved in these type of payment services have been brought under the Estonian MLTFPA and are, hence, required to register and apply preventive measures against money laundering and terrorist financing.

717. § 63 of the MLTFPA stipulates that failure by the manager or employee of a payment service provider to identify, verify or communicate information about a payer or violation of Regulation (EC) No. 1781/2006 is punishable by a fine of up to 300 fine units (i.e. 18 000 EEK or 1150.40 EUR) and, in the event that the failure is committed by a legal person, is punishable by a fine of upto 500 000 EEK (31 955.82 EUR). In addition, the general sanctioning mechanisms described in §§ 57 to 62 and 64 of the MLTFPA are equally applicable to providers of payment services.

3.11.2 Recommendations and comments

718. The FIU should establish a programme of on-site inspections of all payment service providers for checking compliance with their AML/CFT obligations.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**LC**	• Lack of effective supervision of payment service providers.

4 PREVENTIVE MEASURES – DESIGNATED NON FINANCIAL BUSINESSES AND PROFESSIONS

4.1 Customer due diligence and record-keeping (R.12)

(Applying R.5 to R.10)

4.1.1 Description and analysis

719. § 3 MLTFPA specifies that its provisions apply, besides credit and financial institutions also to the following persons

a) Organisers of games of chance (i.e. casinos and gambling houses)
b) Persons who carry out or act as intermediaries in transactions with real estate
c) Traders when a cash payment in a lump sum or in several related payments is made of no less than 200 000 EEK (i.e. 12 782.32 EUR)
d) Pawnbrokers
e) Auditors and providers of accounting services
f) Providers of accounting or tax advice services
g) Providers of trust and company services
h) Notaries public, attorney, bailiffs, trustees in bankruptcy, interim trustees in bankruptcy and providers of other legal services when
   - acting in the name and on account of a customer in financial or real estate transaction;
   - they plan a transaction or perform an official act concerning
     - the purchase or sale of immovable property, enterprises or companies
     - the management of a customer's money, securities or other property
     - the opening or managing of bank or security accounts
     - the acquisition of funds necessary for the foundation, operation or management of trusts, companies or other similar entities.

720. According to Estonian's commercial registry, the number of obligated persons, other than credit and financial institutions, are the following:

Obligated persons	Nr.
Sellers of motor vehicles	331
Sellers of antiques	27
Jewellers, sellers of valuables and watches	69
Real estate agents, developers, purchases, sales, lease and evaluation of real estate	1650
Lawyers and law offices	756
Notaries public	129
Trustees in bankruptcy	85
Bailiffs	49
Auditors	361
Accountants	768
Tax advisors	5
Trust and company service providers	26
Organisers of games of chance	17
Gambling locations	156

721. § 16(1) MLTFPA requires the organisers of games of chance to identify and verify the residential address and the profession or activities of a client who pays or receives in a single transaction or several related transactions an amount exceeding 30 000 EEK (1 917.34 EUR) or the equivalent in another currency. The MLTFPA refers only to residential address and profession or activities and does not require the verification and registration of the name of the client. For such limited transactions, casinos are not required to make copies of identification documents as

otherwise required by § 23 (2) of the MLFTPA. Estonian authorities advised that in practice, organisers of games of chance verify and register address and business activity filed by name.

722. § 16(3) MLTFPA requires notaries public to identify clients and apply due diligence measures on the basis of the Notarisation Act and the Notaries Act with the specifications provided by the MLTFPA (*lex specialis*). According to § 18 of the Notarisation Act, a notary public must obtain and assess information about the essence and goals of a specific transaction having regard to the parties of a transaction, the value of the transaction and the requirements of the MLTFPA. As the Estonian authorities have stated, upon certification of contracts of purchase and sale of immovables or undertakings or upon certification of foundation resolutions or memoranda of association of companies, a notary public must identify the place of residence and the area of activity or profession of natural persons participating in the transaction (incl. the representative of a legal person) as well as the beneficial owner. A notary public does not only identify the will of the parties to a transaction as required in § 18 of the Notarisation Act, but must also fulfil the CDD obligations under the MLFTPA.

723. § 16(3) of the MLTFPA allows a notary public, bailiff, trustee in bankruptcy, auditor, attorney or another legal service provider not to identify and verify the identity of customer, including the beneficial owner, when establishing a business relationship or entering into a transaction, if this is necessary for not interrupting the ordinary course of professional activities and provided that the risk of money laundering and terrorist financing is low.

724. Except for the above special provision of § 16 of the MLTFPA, DNFBP are required to apply due diligence measures specified in Division 1 of Chapter 2 of the MLTFPAs which are also applicable to other obligated entities. Hence, the observations made with regard to Recommendation 5 concerning financial institutions are equally applicable for DNFBP.

725. With regard to criterion 12.2, the comments and observations made for credit and financial institutions under Recommendation 6, 8 (with the exception of criterion 8.2 of the FATF Methodology), 9, 10 and 11 equally apply for DNFBP as the relevant provisions of the MLTFPA apply to both financial institutions and DNFBP. Specifically, although financial institutions are prohibited from opening accounts or entering into transactions with clients who do not maintain a business relationship without the client being present, DNFBP are required under § 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 DNFBP should take to mitigate the risks for non-face-to face relationships and transactions. It is further noted that the power given to the Minister of Finance to issue a regulation to lay down the requirements for the internal rules of procedure for customer due diligence and risk management relates only to credit and financial institutions and not DNFBP (§ 30 (6) MLTFPA).

4.1.2 Recommendations and comments

726. Generally, in Estonia the coverage of DNFBP is very complete and in line with international standards. The interviewees with whom the evaluation team met were also aware of the new MLTFPA (though not necessarily with its content as it came into force shortly before the on-site visit).

727. As the relevant provisions of the MLTFPA apply both to financial institutions and DNFBP in the same way, the comments and observations made for credit and financial institutions under Recommendation 5, 6, 8, 9, 10 and 11 equally apply for DNFBP (with the exception of criterion 8.2 of the FATF Methodology). Thus the Recommendations there are also valid concerning DNFBP.

728. A particularity concerning DNFBP is that § 30 (6) MLTFPA applies only to financial institutions but not to DNFBP. The evaluators recommend that DNFBP should also be required through means of secondary legislation (i.e. Minister of Finance's regulation) to set up comprehensive internal control mechanisms for managing AML/CFT risks having regard to the sort, scope and complexity of their activities.

729. Furthermore, though DNFBP are required under § 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 DNFBP should take to mitigate the risks for non-face-to face relationships and transactions. Estonian authorities should issue such guidance.

730. Casinos should be required not only to identify but also to verify the name of a client who engages in financial transactions equal or above the threshold given by criterion 12.1 of 3 000 USD/EUR; though not required by the Methodology, it may be easier simply to amend the law by using the existing (lower) threshold of the MLTFPA which is 30 000 EEK (1 917.34 EUR).

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors underlying rating
R.12	**PC**	• The same concerns in the implementation of Recommendations 5, 6, 8 – 11 apply equally to DNFBP (see section 3 of the report). • There are no Regulations/Directives to DNFBP laying down requirements for internal control procedures for managing AML/CFT risks. • Though DNFBP are required under § 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 DNFBP should take to mitigate the risks for non-face-to face relationships and transactions. • Casinos are required to identify but not to verify the name of a client who pays or receives in a single transaction or several related transactions an amount exceeding 30 000 EEK (1 917.34 EUR) or the equivalent in another currency.

4.2 Suspicious transaction reporting (R. 16)

(Applying R.13 - 15 and 21)

4.2.1 Description and analysis

731. Criterion 16.1 requires essential criteria 13.1 – 4 to apply to DNFBP. Criteria 13.1-3 are marked with an asterisk. The first two require reports to the FIU where the obliged entity suspects or has reasonable cause to suspect, that funds are the proceeds of criminal activity or has reasonable grounds to suspect or suspects, that funds are linked to terrorism etc or those who finance terrorism. The MLTFPA keeps DNFBP to the same standards as financial institutions and requires them to report to the FIU in respect of suspicious transactions. As broadly described under section 3.7 for financial institutions, the same issues and deficiencies apply equally for DNFBP.

732. Concerning legal professional privilege, § 32 (4) MLTFPA stipulates that the notification obligations do not apply to notaries public and advocates "*when evaluating a customer's legal position, defending or representing the customer in court, challenge or other such proceedings*[54]*, including providing the customer with consultations regarding the initiation or avoidance of proceedings, regardless of whether the information has been received before, during or after proceedings*". The Estonian authorities explained this provision in more detail and explained that they interpret it in such a way that the notification obligation does not apply to consultations provided regarding the initiation or avoidance of a proceeding, regardless of whether the information is obtained prior to, in the course of or after the conclusion of the proceeding. The principle of legal professional privilege is applicable in Estonia concerning criminal, civil and administrative proceedings and in challenge proceedings. Legal professional privilege does not extend to cases where an advocate or notary public acts as a representative of the client in financial or real estate transactions. Furthermore, legal professional privilege does also not extend to provision of a legal service which lies in leading or implementing a transaction, purchase or sale of immovable property or undertaking for a client or management of a client's money, securities or other property or opening bank or securities accounts or acquisition of funds required for foundation, operation or management of a company or foundation or operation or management of a trust, company or other similar entity or in carrying out an official act. The obligation to keep the professional secrets of advocates and notaries public does not apply if the legal counsel participates in money laundering or terrorist financing or 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.

733. In Estonia, no obligated entities are allowed to report suspicious transactions through a self-regulatory organisation (SRO).

734. In practice, notaries seem engaged and to fulfil their obligations; the FIU explained that the quality of STRs coming from notaries is excellent. However, other DNFBP are not so active. Between 2003 and 2007 Lawyers sent only 10 reports, real estate dealers ("Persons who carry out or act as intermediaries in transactions with real estate") sent only 2 reports and accountants/auditors sent only one STR. As mentioned above (para 616), the evaluators were advised by the Estonian authorities, that as the transactions of these entities pass through the banking sector, and as banks also are obliged to report any suspicious transactions that could indicate money laundering or terrorist financing, there is no need of double reporting (a view not shared by the evaluation team as all obliged entities should follow their own reporting obligations and not rely on others).

735. With regard to Recommendation 15, it is noted that § 29(4) MLTFPA exempts DNFBP from the obligation to appoint a contact person if they do not wish to do so and, in such an event, it specifies that the duties of a contact person shall be performed by the management board of a legal person, the head of a branch of a foreign company registered in Estonia or the sole proprietor. In all other respects the duties of a contact person of a DNFBP are the same as for credit and financial institutions.

736. § 29 (1) MLTFPA requires all obligated persons to establish written rules of procedure in respect of due diligence and risk management, collection and storage of data, performance of the notification obligation as well as rules of internal procedure for checking adherence thereof. §§ 30(1) and 30(2) MLTFPA stipulate that the rules of procedure should correspond to the sort, scope and complexity of the economic and professional activities of the obligated person and that these rules of procedure should be regularly reviewed and updated if necessary. § 30(6) stipulates that

[54] The Estonian authorities explained that "challenge proceedings" refers to an administrative appeal procedure. 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 (§§ 71 and 73 Administrative Procedure Act).

the Ministry of Finance should establish the requirements of rules of procedures, including the internal audit rules, for credit and financial institutions only. Hence, obligated persons, other than credit and financial institutions, will not be covered by the regulation to be issued by the Ministry of Finance. It is noted that the MLTFPA imposes no obligation on DNFBP for an independent audit function to test compliance neither does it require screening procedures when hiring employees.

737. With regard to the application of Recommendation 21 by DNFBP, it is noted that the provisions for credit and financial institutions referred to in Part 3.6 of this assessment report equally apply to DNFBP.

738. When it comes to reporting related to terrorist financing, the interviewees were aware of guidance but some mentioned that they would like to receive a consolidated terrorist list in a user-friendly format which would facilitate the identification of situations suspected to be related to terrorist financing (though it has to be noted that the FIU and FSA provide regular updates of the lists on their respective websites – see above paragraphs 281 f; but it seems that some obligated persons were not aware of this service; moreover, the services provided for by the FIU on their website does not provide a list but only a search capability which cannot be used for red-flag systems which would automatically indicate a match with the list) .

4.2.2 Recommendations and comments

739. The same deficiencies in the implementation of Recommendations 13, 15 and 21 in respect of financial institutions apply equally to DNFBP and the Recommendations there concerning financial institutions are also valid in the context of Recommendation 16. In terms of effectiveness, some DNFBP seem less aware of their obligations; e.g. lawyers, real estate dealers as well as accountants and auditors have only sent a very small number of STR so far. Further outreach to these entities that they better understand their reporting obligations is necessary (though it has be noted that the Estonian FIU has already provided a number of training seminars to these entities).

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**PC**	• The same deficiencies in the implementation of Recommendations 13, 15 and 21 in respect of financial institutions apply equally to DNFBP. • Lawyers and real estate dealers as well as accountants and auditors have sent only a very small number of STR so far.

4.3 Regulation, supervision and monitoring (R. 24-25)

4.3.1 Description and analysis

Recommendation 24

740. According to an amendment of the Gambling Act, the Securities Authorities Act and the Lotteries Act in 2005, the Estonian Tax and Customs Board of the Ministry of Finance is responsible for issuing gambling licenses and supervising gambling operators. The on-site inspections and other supervisory procedures employed by the Tax and Customs Board aim at checking existence of revenue stamps on gambling machines and tables, registration of winnings, the age of gamblers, existence and availability of rules of gambling and validity of licenses. The FIU is the authority responsible for checking that gambling operators comply with the requirements of the MLTFPA. At the time of the on-site visit, there were 18 licensed operators of games of chance which maintained 188 gambling sites (casinos), 5.167 gambling machines and 62 gambling tables. Although not prohibited by law, the Estonian authorities advised that there were no internet casinos operating out of Estonia. During the years of 2005-2007, the Estonian Tax and Customs Board carried out on-site inspections at 108 gambling locations. In five cases, the Tax and Customs Board discovered violations of the former MLTFPA and passed that information to the Estonian FIU, which advised that additional on-site inspections were made in these cases. Between 2005-2007, the FIU carried out 54 on-site visits to casinos which ended up in the issue of 8 precepts, 4 misdemeanours and 2 fines.

741. The criminal record of staff of gambling locations is checked by the Tax and Customs Board through checks made in the database of the criminal register with the aim of prohibiting employment at casinos of persons who have been convicted for an intentionally committed criminal offence and whose punishment for such an offence has not expired (§ 13 (2) of the Gambling Act). It is noted that the Tax and Customs Board has limited access to the database of the criminal register through on-line equipment and, hence, it is prevented from checking current convictions for the staff of casinos in a fast and timely manner.

742. Licenses to casinos are also issued by a Government Committee established under the Ministry of Finance in which the FIU also participates. The evaluators were advised that at the licensing stage "fit and proper" checks, including checks of criminal records, are made out of practice on all physical persons who are the beneficial owners of more than 5% of the applicant company's share capital. However, it is noted that transfers of shares after obtaining a license, do not require the prior approval of the Ministry of Finance or other Estonian authorities. The evaluators were also informed that casinos are not required to file any reports or returns with the authorities regarding their financial position and activities after licensing. Furthermore, currency exchange bureaux operate in casinos which are however, licensed and registered under a separate procedure. Clients' winnings are paid either in cash or a bank transfer but only in EEK. It is noted that § 16 (1) MLTFPA requires an organiser of games of chance to establish and verify the identity of a client who pays or receives in a single transaction or several related transactions an amount exceeding 30 000 EEK (1 917.34 EUR) or the equivalent in a foreign currency[55].

743. Under the former MLTFPA, the FIU carried out on-site inspections to other DNFBP such as traders, real estate agents, notaries, lawyers and auditors. From 2005 to 2007, the FIU made 99 on-

[55] Estonian authorities advised that the new Gambling Act has passed Parliament and will become effective on 1 January 2009, eliminating all these deficiencies (the §§ 11-15 regulating the procedure of obtaining qualifying holdings in gambling operators, chapter 4 providing on-going monitoring and supervision of all gambling operations by the supervisory authority, i.e. the TCB).

site visits to traders, 20 to real estate agents, 38 to notaries, 4 to lawyers and 15 to auditors. No on-site visits have been made to trust and company service providers and pawnbrokers[56].

744. There were no provisions in the former MLTFPA about trusts or company services providers. With regard to the obligations from the 3rd EU AML Directive, Estonia has now addressed this issue: hence, trust and company service providers are now defined under § 7 of the MLTFPA as natural or legal persons whose primary economic or professional activity lies in providing a third party with trust and company services prescribed in the law. This means that not all persons providing trust and company services need to register and, thus, be supervised, under § 52 MLTFPA if they are also engaged in other unrelated activities which constitute their main source of income. The evaluators consider this to be a shortcoming in the supervision and monitoring of trust and company service activities which needs to be remedied, particularly as this is not only a hypothetical problem considering that the Estonian system has some comparable arrangements like trusts and also allows foreign trusts to operate in Estonia (for details see below section 5.2).

745. § 47 MLTFPA stipulates that the Estonian FIU is responsible for supervising compliance with the provision of the MLTFPA by organisers of games of chance (i.e. casinos and gambling houses), real estate agents, pawnbrokers, auditors, accountants, tax advisors and trust and company service providers. § 47(3) MLTFPA specifies that the Estonian Bar Association is responsible for the supervision of members of the Bar Association. It is noted that, at the time of the on-site visit, 646 lawyers were members of the Bar Association but, having regard to the fact that the Estonian law does not make it compulsory for a practising lawyer to become a member of the Bar Association, it was estimated that 116 lawyers have chosen to remain outside the membership of the professional association which means that they do not fall under the supervision of the Bar Association; for these lawyers, the FIU would be responsible for supervision (§ 47 (1) MLTFPA) but so far the FIU did not yet supervise any of them and it was also acknowledged that the number of lawyers acting outside may be higher than 116.

746. § 47(4) MLTFPA provides that the Ministry of Justice is the supervisory authority for notaries but it may delegate this power to the Chamber of Notaries. There was apparently some confusion as the implementing provisions of the MLTFPA (§ 72) included an amendment to § 44 (1) of the Notaries Act stating that the Chamber of Notaries "*exercises supervision over fulfilment by notaries public of the requirements of the Money Laundering and Terrorist Financing Prevention Act and legislation adopted on the basis thereof*". This may not necessary be a contradiction as the MLTFPA could also assign two bodies at the same time as supervisors for notaries but with regard to the fact that the Ministry of Justice already officially delegated its AML/CFT supervisory authority concerning notaries to the Chamber of Notaries not even a theoretical conflict of competences could arise. Moreover, the amended § 5(2) of the Notaries Act provides that the Ministry of Justice may give instructions for exercising supervision and change the decisions approved by the Chamber of Notaries on these issues. Estonian authorities advised that services described in the Notaries Act may only be provided by notaries; for notaries the membership to the Chamber of Notaries is mandatory.

747. § 48 MLTFPA empowers the supervisory authorities (FIU, Bar Association, Chamber of Notaries) to carry out on-site inspections and obtain information, documents and copies thereof in the course of those inspections as well as written and oral explanations from the supervised persons, their directors and employees.

748. The FIU is also given the power under § 38 of the MLTFPA to issue precepts and perform other administrative acts in order to exercise its functions deriving from the MLTFPA. The FIU is also responsible for the carrying out of the extrajudicial proceedings for the misdemeanours provided in § 58 (violation of requirement to register and preserve data) and § 62 (failure to apply

[56] The FIU advised that in 2008 it has performed on-site visits to 60 pawnbrokers which resulted in 29 fines.

internal security measures) which provide for a fine of up to 300 fine units à 60 EEK (18 000 EEK; 1150.40 EUR) or 500 000 EEK (31 955.82 EUR) if the breach is committed by a legal person. It has to be noted that the sanctions provided in § 57 MLTFPA for failure to comply with the identification requirements applies to credit and financial institutions only.

749. During 2005-2007, on-site inspections and sanctions imposed by the FIU against DNFBP were as follows:

	On-site visits			Precepts	Misdemeanours	Fine
	2005	2006	2007			
Casinos	11	19	24	8	3	2
Traders	10	12	77	33	1	-
Real Estate	2	-	18	8	-	-
Advocates	-	4	-	1	-	-
Auditors	-	-	15	-	-	-
Notaries	-	10	48	-	-	-

750. It is noted that the number of obligated persons is huge (for a list see above para 720) and, hence, requires the allocation of substantial human resources for the effective monitoring and supervision by the FIU.

751. With regard to Notaries, the Chamber of Notaries is empowered under Section 5 of the Notaries Disciplinary Act to initiate disciplinary proceedings against a notary who has committed a disciplinary offence, including violation of the provisions of the MLTFPA. In such an event, the chamber of Notaries shall inform the Minister of Justice who shall issue a directive for the initiation of the disciplinary proceedings by establishing a committee for examining the case. If the committee concludes that the notary has breached the MLTFPA, then the Minister of Justice proceeds with the imposition of a disciplinary penalty which involves a reprimand, a fine of up to 10 000 EEK (i.e. 639.11 EUR) or removal from office. In the case of a minor violation, the Minister of Justice may refer the case to the Chamber of Notaries which may oblige the notary to undertake additional training as well as inform the body of notaries of the offence committed[57].

752. With regard to lawyers, the evaluators were advised during their meeting with the representatives of the Estonian Bar Association, that the legal service providers in Estonian are mainly involved in litigation proceedings and are rarely involved in trustee and fiduciary services or handling clients' money. Estonian lawyers are also not involved in company formation and administration, a service which is more often provided either by notaries or specialised firms. It seems that at the time of the on-site visit, the Estonian Bar Association was not entirely sure of the specific obligations assigned to the law profession by the MLTFPA. However, the Estonian Bar Association has adopted on 5 February 2008 guidelines for the members of the Bar Association regarding reporting to the FIU, which were approved by the FIU. So far, no on-site visits have been carried out yet [58].

[57] The Estonian authorities advised that after the on-site visit, the Estonian Chamber of Notaries has adopted, in a general meeting on 1 November 2008, the due diligence measures and rules of procedure provided in the MLTFPA. The Chamber of Notaries has exercised supervision over the notaries (until now 4 notaries) regarding compliance with the MLTFPA pursuant to general procedure together with the Ministry of Justice. The Chamber of Notaries has been cooperating with the FIU regarding information from the FIU, but has not yet found any violations. Active monitoring of the requirements of the MLTFPA and legislation adopted on the basis thereof is starting in 2009. The Ministry of Justice has not yet initiated any disciplinary proceedings against a notary for wrongful performance or unsatisfactory performance of official duties deriving from the MLTFPA.

[58] The Estonian authorities advised that in spring 2008 the Estonian Bar Association (BA) recruited a lawyer to work on on-site supervision of lawyers with respect to their obligations arising from the MLTFPA. No on-site visits have been carried out yet. The Board of the Estonian Bar Association has passed the guidelines to the law offices. BA has adopted guidelines regarding identification and fulfilling other obligations arising from the MLTFPA on 9 September 2008. This guideline has also been approved by the FIU in the framework of co-

753. Regarding sanctioning powers of the Estonian Bar Association, § 19 of the Bar Association Act provides: "*§ 19. Disciplinary Liability - (1) The court of honour may impose a disciplinary penalty for violation of legislation which provides for the activities of advocates or for violation of the requirements for professional ethics. (2) Disciplinary penalties are: 1) reprimand; 2) fine in favour of the Bar Association in the extent of up to two months earnings of the advocate; 3) suspension of professional activities for up to one year; 4) disbarment.*"

Recommendation 25

754. Section 39 empowers the FIU to issue guidelines of advisory nature for the explicit purpose of explaining the legislation for the prevention of money laundering and terrorist financing. The same section stipulates that the FIU should issue advisory guidelines regarding the characteristics of suspicious transactions and terrorist financing. The guidelines for the characteristics of terrorist financing should be issued in coordination with the Security Police Board. In 2004, the FIU issued guidelines for the obligated entities on the characteristics of suspicious transactions including indicators. The guidelines were divided for the various entities (guidelines for credit and financial institutions/guidelines for others). In 2007, the FIU developed in cooperation with the Security Police Board also a guideline particularly related to the characteristics of terrorist financing related transactions. Concerning DNFBP, the FIU has not yet issued advisory guidelines to explain legislation on AML/CFT matters. However, no other guidelines have been issued on any additional measures that DNFBP should take to ensure that their AML/CFT measures are effective. It is also noted that the Chamber of Notaries and the Estonian Bar Association have not issued any guidelines containing indicators of money laundering and terrorist financing or recommending the assumption of a additional AML/CFT measures.

755. As stated above, guidelines issued by the FIU are of strictly advisory nature and, hence, they are not legally binding, enforceable and sanctionable.

4.3.2 Recommendations and comments

Recommendation 24

756. Beneficial owners and managers of casinos should be subject to fit and proper checks at the time of licensing, transfer of ownership or taking up employment.

757. The Law should require the registration of all persons providing trust and company services irrespective of whether or not the provision of such services constitute their primary professional or economic activity.

758. The Estonian Bar Association is responsible for the AML/CFT supervision of their members only. It is not compulsory for a practising lawyer (independent legal professionals) to be a member of the Bar Association, thus they fall only under the supervision of the FIU (§ 47 (1) MLTFPA) and were not supervised so far. The FIU should identify how many of such lawyers exist (e.g. by a mandatory registration requirement) and should supervise them (alternatively it could be made mandatory for these lawyers to become members of the Bar Association and that they are supervised by the Bar Association).

759. The Chamber of Notaries and the Estonian Bar Association should establish monitoring and supervisory mechanisms for checking compliance of their members with the AML/CFT obligations.

---

operation between the FIU and the Board of the BA. BA has included MLTFPA issues in the training programs of lawyers. On site inspections are planned to start within next couple of months.

760. Additional staff should be provided by the FIU to ensure adequate and effective supervision of all obligated entities subject to its supervision.

Recommendation 25

761. The FIU, the Chamber of Notaries and the Estonian Bar Association should prepare and issue guidelines assisting obligated entities in complying with their AML/CFT obligations.

4.3.3 Compliance with Recommendations 24 and 25 (criterion 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.5 underlying overall rating
R.24	**PC**	• Lack of fit and proper checks to beneficial owners and managers of casinos. • Not all trust and company service providers required to be registered. • Lawyers acting outside the Bar Association are not subject to effective supervision by the FIU. • Lack of adequate mechanisms for supervision by the Estonian Bar Association and Chamber of Notaries. • Lack of sufficient supervisory staff in the FIU.
R.25	**PC**	• Insufficient guidance to DNFBP by supervisory bodies (FIU, Bar Association, Chamber of Notaries).

4.4 Other non-financial businesses and professions/ Modern secure transaction techniques (R.20)

4.4.1 Description and analysis

762. Criterion 20.1 states that countries should consider applying Recommendations 5, 6, 8 to 11, 13 to 15, 17 and 21 to non-financial businesses and professions (other than DNFBP) that are at risk of being misused for money laundering or terrorist financing. The MLTFPA goes beyond the categories of DNFBP that need to be covered under the FATF Recommendation.

763. § 3 of the MLTFPA specifies that the obligations prescribed in the Law are also applicable to
a) traders covered by the Trading Act when a cash payment of no less than 200 000 EEK (i.e. 12 782.32 EUR) is made in one or a series of related transactions,
b) pawnbrokers and
c) organisers of games of chance besides casinos (i.e. all types of gambling houses).

764. Regarding traders and pawnshops, the FIU carried out a search in the commercial register and extracted the number of organisations which are captured by the MLTFPA:

Entities	No
Pawnshops	81
Wholesale and retail sale of cars, trucks, trailers and small buses	297
Intermediation of machinery, industrial equipment, ships and aircraft	34

Retail sale of valuables, jewellery and watches	69
Retail sale of antiques	27
Total	**508**

765. The banking sector in Estonia has achieved a remarkable growth in the use of modern technology for conducting financial transactions. Payments in Estonia are mostly made through the banking channels or the use of credit or debit cards and cash is not very common for effecting payments. According to the statistics of the Bank of Estonia, the number of payments initiated in cash in credit institutions, represents only 0.26% of all payments. Moreover, the currency in circulation represents 5.1% of GDP compared to an average of 6.1% in the Euro area.

4.4.2 Recommendations and comments

766. Estonia is in compliance with Recommendation 20.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**C**	

5 LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANISATIONS

5.1 Legal persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and analysis

767. Recommendation 33 requires countries to take legal measures to prevent the unlawful use of legal persons in relation to money laundering and terrorist financing by ensuring that their commercial, corporate and other law require adequate transparency concerning the beneficial ownership and control of legal persons. Competent authorities must be able to have access in a timely way to beneficial ownership and control information, which is adequate, accurate and timely. Competent authorities must also be able to share such information with other competent authorities either domestically or internationally. Bearer shares issued by legal persons must be controlled.

Transparency concerning beneficial ownership and access to information (criteria 33.1 and 33.2)

768. The procedures for establishing a company and the type of companies in Estonia that can be registered with the commercial register are described in Section 1.4 of this report.

769. Generally it can be said that systems are in place to understand the ownership and management of legal persons but the concept of beneficial ownership is not present in the Estonian company legislation. The concept is taken and applied within the framework of combating money laundering and terrorist financing.

770. The transparency with respect to the legal persons is provided through the register proceedings. Information on the shares of private limited liability companies is available in the Commercial register. The ownership of shares in public limited companies could be traced at the Estonian Central Register of Securities where the issuance of shares and their transfer are registered. As regards management and control, all commercial companies are required to provide this information to the Commercial Register.

771. The Commercial register is maintained by the Registration departments of County Courts. It contains information on sole proprietors, general partnerships, limited partnerships, private limited companies, public limited companies, commercial associations, European companies and branches of foreign companies. Entries in the register are made by the registrar in whose territorial jurisdiction the seat of the company or the enterprise of a sole proprietor is located. According to Estonian authorities the register has a strong conclusive force and aim at ensuring legal certainty.

772. The register is maintained electronically. Entries in the commercial register are public. Everyone has the right to examine the card register and the business files, and to obtain copies of registry cards and of documents in the business files (§ 28 of the Commercial Code). A register entry has legal effect with respect to third parties as from the moment when data about making the entry (dates of submission of the application, making the entry order and making the entry, etc.) has been published on the web-page of the Centre of Registers and Information Systems (www.rik.ee).

773. Register entries are made on the basis of digitally signed or notarised applications as well as on the basis of court judgments. Registers are maintained at the court to ensure the independence and legal competence of the registrar. Original documents (including a bank notice concerning payment of a monetary contribution, a notice concerning the planned main activity) and notarised

copies thereof are submitted to the registration department of the court. According to § 33 (5) of the Commercial Code the registrar shall not make an entry in the register if the petition or documents appended thereto do not comply with the law or are submitted prior to the term permitted or after the term prescribed by law. Apart from that and concerning verification of data it has to be noted that controls are performed only formal on the completeness of the documents. The registering court is only obliged to determine whether the application contains all requirements and if the stipulated documents have been attached. Consequently, the court is not authorised to engage in determining the authenticity of the documents or of their content. Thus, rejection of entry into the court register would only take place in case of obvious incorrectness or invalidity of the data submitted. In this respect the failure to submit the required information or the submission of incorrect information is sanctionable by a fine according to § 71 Commercial Code ("Liability of undertaking"). Every member of the management board may be punished separately by a fine in the amount of up to two hundred minimum daily rates for submission of false information or failure to submit the prescribed information to the registration department of the court (§ 71 of the Commercial Code in conjunction with §§ 46 and 601 CCP). Imposition of fines may be repeated until the corresponding deficiency is eliminated. Intentional submission of false information to the registration department of the court or to the notary may be punished as a criminal offence with a fine or up to 2 years' imprisonment (§ 281 PC).

774. Private limited companies and public limited companies must submit annual reports to the Register even if the company has no economic activities.

775. If a foreign company wants to permanently offer goods or services in its own name in Estonia, it must register a branch in the commercial register. A branch of a foreign company is not a legal person. The company is liable for the obligations arising from the activities of the branch. The information about foreign companies from the EU is available via an internet-based system, the European Business Register (EBR).

776. In order to enter a company in the commercial register, the management board must submit an application to the commercial register. The application should be accompanied by the memorandum of association specifying the names and places of residence or seats of the founders and the names and personal identification codes of the members of the supervisory board, and of auditors, if the company has any auditors (§§ 138, 144, 243, 250 Commercial Code).

777. If a company has a supervisory board and auditors, the registration department of the court should be notified of a change in the membership (the names, personal identification codes, dates of entry into force of authorisations and addresses of the members) within five days. The registrar may also be notified electronically of changes in information (§§ 184, 309, 318, 320 Commercial Code).

778. According to § 182 Commercial Code, the management board of a private limited company is obliged to keep a list of shareholders which sets out the names, addresses, personal identification codes or registry codes and the nominal value of their shares. The shareholders, members of the management board and supervisory board, competent state agencies and other persons with a legitimate interest have the right to examine the list of shareholders.

779. If so decided by the shareholders, shares may be entered in the Estonian Central Register of Securities. In such case, the list of shareholders shall be maintained by the registrar of the Estonian Central Register of Securities. The management board of a private limited company is obliged to ensure timely submission of correct information provided by law to the person maintaining the list of the shareholders. Upon entry of shares in the Estonian Central Register of Securities, the management board of the private limited company shall promptly submit a notice from the registrar of the Estonian Central Register of Securities concerning registration of the shares to the registrar of the commercial register.

780. The list of shareholders of private limited companies and shareholders of public limited companies who hold more than ten percent of the votes determined by shares are also disclosed in the commercial register. This data has informative meaning. The registrar shall input the list of shareholders of a private limited company in the register on the basis of the documents of establishment and amend the data on the basis of the notice of transfer of the share and the resolution on increase and reduction of share capital. The list of holders of shares who hold more than ten per cent of the votes determined by shares shall be sent by the Estonian Central Register of Securities to the Commercial Register once in a quarter.

781. The transfer of a share of a private limited company must be notarised, except in the case when the list of shareholders is maintained by the Estonian Central Register of Securities (ECRS).

782. The share register of public limited companies is maintained by the Estonian Central Register of Securities (ECRS). Before entry in the commercial register, the new public limited company shall register its shares in the ECRS.

783. According to § 233 of the Commercial Code this share register sets out the name, address and personal identification code or registry code of the shareholder; the class and nominal value of the shares, and the serial numbers of the shares; the date of subscription and acquisition of the shares. The management board of the public limited company is obliged to ensure timely submission of correct information provided by law to the person maintaining the share register.

Securities

784. According to § 4 of the Estonian Central Register of Securities Act (ECRSA) the following information shall be entered in the register with regard to an issuer and the securities issued thereby: the name, seat and, if possible, registry code of the issuer; the type, nominal value (including currency) and amount of the securities; the names, addresses and personal identification codes or registry codes of the owners of the securities and, in the absence of a personal identification code, their date of birth, and the number of respective securities registered in the securities account opened in the name of person included in the list of owners of the securities; information concerning pledges of securities.

785. According to § 5 of the ECRSA, a securities account in the register may be opened for any Estonian or foreign person. A person may have several securities accounts. The following information shall be entered in the register with regard to a securities account: the name of the owner of the securities account; the address of the owner of the securities account; if the owner of the securities account is a natural person, his or her personal identification code or, in the absence thereof, date of birth; if the owner of the securities account is a legal person, a reference to the register in which the legal person is registered, and the registry code if the legal person is registered; the number of the bank account held by the owner of the securities account in a credit institution which performs transactions relating to the register, and the business name of the credit institution; the number of the securities account and the date on which the securities account was opened; the amount and denotation of the type of the securities in the securities account; if a security is owned by several persons, in addition to information regarding the owner of the securities account also the names, addresses, and personal identification codes or registry codes, or, in the absence of a personal identification code, the date of birth of the joint owners, and information regarding which the joint owners is entitled to dispose of the securities in joint ownership; the time of acquisition of the securities and the times at which other entries are made.

786. A copy of the approved annual report signed by the management board together with the profit distribution proposal and the auditor's report (if auditing is compulsory) shall be submitted to the registrar within six months after the end of the financial year. The areas of activity of the financial year and the changes planned in the new year shall be described in greater detail in the management report. The list of shareholders shall be annexed to the report.

787. Amendment of the name and personal identification code of a natural person in an entry of the commercial register is carried out exempt from state fees on the basis of a corresponding notice and the amendment to the population register. This provision also applies in the case of deletion of a deceased person's data from the commercial register unless the entry includes inheritable shareholder's rights or other such rights (§ 33(7^2) Commercial Code). The merger of legal persons as well as an amendment of the name of a legal person, legal form or registry code in an entry in the commercial register concerning another person is carried out on the basis of a corresponding notice and the amendment to the corresponding register (§ 33(7^3) Commercial Code). Before amending personal data, the registrar needs to check the existence in the corresponding register of the amendment on the basis of which the entry is to be made. A document issued by a foreign state shall be legalised or authenticated by a certificate replacing legalisation (apostille), unless otherwise provided for in an international agreement. If incorrect information is submitted to the commercial register, the persons who signed the petition shall be solidarily liable for any damage wrongfully caused.

788. To sum up, the commercial register must be informed of any important changes in the statutes, structure or ownership of a company and the latter must update the information that is held by the register: if the data entered in the commercial register changes (including in the case of appointment, removal or change of the right of representation of a member of the management board of a company or a liquidator, or dissolution of a company) an application for amendment of registry information must be immediately submitted to the commercial register (§ 33 (7) Commercial Code). Upon amending information in the commercial register, a registrar of the commercial register is required to make the corresponding necessary amendments in the commercial register within 15 days.

Beneficial ownership

789. As described in Section 3.2, § 8 MLTFPA provides the legal definition of the beneficial owner. § 89 (2^1) Credit Institutions Act (CrIA) stipulates that upon entry into contract or transaction, the credit institution is required to identify a client or the representative thereof. If a person or the representative thereof has been identified by the credit institution earlier, the credit institution shall decide on the need for additional identification. A credit institution has the right to verify the validity of identity documents presented for identification. For verification of identity documents, a credit institution has the right to obtain personal data from the databases of state agencies which issued the documents.

790. § 13 (1) 3) MLTFPA provides among the due diligence measures to be applied identification of the beneficial owner, including gathering information on the ownership and control structure of a legal person, trust, civil law partnership or other contractual legal arrangement on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source. The Guidelines "Additional measures for preventing money laundering in credit and financial institutions", adopted by the Management Board of the Financial Supervision Authority in June 2002 contain a special Part 3 “Identification of legal persons on creating relationship”. They prescribe that for the *identification of legal persons* the data in respect of the legal status, management, all representatives, major shareholders, objectives of activity and activity profile of the person, likewise the rights of the person to assume obligations shall be established. In the case of legal persons in private law, their passive legal capacity is verified by obtaining a certificate from the state register or the customer itself or from both[59]. Information in respect of their shareholders, partners and other persons who have control over or any other

[59] On 22 October 2008, the FSA guidelines „Additional measures for prevention of money laundering and terrorist financing in credit and financial institutions” were adopted. These guidelines contain also a special part on identification of legal persons.

essential impact on such legal persons shall be requested. All the documents submitted in respect of representation of a legal person are to be issued or confirmed by respective authorities up to 30 days prior to submitting thereof to the financial institution. Documents issued in foreign countries have to be apostilled or legalized (except countries, that Estonia has agreements of mutual recognising of documents – Latvia, Lithuania, Poland, Ukraine, Russia) and there is no 30 days restriction for that.

791. In respect of legal persons in public law and international organisations the documents serving as the basis for their activity shall be established and they shall be requested to submit the relevant documents. On identifying non-resident legal persons, credit and financial institutions are obliged, to the extent possible, to observe the same requirements which apply to resident customers, considering the peculiarities arising from the non-resident customer's country of residence and legal status.

792. The Estonian authorities explained that all the investigative and prosecutorial authorities as well as the regulatory, supervisory, and other competent authorities in Estonia have on-line access to the information from the relevant registers to identify natural and legal persons. This includes the commercial register (companies register) and non-profit associations and foundations register, habitants register, etc.

793. § 28 Commercial Code provides for the access to the commercial register:

(1) Entries in the commercial register are public. Everyone has the right to examine the card register and the business files, and to obtain copies of registry cards and of documents in the business files.

(2) The authenticity of copies of registry cards and copies of other documents preserved in a registration department shall be certified by an assistant judge or a registry secretary authorised therefor.

(3) A registry file may be examined by a competent state agency including by the court in the course of a proceeding, a bailiff or a person with a legitimate interest in the matter.

(4) At the request of a person, the registrar shall issue a certificate that an entry has not been amended or that a particular entry is not in the register.

794. The Commercial Code envisages that Estonian companies may have only registered shares. During the on-site visit it was clarified that under the previous Commercial Code there was a possibility for public limited companies to issue bearer shares but this possibility was abandoned and since 2002 Estonian companies may have only registered shares. § 88 (5) of the Estonian Central Register of Securities Act (ECRSA; which came into force on 1 January 2001) provides that a public limited company which has issued bearer shares shall exchange them for registered shares not later than by 31 December 2001. The registrar of the commercial register has the right to require a public limited company whose shares are not registered with the Estonian Central Register of Securities to submit an extract containing valid information from the share register. In order to certify the authenticity of the extract, it shall be signed by at least one member of the management board or, if the members of the management board are only authorised to represent the public limited company jointly, by the members of the management board authorised to represent it jointly. (§88 (6) ECRSA). § 88 (7) of the ECRSA provides that a public limited company which has failed to perform an obligation specified in § 88 (5), i.e. change bearer shares to registered shares, within the specified term shall be deemed to have undergone compulsory dissolution.

Additional elements

795. As stated above, the commercial register and other registers are maintained electronically. Entries in the commercial register are public. Everyone has the right to examine the card register and the business files, and to obtain copies of registry cards and of documents in the business files.

5.1.2 Recommendations and comments

796. 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. Legal persons are not permitted to issue bearer shares. However, 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.

797. On the positive side it has to be noted that there are safeguards in Estonian legislation that the information kept in registers is up to date. Measures are in place to ensure that companies submit their annual accounts, and lack of compliance with this may be sanctioned. There are even penal sanctions for submission of incorrect information to the registrars. However, while this seems to provide efficient measures on the side of the applicants, there are no similar requirements for registrars: though the registrar may demand supplementary documents from the undertaking if these are necessary to determine the facts which are the basis for an entry (§ 32 Commercial Code), but there is no obligation for verification of documents or any kind of ongoing 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.

798. There are rules for the obligated entities to establish the beneficial ownership of their clients. Nevertheless, 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 persons 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.

799. In practice, one can conclude that the Estonian registration system provides a useful tool to gather rather comprehensive and accurate information because in order to make use of rights which are registered it is always necessary that they are kept in the register. Thus, economic interests guarantee a high level of accuracy of the information kept by registers.

5.1.3 Compliance with Recommendation 33

	Rating	Summary of factors underlying rating
R.33	**LC**	• There is limited control over the implementation of obligations of legal persons to submit updated information on ownership and control to the commercial register. • Requirements that limited liability companies maintain share registers and shareholder registers are not supervised. • Though in practice the Estonian registration system provides a useful tool to gather rather comprehensive and accurate

		information, the legal framework does not entirely ensure adequate, accurate and timely information on the beneficial ownership and control of legal persons.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and analysis

800. The Estonian legal system does not allow for the creation of trusts. Estonia has not signed the Convention on the Law applicable to Trusts and on their Recognition (1 July 1995, The Hague)[60]. However, there are no obstacles for Estonian citizens to be trustees of foreign trusts and Estonian legal practitioners may establish foreign trusts for their Estonian clients.

801. Domestic trusts cannot be established in Estonia as the notion of "trust" is unknown in its domestic legislation. There was some uncertainty whether legal arrangements similar to those of a trust may arise in Estonia in connection of a civil law partnership or another similar contractual legal entity regulated by the Law of Obligations Act. However, in course of the pre-meeting it could be clarified that these organisational forms have nothing in common with trusts or legal arrangements as described under FATF Recommendation 34.

802. § 7 MLTFPA provides a definition of a trust and company service provider in order to allow trusts, which exist under foreign legislations, to run business in Estonia (a provision which was introduced to the MLTFPA due to requirements of the 3rd EU AML Directive). Thus, foreign trusts may operate in Estonia. All entities conducting business, which would include trustee activities, are obliged to maintain accounting records. If a foreign trust comes to an Estonian financial institution as a customer, it is considered in the same way as any other legal person which is a customer of the financial institution and the general CDD requirements as given by the MLTFPA applies.

5.2.2 Recommendations and comments

803. Under the present circumstances, Recommendation 34 is not applicable as trusts cannot be established in Estonia.

5.2.3 Compliance with Recommendation 34

	Rating	Summary of factors underlying rating
R.34	**NA**	

[60] Status table can be found at: http://www.hcch.net/index_en.php?act=conventions.status&cid=59

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and analysis

General

804. The non-profit organisations in Estonia are either non-profit associations (NPA) or foundations. They are considered as legal persons. Their passive legal capacity commences as of entry in the Non-profit Associations and Foundations Register, which is maintained by the registration departments of the County courts and terminates as of their deletion from the register. On 1 September 2007, the number of registered non-profit organisations in Estonia was 25 104 (25 853 associations and 749 foundations). Over a half of the NPAs registered in the Register of Non-profit Associations and Foundations are apartment associations, garage associations and gardening associations. This number includes about 12 000 housing associations. Of the remaining 11 000 organisations about 1 200 are actual public benefit organisations. It is estimated that about 28 000 people (4-5% of the Estonian workforce) are employed in the non-profit sector. Most organisations are registered in Tallinn. Estonian associations and foundations have activities as service providers, advocacy groups, think tanks, institutes, clubs, networks, umbrella organisations etc.

805. Non-profit associations include apartment-, housing-, garage- and garden-associations as well as political parties, trade unions, churches, congregations and monasteries. A foundation is a legal person in private law which has no members and which is established to administer and use assets to achieve the objectives specified in its articles of association. The income of non-profit associations and foundations may be used only to achieve the objectives specified in the articles of association. They are not allowed to distribute profits among their members.

806. The legal framework for Non-profit Associations (NPAs) includes the Non-profit Associations Act (as of 1 October 1996, Non-profit Associations may only be founded pursuant to the procedures provided for in this act) and specific acts depending on the category of the association (the Apartment Associations Act, the Trade Unions Act, the Political Parties Act, the Churches and Congregations Act, the Land Improvement Act in case of a land improvement association, the Creative Persons and Artistic Associations Act, etc.).

807. As of 1 October 1996, foundations may only be founded pursuant to the procedure provided for in the Foundations Act. It must be noted that the provisions in both acts which regulate the areas relevant for the purpose of the MONEYVAL evaluation are quite similar and at some points identical.

808. Estonian authorities stated that they exercised a detailed overview of the activities and size of NPOs.

Reviews of the domestic non-profit sector

809. The Security Police Board together with the Ministry of Justice has reviewed the activities, size and other features of the domestic NPO-sector in 2007. As a result of the study it was concluded that the Estonian NPOs are generally not at risk of being misused for terrorist financing. According to Europol's "Terrorist Activity in the European Union: Situation and Trends Report (2006)"[61], Estonia, Finland, Hungary, Latvia, Lithuania, Slovenia and Slovakia are the least threatened EU countries by terrorism and activities supporting terrorism. However, it has to be noted that this study did not include a review of the adequacy of laws and regulations related to the NPO sector.

[61] http://www.statewatch.org/news/2006/may/europol-terr-rep-2004-2005.pdf.

810. Estonian authorities confirmed that they do not have any information and there are no indications which would refer to the fact that funds are collected for or forwarded to terrorists or movements associated with terrorists through NPOs in Estonia. There is also no information about Estonian NPOs providing any logistic support to terrorists or recruiting persons for terrorist purposes. Although, according to Estonian authorities such activities cannot be ruled out in the future, they are considered unlikely.

811. As regards alleged international communication of NPOs or establishment of NPOs by or with the participation of persons supporting terrorism, authorities stated that so far it has not been identified that any NPOs would communicate with foreign NPOs suspected of terrorist financing or that any Estonian NPOs would be used by such foreign NPOs. Also, it has not been found that terrorists or persons supporting terrorism would have attempted to establish any NPOs which are run or controlled by them fictitiously. There are no NPOs in Estonia which have a global reach.

812. Estonian authorities consider the state supervision over NPAs as effective and that supervision issues are not a risk. Their conclusion is that the size, activities and characteristics of the NPA are not attractive means for facilitating terrorist financing.

Protecting the NPO sector from terrorist financing through outreach and effective oversight

813. The evaluation team was not informed about any awareness-raising measures in the NPO sector about the risks of terrorist abuse and the available measures to protect against such abuse.

814. The Memorandum of association of a Non-profit Association and the Articles of association of a Foundation must set out the name, location, address and objectives of the NPO, the names and residences or locations, and the personal identification codes or registry codes of the founders, the obligations of the founders with regard to the non-profit organisation; the names, personal identification codes and residences of the members of the management board (§ 6 Non-profit Associations Act, § 8 Foundations Act).

815. According to § 10 Non-profit Associations Act (NPAA), the information entered in the register includes the names and personal identification codes of the members of the management board and the specifications for the right of representation of the management board; the name, the location and address of the non-profit association, the date of approval of the articles of association the term of the association if the non-profit association has a specified term. Since 1 January 2007, residences of the members of the management board are not anymore entered into the register, but the memorandum of association shall set out the residence of the members of the management board. The members of the management board of a non-profit association and liquidators who do not have a place of residence registered in the population register must submit their address to the registrar and immediately communicate the change of the address (§ 78^1(6) NPAA). In the case of a change in the data in the Non-profit Associations and Foundations Register, among other things, upon appointment and removal of the members of the management board and of the liquidators, change of the right of representation and dissolution of an association, an application for amendment of the data entered in the Non-profit Associations and Foundations Register must be submitted (§ 10 NPAA - "*Entry of information in register and change thereof*"); in order to enter a new member of the management board in the register, the notarised specimen signature of the new member shall be appended to the petition. According to § 33 (7) Commercial Code (in conjunction with § 76 NPAA which makes a number of provisions from the Commercial Code applicable for non-profit associations), an application for amendment of registry information shall be *immediately* submitted to the commercial register if the data entered in the commercial register change. The registrar can impose a fine on the legal person or any other person required to submit the information to the register (board member, liquidator) if it fails to submit information (§ 71 Commercial Code).

816. § 39 Foundations Act provides for access to information on activities of a foundation: a beneficiary or "*other person with a legitimate interest"* (including competent authorities) may

demand information from a foundation concerning the fulfilment of the objectives of the foundation. The beneficiary or other person with a legitimate interest may examine the annual accounts of the foundation and the activity report of the management board, the auditor's report, accounting documents, the foundation resolution and the articles of association. If a foundation does not comply with the demand an entitled person may demand exercise of the entitled person's rights by a court proceeding (§ 39 (3) Foundations Act).

817. § 81 Non-profit Associations Act imposes a notification obligation to the state authorities and relevant institutions: the courts, state and local government agencies, and notaries are required to notify the registrar of any incorrect information in the register or of any information not submitted to the register of which they become aware due to their office.

818. The register may collect information on its own initiative: According to § 82 NPAA, if a registrar has information concerning the incorrectness of an entry or that an entry is missing, the registrar may make the appropriate inquiries. Upon ascertaining that an entry is incorrect or missing, the registrar notifies the Non-profit Association on the basis of whose petition the entry should have been made. If no objection to making, correcting or deleting the entry is made within two weeks after notification, the registrar shall make, correct or delete the entry. In cases of incorrect or missing entry the registrar may impose a fine on obligated persons. If the making of an "ex-officio entry" would result in the deletion of a Non-profit Association from the register, the registrar may initiate the compulsory dissolution of this association at court.

819. In addition, pursuant to § 12 (2) NPAA, the registrar has the right to demand at any time information from the management board of a Non-profit Association on the number of its members (there should be at least two members). If the management board does not submit a petition for dissolution of the Non-profit Association within three months when the number of members falls below two or any other number prescribed by law or the articles of association, the registrar shall commence the compulsory dissolution of the Non-profit Association.

820. Compulsory dissolution of NPOs is regulated in § 40 NPAA and § 46 Foundations Act: a Non-profit Organisation is dissolved by a court ruling at the request of the Minister of Internal Affairs or another interested person (amongst other reasons provided by law) if:

a) its objectives or activities are contrary to law, the constitutional order or good morals;
b) the activities of the non-profit organisation do not comply with the objectives in the articles of association;
c) economic activity becomes the main activity of the non-profit organisation;
d) the management board does not submit a petition for dissolution provided by law.

A court may set a deadline for elimination of deficiencies. A court may also decide the compulsory dissolution on its own initiative unless otherwise provided by law.

821. As already mentioned (see above para 773), every member of the management board may be punished separately by a fine in the amount of up to two hundred minimum daily rates 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 registration department of the court and to the notary may be punished pursuant to criminal procedure by a fine or imprisonment.

822. As stated earlier, all non-profit organisations in Estonia are entered in the Non-profit Associations and Foundations Register in the registration departments of the County courts. The information in the register is public. § 77 provides that *everyone* (including competent authorities) has access to the register, including the right to examine the card register and the public files of NPOs and to obtain copies of registry cards and of documents in the public files of NPOs.

823. NPOs are required to maintain accounting like all persons in private law and their activities are subject to supervision by auditors (§§ 34, 35, 36 NPAA and §§ 33, 34, 35 Foundations Act). According to § 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. NPAs are obliged to submit a signed original copy of their annual report to the regional authority of the Tax and Customs Board within six months after the end of the financial year (§ 55 (1) of the Income Tax Act). This is done only for tax purposes. In case of foundations the management board shall submit approved annual reports to the register within the same time frame.

824. Estonian authorities clarified that an amendment to the registration system of non-profit associations will render the economic activities of the associations more transparent. The annual reports of all non-profit associations will have to be presented to the court registrar within six months after the end of the financial year. The annual reports will be submitted electronically and guarantee a better supervision over the economic activities of non profit associations. The amendment to the Non-profit Associations Act has been submitted to Parliament on 20 February 2008. It was expected the draft to be adopted as law before 19 June 2008 and the new regulation to be applicable to the economic year accounts of the year 2009 and the following[62].

825. Estonian authorities explained that NPOs in Estonia do not have access to any significant funds. Charity is aimed primarily at social assistance of those in need and very little attention is paid to fundraising. Many NPOs are funded by the state or local authority. Cultural associations of minorities are supported via the Integration Foundation. Tatar, Azerbaijani, Kazakh, Uzbek and Bashkir minorities account for most of the Muslim community in Estonia and their organisations and associations are supported nationally and are involved in various support projects of the Integration Foundation. There are no branches of any global Islamic charity organisations in Estonia. According to Estonian authorities, NPOs conduct few cash transactions and the amounts are very small. Apparently there are no NPOs in Estonia which would have a global grasp.

Targeting and attacking terrorist abuse of NPOs through effective information gathering, investigation

826. Estonian authorities consider their possibilities to effectively investigate and gather information on NPOs as sufficient due to the fact that the information in the Non-profit Associations and Foundations Register is publicly available.

827. The Tax and Customs Board and the FIU have concluded a cooperation agreement, the purpose of which is to improve inter-agency cooperation in exchange of operative information for the purpose of prevention and detection of money laundering. The FIU submits information inquiries to the Tax and Customs Board in the framework of the inspection file and the latter provides the former with its own assessment and background information. Information is exchanged by e-mail in encrypted form. The Tax and Customs Board has held several meetings where cooperation issues have been discussed. Joint training of the officials of the Information Department of the Tax and Customs Board and the FIU in the area of exchange of information has been planned for the purpose of exchanging experiences.

828. The police have online access to the Non-profit Associations and Foundations Register, the Citizens Register, etc. – all the registers required for identification of legal persons involved in an NPO. All data in the register is available for the police (information maintained electronically is available online, incl. the financial information collected by the register).

[62] The draft was adopted by Estonian Parliament on 4 July 2008 and entered into force on 10 July 2008.

829. There are no particular mechanisms in place for a prompt sharing of information among all relevant competent authorities in order to take preventive or investigative action when there is suspicion or reasonable ground to suspect that a particular NPO is being exploited for terrorist financing purposes or is a front organisation for terrorist fundraising. The normal co-operation mechanisms among competent authorities are considered adequate to secure fast concerted reactions of the authorities if the need may be.

Responding to international requests for information about an NPO of concern:

830. No special points of contact or distinguished procedures to respond to international requests for information regarding particular NPOs that are suspected of terrorist financing or other forms of terrorist support have been appointed or developed.

5.3.2 Recommendations and comments

831. The Security Police Board together with the Ministry of Justice have reviewed the activities, size and other features of the domestic NPO-sector in 2007. No cases of terrorist financing or any other offences connected with terrorism are known to have been committed. Estonia is said to belong to a group of countries which are the least threatened in Europe, but some radical groups seem to be trying to establish contacts in Estonia and neighbouring countries. However, there was no review of the adequacy of relevant laws and regulations to prevent the abuse of NPOs for financing of terrorism which should be done as soon as possible.

832. Estonia has mechanisms in place to obtain information and to monitor the financial activity of Non-profit Associations and Foundations. Authorities perceive the threat of terrorist financing in Estonia as very limited. In May 2007, a formal review was conducted jointly by the Ministry of Justice and the Security Police Board to identify the features and types of non-profit organisations (NPOs) and whether they are at risk of being misused for terrorist financing. There were no indications that funds are collected for or forwarded to terrorists or movements associated with terrorists through NPOs in Estonia. Therefore no other legislative, administrative or organisational measures have been undertaken which would contribute to better prevention in respect of financing terrorism through NPOs. There are no programmes in place to raise awareness within the NPO sector of the risks of terrorist financing abuse or to strengthen its resistance to terrorist financing.

833. There is no adequate system of supervision or monitoring concerning NPOs as envisaged by the Interpretative Note to SR VIII. The registers are electronically based and public, but the information they contain is not reliable: it is not checked and the registrars put in only the information sent by the respective persons. There is no clear supervisory power over the activity of the NPOs. With the exception of the audits conducted by tax authorities, there appears to be no active compliance monitoring by the authorities to ensure that the obligations of NPOs to submit information, keep records, etc are in fact complied with.

834. There are not enough measures in place to ensure that terrorist organisations cannot pose as legitimate non-profit organisations or that funds or other assets collected by or transferred through such organisations are not diverted to support the activities of terrorists or terrorist organisations, as required by Criteria VIII.2 and VIII.3.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating

SR.VIII	**PC**	• No review of the adequacy of relevant laws and regulations to prevent the abuse of NPOs for financing of terrorism has been undertaken. • Authorities do not conduct outreach or provide guidance on terrorist financing to the NPO sector. • There is no supervision or monitoring of the NPO sector as envisaged by the Interpretative Note to SR VIII. • There are no particular mechanisms in place for a prompt sharing of information among all relevant competent authorities when there is suspicion that a particular NPO is being exploited for terrorist financing purposes. • No special points of contact or distinguished procedures to respond to international requests for information regarding particular NPOs.

6 NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and co-ordination (R. 31)

6.1.1 Description and analysis

835. Recommendation 31 (and criterion 13.1) is concerned with co-operation and coordination between policy makers, the FIU, law enforcement, supervisors and other competent authorities.

836. § 37 (1) 6) MLTFPA states that one of the function of the Estonian FIU is cooperation with obligated persons, investigative bodies and police institutions in the prevention of money laundering and terrorist financing.

837. According to Order No. 285 of the Government of the Republic of 11 May 2006, the Government Committee for Coordination of Issues concerning prevention of Money Laundering and Terrorist Financing (hereinafter: Government Committee) 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 Government Committee. The functions of the Government Committee 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 in force and coordinating drafting a new legislation;
- making proposals to the Government of Estonia for improving the measures for prevention of money laundering and terrorist financing and for amendments of the respective legislation;
- coordinating international cooperation on prevention of money laundering and terrorist financing, including coordinating the making of the respective policy of the EU at national level.

838. The "Advisory Committee on Prevention of Money Laundering and Terrorist Financing" (hereinafter: Advisory Committee) was established in 2006 in order to improve the awareness of the private sector on money laundering issues, to take part in the development of the system for the prevention of money laundering and also in the drafting of the legal instruments related to money laundering and terrorist financing. The Government Committee nominates members of the Advisory Committee among representatives of the obligated persons of the MLTFPA. According to its rules of procedure, the Advisory Committee meetings take place as appropriate but at least once every 2 months. Every member of the Advisory Committee can propose items for the agenda. The aim of the Advisory Committee is to involve the private sector in elaborating regulations which concern them and to exchange information and to express opinions to the Government Committee. The Advisory Committee gives opinions and makes propositions to the Government Committee concerning various issues which include amongst others:

- Coordination of implementation of legal acts concerning money laundering and terrorist financing prevention and the authority and capacity of respective institutions;
- Implementation of the MLTFPA in force as well as new regulations or drafts;
- Enhancement of measures of money laundering and terrorist financing prevention and amendments to respective legal acts.

839. The Estonian authorities informed the evaluation team that this Advisory Committee has developed a communication plan which concerns communication through various media for the improvement of money laundering awareness (of the general population as well as entrepreneurs). Booklets introducing new requirements of the MLTFPA and the importance of prevention of money laundering have been produced where every member association or organisation has the

possibility to insert more specific leaflets concerning rules applicable to them (for example, the credit institutions and notaries share the general booklet, but have different leaflets inside explaining to customers the new requirements).

840. The FIU actively participates in the working group for the prevention of money laundering which is a cooperative body of Estonian commercial banks, the FSA, the Bank of Estonia, the FIU and the Estonian Banking Association. Tasks of this working group include:

- monitoring of trends in the prevention of national and international money laundering,
- promoting "best practices" to interested parties,
- recommendations to increase the effectiveness of the system of money laundering prevention,
- assistance in the detection of criminal offences,
- exchange of ideas, in-service training and cooperation.

841. The evaluators were advised that, in the field of supervision, the Estonian FIU is co-operating closely with the Financial Supervision Authority through regular meetings. In order to improve it's co-operation in the field of supervision, the Estonian FIU is planning to sign Memoranda of Understanding with entities which were recently assigned as supervisory bodies in the AML/CFT area, such as the Estonian Bar Association and the Chamber of Notaries. Furthermore, the Estonian authorities referred to an agreement of mutual cooperation for combating financial crime between the FSA, the Police Board, including FIU and the Prosecutors Office which was signed on 20 January 2003 and which provides grounds for cooperation on supervisory and mutual training issues. However, the evaluators did not see an English version of this agreement and it is unclear to what extent it deals with AML/CFT issues (and not with financial crimes in general). Furthermore, there are now new supervisory authorities (the Estonian Bar Association; the Chamber of Notaries) where the cooperation and coordination between supervisory authorities does not yet seem to be formally structured.

842. While the FIU analyses suspicious transaction reports and, in case of necessity, forwards them to investigative bodies, it closely cooperates on a day-to-day basis with the agencies involved in criminal proceedings: The Central Criminal Police and its prefectures, the Prosecutor's Office, the Security Police Board, the Tax and Customs Board and the courts.

843. The Estonian FIU has signed co-operation agreements (Memoranda of Understanding) with the following authorities:

- Customs and Tax Board. This MoU regulates the conditions for information exchange between authorities in order to prevent and discover possible Money Laundering. Both authorities have appointed contact persons who co-operate on a daily basis.
- Security Police Board for the exchange of information regarding Terrorist Financing. The director general of the Security Police Board has appointed a contact person who co-operates with the Estonian FIU in accordance with MLTFPA article 45. The contact person of the Security Police Board is subject to the provisions of clauses 37 (1) 1), 6) and 7), § 41, § 43 (1) to (5) and § 44 (2). The contact person of the Security Police Board has the right to exercise supervision specified in § 48 jointly with the Financial Intelligence Unit.

6.1.2 Recommendations and Comments

844. The new MLTFPA has assigned new supervisory bodies for AML/CFT matters, such as the Chamber of Notaries and the Bar Association. So far there seems to be no much formal co-ordination (in terms of formal agreements, sharing of information etc.) between the supervisory bodies. To improve the national cooperation in the AML/CFT area, supervisory authorities and, in particular, the FSA and the FIU should devise a formal agreement through a Memorandum of Understanding or other means for cooperation and coordination on supervisory matters.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**LC**	• There seems to be no much formal co-ordination (in terms of formal agreements, sharing of information etc.) between the supervisory bodies.

6.2 The Conventions and United Nations Special Resolutions (R. 35 and SR.I)

6.2.1 Description and analysis

Recommendation 35

845. Estonia has ratified all relevant conventions:
- 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention)" was ratified and entered into force for Estonia on 10 October 2000.
- The Palermo Convention (UN Convention Against Transnational Organised Crime) was ratified and entered into force for Estonia on 29 September 2003.
- The Terrorist Financing Convention was ratified and entered into force for Estonia on 21 June 2002.
- The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Strasbourg, 1990) was ratified and entered into force for Estonia on 1 September 2000.

The Conventions were transposed into national law by various provisions.

846. Estonia has signed, ratified and implemented the *Vienna Convention* and the *Palermo Convention* and all physical elements of the money laundering offence, as required by these conventions, appear to be covered. Self-laundering is a criminal offence in Estonia. However, as to the effective implementation of the Vienna and Palermo Convention it must be repeated that the evaluation team was left with some doubts as to whether a conviction or at least indictment for the predicate offence is a prerequisite for a money laundering conviction.

847. As regards the *Vienna Convention*, trafficking in drugs and other offences related to drugs and psychotropic substances is criminalised in Chapter 12, Division 1 „Offences Relating to Narcotics" of the Penal Code. Associated money laundering is also an offence, as the Estonia money laundering offence follows an "all crimes approach". The Penal Code provides for extended confiscation of the proceeds of trafficking in drugs. Some concerns regarding the protection of the rights of bona fide third parties were noted under Recommendation 3. Legislation in Estonia also provides for mutual legal assistance and extradition. A detailed analysis on the legal system governing mutual legal assistance and extradition is provided below (see Recommendations 36 – 39).

848. Concerning the implementation of the *Palermo Convention*, Estonia has criminalised laundering of proceeds of crime. Forming or leading of or membership or recruiting members to a criminal organisation is punishable under §§ 256 and 255 Penal Code. The Penal Code provides for the extended confiscation of the proceeds of this crime.

849. The terrorist financing offence (§ 237 PC) criminalises the majority of offences that are listed in the Annex to the *Terrorist Financing Convention*. Yet, some of the elements required under the Terrorist Financing Convention are not covered: financing of an individual terrorist is not

criminalised; the current law does 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. Furthermore, not all conducts as referred to in Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions are covered (see above para 196).

850. The Estonian money laundering offence follows an all crimes-approach, i.e. all crimes may be predicate offences for money laundering, and thus also terrorist financing as far as it is criminalised can be a predicate offence for money laundering.

Additional elements

851. The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime was ratified and entered into force for Estonia on 1 September 2000. Estonia has not yet signed the CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198).

Special Recommendation I

852. The Terrorist Financing Convention was ratified and entered into force for Estonia on 21 June 2002.

853. Under Section 2.4 of this report, the main issues concerning the implementation of the UNSC Resolutions were discussed. As stated there, the legal framework and the effectiveness of the enforcement side should be further improved in order to be in line with the international standards. The areas of concern are the lack of a national mechanism to freeze the funds of EU internals and the lack of procedure to consider requests for freezing from other countries; the 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. In addition, Estonia does not have an established national procedure for the purpose of considering delisting requests.

6.2.2 Recommendations and comments

854. The evaluators' team welcomed that Estonia ratified all the relevant instruments and that measures are taken to implement their requirements. Some issues still need to be addressed (their detailed assessment was made under Section 2 of the present report) in order for Estonia to be fully in line with requirements of international Conventions; thus, the same comments as are made above in relation to the implementation of the respective Conventions and the UN Security Council Resolutions apply here.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**LC**	*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 "collecting of funds".

		• No specific criminalisation of the 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 are not covered.
SR.I	**PC**	• 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.

6.3 Mutual legal assistance (R.32, 36-38, SR.V)

6.3.1 Description and analysis

Recommendation 36

855. Estonia provides mutual legal assistance in criminal matters on the basis of international conventions: the *European Convention on Mutual Assistance in Criminal Matters* (CETS 30) and *Additional Protocol* (CETS 99) thereto *(*both in force for Estonia since 27 July 1997) and the *Second Additional Protocol* (CETS 182) which is in force for Estonia since 1 January 2005. This legal framework is supplemented by the *2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union* and the *Additional Protocol* thereto of 2001. The provisions of the latter Convention are especially aimed at making the investigation of organised crime more efficient. The Protocol to the Convention includes provisions on the granting of legal assistance involving bank account information. Estonia is also a party to several bilateral and multilateral agreements, which regulate relationships with other States in the area of cooperation in criminal matters. Such agreements are in force with Finland, USA, Ukraine, the Russian Federation, Lithuania, Latvia and Poland. In addition, Estonia may provide MLA in the absence of a treaty.

856. Mutual legal assistance in criminal matters is regulated in Chapter 19, Division 3 of the Code of Criminal Procedure.

857. According to § 433 (1) CCP, international co-operation in criminal procedure comprises extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings commenced, co-operation with the International Criminal Court and extradition to member states of the European Union. International co-operation in criminal matters is effected pursuant to the provisions of the CCP unless otherwise prescribed by the international agreements of the Republic of Estonia or the generally recognised principles of international law. The Estonian Constitution provides that "*if laws or other legislation of Estonia are in conflict with international treaties ratified by the Parliament, the provisions of the international treaty shall apply*."

858. The Estonian authorities clarified that the explanatory memoranda and commentaries to international conventions are part of the preparatory works to the laws on the ratification of international instruments and therefore can be used as a legal source when interpreting the legislation.

859. § 463(1) CCP regulates the coercive and non-coercive measures that Estonia can undertake to respond to a request for mutual legal assistance (MLA request). Assistance in criminal matters is provided at the stage of preliminary investigations and at the stage of trial proceedings. Measures specific to MLA are regulated under §§ 460 to 487 CCP and MLA may be provided in the following forms:
- *Tracing and interception of (tele-)communications* (including interception; recording and transcription of telecommunications; tracing of telecommunications; interception and recording of other forms of communication; interception of mail; observation);
- *Examination, body search and expert evaluation* (including superficial body search; invasive body search; psychiatric medical examination; control of identity; measures for judicial identification; technical or scientific examinations or expert evaluations);
- *Obtaining of documents* (including order to produce documents; other possibilities of obtaining information concerning taxes or bank accounts; access to public documents in judicial files; communication of individual police records; spontaneous exchange of information), thus complying with criterion *36.1.a* and *c* of the Methodology;
- *Assets - seizure, confiscation and restitution* (including seizure of assets; freezing of bank accounts; restitution; interim measures in view of confiscation; confiscation), thus complying with criterion *36.1.f* of the Methodology
- *Visit and search of places* (including visit to and search of homes; visit and search on the site of an offence)
- *Summoning and hearing of witnesses, victims and suspects* (including summoning witnesses; hearing of witnesses by standard procedure, by video conference or by telephone; hearing of children; hearing of persons collaborating with the inquiry; hearing of victims/plaintiffs; hearing of experts; summoning suspects/persons accused; hearing of suspects/persons accused by standard procedure and by video conference; confrontation), thus complying with criterion *36.1.b* of the Methodology
- *Cross-border operations* (including controlled deliveries and joint investigation teams (§ 471 CCP).

860. With regard to criterion 36.1.f, it must be pointed out that § 470 CCP provides for the possibility of handing over property to foreign states by a ruling of the judge of the county court of the location of the property. For securing the handling, all available provisional measures under Estonian CCP may be used. In cases of urgency, property may be seized or a search may be conducted at the request of a foreign state before receipt of the request to hand over property (§ 470 (4) CCP). If a requesting state requests execution of confiscation to be taken over, the convicted offender must have a counsel. The counsel in the taking over of execution must be an advocate (§ 480).

861. § 473 CCP allows Estonian authorities to provide spontaneous information: a competent judicial authority may forward to a foreign state information obtained by a procedural act performed without prior request for MLA when such information may be the reason for initiating a criminal proceeding in the foreign state or may assist in ascertaining the facts relating to a criminal offence subject to a criminal proceeding already initiated.

862. Estonian authorities consider that they provide mutual legal assistance timely and efficiently and in a constructive manner. There is no other experience on international co-operation in criminal matters with Estonia, in FATF or MONEYVAL countries, which would show the contrary. A MONEYVAL country (Ukraine) assesses its practice of cooperation with the FIU as a very positive one: "*the responses received from FIU of Estonia were always substantial, informative and rather fast in comparison to other FIUs*".

863. As an example of the constructive approach towards international co-operation in criminal matters, the Code of Criminal Procedure provides in § 463 (1) that requests for assistance are complied with pursuant to the CCP. Nevertheless, at the request of a foreign state, a request may

be complied with pursuant to procedural provisions different from the provisions of the CCP unless this is contrary to the principles of Estonian law.

864. Restrictions for mutual legal assistance are stated in § 436 (1) CCP and include: danger for the security, public order or other essential interests of the Republic of Estonia; conflict with the general principles of Estonian law; 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.

865. Yet, as discussed in Section 2.1 with regard to criterion 1.5 (see para 168 ff), the level of proof of the extra-territorial predicate offence which is required in order to prosecute the money laundering offence in Estonia is still unclear. From the seven convictions for money laundering passed in Estonia no one has been based on a predicate offence which took place abroad. Therefore it is up to the court practice to confirm the understanding of the authorities met that a conviction for an extra-territorial predicate offence is not a necessary element in a prosecution for money laundering.

866. The central authority for sending and receiving MLA requests is the Ministry of Justice (the International Judicial Cooperation Division of the Courts Department). After checking and establishing that the MLA request sent to it meets formal requirements (§460 CCP), the Ministry of Justice sends it to the State Prosecutor's Office. The latter verifies whether compliance with the request is admissible and factually possible and in turn forwards the request to the competent judicial authority for execution. In cases of application of the Estonian Penal Code to criminal offences committed outside the territory of Estonia, the State Prosecutor's Office shall be immediately informed (§ 435(3) CCP). The materials received as a result of compliance with a request from a foreign state shall be sent to the Ministry of Justice through the State Prosecutor's Office and the Ministry of Justice shall forward the materials to the requesting state (§ 463(2) CCP). According to §435(2) CCP, the following entities are also competent to engage in international cooperation: courts, the Police Board, Central Criminal Police, Police Prefectures, the Tax and Customs Boards, Border Guard Administration, Competition Board and the Headquarters of the Defence Forces. In cases of urgency, a request may be submitted also through Interpol and communicated concurrently through the judicial authorities.

867. Estonia does not refuse assistance solely on the ground that the act can be regarded as a fiscal offence. The Code of Criminal Procedure does not recognise this as a ground for refusal. This is also expressly prohibited in the Additional Protocol to the European Convention on Mutual Assistance in Criminal (CETS 99) to which Estonia is a party.

868. § 433 (4) CCP provides that if adherence to the requirement of confidentiality is requested in the course of international co-operation in criminal matters, such requirement shall be complied with to the extent necessary for the purposes of co-operation. If compliance with the confidentiality requirement is refused, the requesting state shall be immediately notified of such a refusal.

869. Bank secrecy cannot be invoked as a ground for declining to provide MLA. There is no such restriction in the CCP and pursuant to § 88(5) of the Credit Institution Act, "*in response to a written inquiry, a credit institution shall disclose information subject to banking secrecy to courts, pre-trial investigation authority and the Prosecutor's Office if a criminal proceeding is commenced, and on the basis of a request for legal assistance received from a foreign state based on an international agreement*".

870. There is no legal impediment for using the powers of law enforcement agencies required under Recommendation 28 in the mutual legal assistance framework. Special investigative techniques are available only for investigating offences with a maximum punishment of at least three years'

imprisonment. Therefore special investigative techniques may be used when completing MLA requests concerning money laundering and terrorist financing offences.

871. As regards the measures for avoiding the conflict of jurisdictions, Division 4 of Chapter 19 CCP regulates the possibilities for transfer of criminal proceedings. Estonia is a party to the European Convention on transfer of criminal proceedings since 27 July 1997.

872. § 474 CCP envisages that the transfer of a criminal proceeding initiated with regard to a person suspected or accused of a criminal offence to a foreign state may be requested if:

a) 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;
b) criminal proceedings concerning the same or any other criminal offence have been initiated with regard to the person in the requested state;
c) the evidence or the most relevant pieces of evidence are located in the foreign state;
d) 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.

873. The procedure is as follows: a request for transfer shall be sent to the Public Prosecutor's Office together with the criminal file or an authenticated copy thereof, and other relevant materials. The Public Prosecutor's Office shall verify whether the transfer of a criminal proceeding is justified and send the materials to the Ministry of Justice who shall forward them to the foreign state. After submission of a request for the transfer of a criminal proceeding, charges shall not be brought against the person for the criminal offence regarding which transfer of the proceedings was requested, and a court judgment previously made with regard to the person for the same criminal offence shall not be executed. The right to bring charges and execute a court judgment will be regained if:

a) the request for transfer is not satisfied;
b) the request for transfer is not accepted;
c) the requested state decides not to commence or to terminate the proceedings;
d) the request is withdrawn before the requested state has given notice of its decision to satisfy the request (§ 474 (5) CCP).

874. Estonia is also able to take over criminal proceedings (§ 475 CCP): 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. Acceptance of a request to take over a criminal proceeding may be refused in whole or in part if:

a) the suspect or accused is not an Estonian citizen or does not live permanently in Estonia;
b) 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;
c) 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 elements

875. As already explained, the central authority for sending and receiving MLA requests is the Ministry of Justice. Pursuant to Article 15, paragraph 6, of the *European Convention on Mutual Assistance in Criminal Matters* (CETS 30), the Republic of Estonia declared that a copy of the letters rogatory addressed directly to the judicial authorities shall be transmitted to the Ministry of Justice of Estonia. This declaration was confirmed when ratifying the Second Additional Protocol, which encourages in principle the direct contacts among judicial authorities. Article 6 of the *2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union* foresees direct contacts between competent authorities.

Recommendation 37

876. According to the Estonian authorities, mutual legal assistance does not depend on the fulfilment of a dual criminality requirement and the CCP contains no rules that would require dual criminality. However in a declaration pursuant to Article 23, paragraph 1 and Article 2 of the *European Convention on Mutual Assistance in Criminal Matters* (CETS 30), Estonia has *"reserved the right to refuse her assistance in case the request concerns an act which is not considered an offence under Estonian laws"*

877. At the same time, there are limitations in the scope of the Estonian money laundering offence: conspiracy to conduct a money laundering offence is not criminalised; it is not entirely clear whether prior conviction for predicate offence is required for convicting money laundering. The Estonian terrorist financing offence does not cover financing of an individual terrorist thus the scope of the offence is more narrow compared to international standards. These limitations in the money laundering and terrorist financing offences in turn limit the extent to which coercive measures may be applied in Estonia in response to a request for legal assistance because of the requirement of dual criminality contained in the reservation to the *European Convention on Mutual Assistance in Criminal Matters* (CETS 30). The EU Council Framework Decision of 22 July 2003 on the execution in the European Union of orders of freezing property or evidence (OJ L 196, 2.8.2003 p. 45), which provides for an exception to the requirement for dual criminality where a request to apply a freezing order is received from a European Union country, has been implemented by Estonia with an amendment to the CCP (§§ 508^{1}—508^{12}).

878. Estonian authorities stated that Estonia will only execute letters rogatory for search or seizure of property where execution is consistent with Estonian law and with prejudice to reservation and declaration made by Estonia, in the instrument of ratification of the *European Convention on Mutual Assistance in Criminal Matters* (CETS 30).

879. Therefore, the concerns expressed by the evaluators in the second MONEYVAL evaluation report on the possible restriction of providing mutual legal assistance due to the requirement for dual criminality still remain.

Recommendation 38

880. In the Second Evaluation Report the Estonian authorities were recommended to review their domestic legislation to ensure that it does not contradict the wide obligations under the Strasbourg Convention to take provisional measures on behalf of foreign states where the subject matter of the application is criminal proceeds, as widely defined in that Convention, and that it is capable of rendering such assistance where there is no extradition request. This recommendation was made on the basis of the existing provisions in the CCP in force since 2000 concerning provisional measures to secure confiscation on request of a foreign state (§413^{2} and §413^{9}).

881. The present version of the CCP does not contain such a detailed regulation of this issue. In their replies to the Questionnaire, Estonian authorities referred to the general provision of § 142 CCP, which regulates the seizure of property as recording the property of a suspect, accused or civil defendant or the property which is the object of money laundering and preventing the transfer of the property. As § 142 CCP does not address international aspects, Estonian authorities stated that the legal basis for applying this article in international co-operation matters would be § 433 (3) CCP, which reads as follows: "*International co-operation in criminal procedure shall be effected pursuant to the provisions of the other chapters of this Code in so far as this is not in conflict with the provisions of this Chapter."*

882. Requests for seizure and confiscation of assets may be made under the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (*Strasbourg Convention*; CETS 141).

883. Estonia is a party to the European Convention on the International Validity of Criminal Judgements (CETS 70). The general conditions for enforcing foreign criminal judgments are found in the Division 5 CCP "*Recognition and Execution of Judgments of Foreign Courts*". § 476 CCP provides that assistance may be provided to a requesting state in the execution of a punishment or any *other sanction* imposed for a criminal offence if a corresponding request together with the court judgment which has entered into force or an authenticated copy thereof has been submitted to the Ministry of Justice. According to the Estonian authorities the term "*other sanction*" implies also confiscation and this confiscation must be ordered in a foreign judgement, which is final and enforceable.

884. § 477 (4) states that if a judgment on confiscation made in a requesting state concerns a person outside the proceeding, the judgment shall not be executed in Estonia if such third party has not been given the opportunity to protect his or her interests, or the judgment is in conflict with a court decision made in the same matter by way of civil procedure pursuant to Estonian law. The procedure requires the Ministry of Justice to verify whether a request is in compliance with the requirements and has the required supporting documents and, in the case of compliance, the Ministry of Justice forwards the request to the court immediately. The rights of the person convicted are guaranteed in Estonian law in § 480 CCP, which provides for the participation of a counsel (an advocate) in taking over of execution of confiscation. The jurisdiction over recognition of foreign court judgment belongs exclusively to the Harju County Court and it has to decide within thirty days as of the receipt of the request. Persons outside the proceedings whose interests are concerned by a court judgment may be summoned to a court session if they are in Estonia. In deciding on confiscation, the participation of a third party is mandatory. If after summoning it turns out that the person is not present in Estonia, the confiscation procedure may continue. Estonian authorities advised that there has been executed so far one case of a foreign confiscation order where a third party was involved. Pecuniary punishments, fines to the extent of assets and *amounts subject to confiscation* shall be converted into EEK on the basis of the exchange rate applicable on the date of specification of the punishment.

885. The Estonian authorities consider that § 84 Penal Code ("Substitution of confiscation") applies also in international context and therefore the requirements in Criterion 38.1 are also met where the request relates to property of corresponding value. This provision reads as follows: „*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.*"

886. Estonia has not concluded special bi- or multilateral agreements enabling co-ordination of seizure and confiscation actions with other countries.

887. Estonia does not have and it was also not considered establishing an asset forfeiture fund into which all or a portion of confiscated property will be deposited and will be used for law enforcement, health, education or other appropriate purposes.

888. § 85 (1) PC envisages that confiscated objects shall be transferred into state ownership or, in the cases provided for in an international agreement, shall be returned. §§ 469-470 CCP contain provisions on the transfer of confiscated property to Estonia and to another state: A foreign state may be requested to hand over property located in such state if "*the property claimed has been acquired by a criminal offence"* subject to proceedings in the requesting state or if the property is required as physical evidence in a criminal proceeding conducted in the requesting state. Dual criminality is requested. The rights of a third party shall be preserved and the property shall be delivered to the entitled person outside the proceedings at the request of the person after the entry into force of the court judgment. In cases of urgency, seizure of property or the conduct of a search may be requested before submission of a request to hand over property.

889. Handing over of property to a foreign state by Estonia shall be decided by a ruling of a judge of the county court of the location of the property. Handing of property over to the requesting foreign state shall be organised by the competent judicial authority. In cases of urgency, property may be seized or a search may be conducted at the request of a foreign state before receipt of the request to hand over property.

Additional elements

890. There are no provisions in Estonian law that would allow for the recognition and enforcement of foreign non-criminal confiscation orders in Estonia

Special Recommendation V

891. SR V requires, among other things, that each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquires and proceedings related to financing of terrorism, terrorist acts and terrorist organisations.

892. The MLA mechanisms applicable in Estonia were described above, while assessing the compliance with Recommendations 36 to 38. The same legal provisions are applicable to terrorism financing.

Statistics

893. The Estonian FIU provided the following statistics concerning mutual legal assistance:

Mutual legal assistance in money laundering cases			
	2005	**2006**	**2007**
To Estonia	6	5	35
From Estonia	0	2	8

Mutual legal assistance in financing terrorism cases			
	2005	**2006**	**2007**
To Estonia	0	3	0
From Estonia	0	1	0

894. Before the plenary discussion, Estonian authorities advised that they also keep statistics concerning:
- source of request (country of origin);
- type of offence;
- date of the request;
- date for the fulfillment of the request;
- time period for fulfilling the request.

6.3.2 Recommendations and comments

895. Estonian authorities have the power and resources to respond to requests for legal assistance from abroad in a timely, constructive and effective manner. The Ministry of Justice is the central authority in co-operation in criminal matters; it has enough instruments and legal possibilities at its disposal to handle the incoming requests, to check them for compliance and to co-operate with the judicial authorities thus enabling Estonia to complete MLA requests in a timely manner. There is a mechanism available for prioritizing and expediting assistance in urgent cases. When Estonia

is submitting MLA requests to a foreign state and the case is urgent, the request may also be submitted through the International Criminal Police Organisation (Interpol) and communicated concurrently through the judicial authorities.

896. The ability to respond to foreign requests for formal investigative assistance or the provision of material for formal evidence in money laundering cases depends on whether the money laundering offence is punishable as a criminal offence in Estonia. The ability to respond to requests for investigative assistance on confiscation issues will depend on whether the offence for which confiscation is being pursued in the requesting state is liable for confiscation measures in Estonia

897. However, international cooperation in the area of money laundering and terrorist financing could in some instances suffer from certain gaps in the national legislation, in particular in respect of the dual criminality requirement and the deficiencies in covering international standards concerning the terrorist financing offence. Apart from this there is also the inability to execute the civil confiscation orders.

898. Arrangements for coordinating seizure and confiscation action with other countries should be established. Consideration should also be given to establishment of an asset forfeiture fund as well as to sharing of confiscated assets with other countries when confiscation is a result of coordinated law enforcement action.

899. In addition, Estonia was unable to show that statistics are kept on the predicate offences, the nature of the request, whether it was granted or refused, and the time required to respond. Thus it is very difficult to evaluate the effectiveness of these measures in practice.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors underlying rating
R.36	**LC**	• The shortcomings of the money laundering and the terrorist financing offence may limit mutual legal assistance based on dual criminality.
R.37	**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.
R.38	**LC**	• No arrangements for coordinating seizure and confiscation action with other countries are established. • Establishment of an asset forfeiture fund was not considered. • No sharing of confiscated assets with other countries when confiscation is a result of coordinated law enforcement action is applied.
SR.V	**LC**	• The shortcomings of the domestic legislation intended to cover the financing of terrorism may limit mutual legal assistance based on dual criminality.

6.4 Extradition (R. 37 and 39, SR.V)

6.4.1 Description and analysis

900. Estonia requests dual criminality in order to implement European Convention on Extradition from 1957 and other international conventions, containing extradition rules as well as on the basis of bilateral agreements concluded by Estonia so far. The rule for dual criminality is stipulated in § 439 (1) CCP "*General conditions for extradition of persons to foreign states*", which reads as follows:

> *Extradition of a person for the purposes of continuation of the criminal proceedings concerning him or her in a foreign state is permitted if the person is suspected or accused of a criminal offence which is punishable by at least one year of imprisonment according to both the penal law of the requesting state and the Penal Code of Estonia."*[63]

901. Concerning the European Arrest Warrant (EAW), Estonia implements the principles laid down in the Framework decision on EAW. Therefore, in relation with another EU Member State, dual criminality is not required for the designated offences, if in the issuing State they carry no less than three years of imprisonment or with another more severe penalty, or for them a measure requiring detention for no less than of 3 years is provided. The list of the offences includes money laundering and terrorism financing.

902. Extradition in Estonia is based on the European Convention on Extradition (CETS 24), the EU Council Framework Decision on the European Arrest Warrant and the surrender procedures between Member States, bilateral and multilateral extradition agreements.

903. Extradition and surrender procedures are regulated in chapter 19 of Code of Criminal Proceedings.

904. Estonia is also party to several international agreements addressing exclusively or partially MLA and extradition issues, e.g.

- Agreement on cooperation in crime prevention between Government of Republic of Estonia and Government of Republic of Finland;
- Agreement on legal assistance and legal relationships in civil and criminal matters between Republic of Estonia and Ukraine;
- Agreement on legal assistance and legal relationships in civil, family and criminal matters between Republic of Estonia and Russian Federation;
- Agreement on legal relationships between Republic of Estonia, Republic of Lithuania and Republic of Latvia;
- Agreement on mutual legal assistance between Government of Republic of Estonia and Government of United States of America;
- Agreement on provision of legal assistance and legal relationships in civil and criminal matters between Republic of Estonia and Republic of Poland;
- Convention Drawn up on the Basis of Article K.3 of The Treaty on European Union, Relating to Extradition Between the Member States of the European Union;
- Convention Drawn up on the Basis of Article K.3 of the Treaty on European Union, on Simplified Extradition Procedure Between the Member States of the European Union;
- Convention Drawn up on the Basis of Article K.3 of the Treaty on European Union, on Mutual Assistance and Cooperation between Customs Administrations;
- Convention implementing the Schengen Agreement;

[63] Emphasis added.

- Convention on Cybercrime;
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime;
- European Convention on Extradition and its two Additional Protocols;
- European Convention on International Validity of Criminal Judgements;
- European Convention on Mutual Assistance in Criminal Matters and its Additional Protocol;
- European Convention on the Supervision of Conditionally Sentenced or Conditionally Released Offenders;
- European Convention on the Suppression of Terrorism;
- European Convention on the Transfer of Proceedings in Criminal Matters;
- European Convention on the Transfer of Sentenced Persons and its Additional Protocol;
- Extradition Treaty between the Government of the Republic of Estonia and the Government of the United States of America.

Extradition procedure with non EU countries

905. In order to be extraditable, a criminal offence should be punishable by at least one year of imprisonment. Thus, money laundering is an extraditable offence in Estonia. According to Estonian authorities there are no particular obstacles for extraditing persons charged with a money laundering offence.

906. However, absence of dual criminality provides a ground for refusing extradition. Extradition requests are handled with urgency.

European Arrest Warrant (Extradition procedure with EU countries)

907. The Code of Criminal Proceedings implements in §§ 490-508 the Council Framework Decision on the European Arrest Warrants and the surrender procedures between EU Member States. Both the criminal offences of money laundering and terrorist financing fit into categories of criminal offences for which the principle of dual criminality is abolished within the European Union. The fact that a person is a national shall not be a ground for refusing execution of a European Arrest Warrant. Simplified surrender is made dependent on consent of the person subject to surrender.

908. The EAW should be sent in the form set out in the Framework Decision and must contain:
– the name and nationality of the person sought;
– details of the issuing judicial authority;
– details of the offences, the dates, times and circumstances and the degree of involvement of the person sought;
– whether the person has been convicted, sentenced or is liable to detention or whether a warrant for the person's arrest has been issued; the penalty to which the person would be liable if convicted or to which he or she is liable, having already been convicted, or the penalty imposed.

909. The EAW procedure has not been applied, as yet, in a money laundering case or in the case of terrorist financing.

910. Concerning extradition it has to be noted that the Estonian Constitution prohibits to extradite Estonian citizens to foreign states:

> ***Art. 36****. [...] No Estonian citizen shall be extradited to a foreign state, except under conditions prescribed by an international treaty and pursuant to procedure provided by such treaty and by law. Extradition shall be decided by the Government of the Republic. Everyone who is under an extradition order has the right to contest the extradition in an Estonian court [...]..*

911. From this general restriction exist some exceptions as Estonia can extradite its nationals according to provisions of international commitments; e.g. under the European Arrest Warrant (EAW), Estonian nationals may be extradited under condition that the execution of detention shall take place in Estonia (but Estonian nationals shall not be extradited for execution if the verdict has already been made).

912. Another limitation concerning extradition of Estonian nationals can be found in § 440 (2) CCP: extradition of an Estonian citizen is not permitted if the request for extradition is based on a military offence within the meaning of the provisions of the European Convention on Extradition and the Additional Protocols thereto.

913. Criterion 39.2(b) requires that a country that does not extradite its own nationals solely on the grounds of nationality, should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the extradition request. In Estonia, such a situation may occur when there is a case outside the scope of the EAW and no other int. arrangements exist. However, the Estonian authorities could not point to a specific provision which would provide for such a possibility. Though the Estonian authorities explained that if extradition of Estonian nationals is refused they would be considered for prosecution in Estonia (Estonian authorities pointed inter alia to § 474 (5) CCP), this is not the same as required by criterion 39.2b), particularly is missing that such requests should be submitted *without undue delay* to competent Estonian authorities.

914. As regards the applicable procedure, the extradition of an Estonian citizen is decided by the Government of where the draft extradition decisions is prepared and submitted by the Ministry of Justice. The extradition of a foreigner is decided by the Minister of Justice (§ 452 (1), (2) CCP).

915. Concerning the cases where Estonia can extradite its own nationals, there are no obstacles as regards international cooperation in procedural or evidentiary aspects.

916. The procedure for the extradition of a person to a foreign state is divided into the preliminary proceeding in the Ministry of Justice and the Public Prosecutor's Office, verification of the legal admissibility of the extradition in court, and deciding on extradition falling within the competence of the executive power (§ 443 CCP).

917. To avoid undue delays and in line with Criterion 39.4, time limits are envisaged at each stage of the above described procedure. Relevant provisions can be found in

- § 444 (3) CCP: a request for extradition which meets the requirements and the supporting documents shall be sent by the Ministry of Justice to the Public Prosecutor's Office *promptly*;
- - § 445 (4) CCP: the Public Prosecutor's Office shall send a request for extradition which meets the requirements and the additional materials to the court *immediately*.
- § 447 (2) CCP: in cases of *urgency*, a preliminary investigation judge may apply provisional arrest at the request of the Public Prosecutor's Office before the arrival of the request for extradition;
- 447 (5) CCP: a person with regard to whom provisional arrest has been applied may be released if the requesting state fails to send the request for extradition within *eighteen days* as of the application of provisional arrest with regard to the person. A person with regard to whom provisional arrest has been applied shall be released if the request for extradition does not arrive within *forty days* as of the application of provisional arrest;
- § 450 (1) CCP: in order to verify the legal admissibility of an extradition in court, a court hearing shall be held within *ten days* as of the receipt of the request for extradition by the court;
- § 452 (6): a decision on the extradition of a person which has entered into force shall be *immediately* sent to the Central Criminal Police who shall organise the execution of the decision;

- § 452 (8): the Ministry of Justice shall *immediately* notify a requesting state of a decision to grant or refuse to grant extradition.

918. In case of conflicting requests for extradition, § 441 CCP provides that if extradition of a person is requested by several states, the state to which the person is to be extradited shall be determined having regard, primarily, to the seriousness and place of commission of the criminal offences committed by the person, the order in which the requests were submitted, the nationality of the person claimed and the possibility of his or her subsequent extradition to a third state.

Additional elements

919. According to § 444 CCP, the central authority in extradition matters is the Ministry of Justice. Therefore, the direct transmission of the extradition requests between the competent ministries is the general rule. The Ministry of Justice verifies the compliance of a request for extradition with the requirements, and the existence of the necessary supporting documents. If necessary, the Ministry of Justice may grant a term to a requesting state for submission of additional information. If a request for extradition submitted by a foreign state is received directly by the Public Prosecutor's Office, the Ministry of Justice should be immediately notified of such a request. If a request for extradition is received directly by the Public Prosecutor's Office, additional information may be requested without the mediation of the Ministry of Justice (§ 445 CCP). For requests between EU member states, direct contact between the competent authorities is permitted.

920. § 449 CCP provides for a simplified extradition procedure

> *"(1) An alien may be extradited to the requesting state pursuant to the simplified procedure without verification of the legal admissibility of the extradition, on the basis of a written consent granted by the alien in the presence of his or her counsel.*
> *(2) A proposal to consent to extradition pursuant to the simplified procedure shall be made to the person claimed upon his or her detention. The consent shall be immediately communicated to the Minister of Justice who shall decide on the extradition of the person pursuant to the procedure provided for in § 452 of this Code.*
> *(3) A decision of the Minister of Justice on the extradition of an alien pursuant to the simplified procedure shall be promptly forwarded to the Central Criminal Police for execution and to the Public Prosecutor's Office for their information. A decision by which extradition pursuant to the simplified procedure is refused shall be sent to the Public Prosecutor's Office who shall decide on the submission of a request to take over the criminal proceeding from the foreign state."*

Special Recommendation V

921. Since terrorist acts and financing of terrorism are crimes under Estonian law punishable by over 1 year of imprisonment, and thus are in terms of law extraditable offences, extradition for such offences of any person, irrespective of nationality, may be granted.

922. Nevertheless the deficiencies in the legal regulation of terrorist financing compared to the international standards (financing of individual terrorist act is not criminalised, collecting of funds needs further legal improvement etc.) and the requirement for dual criminality may impede the extradition for terrorist financing offence.

Statistics

923. Estonian authorities provided the following statistics concerning extradition requests:

Extradition requests								
	Requests sent				Requests received			
	2004	2005	2006	2007	2004	2005	2006	2007
in total	18	11	6	2	13	9	1	6
executed	18	11	6	2	13	9	1	4
refused	-	-	-	-	-	-	-	2
pending	-	-	-	-	-	-	-	-
suspended	-	-	-	-	-	-	-	-

924. The evaluation team was not provided with statistics showing the time in which Estonia responded to extradition requests. In the absence of such statistics it is not possible to determine whether extradition requests are handled without undue delay.

6.4.2 Recommendations and comments

925. The extradition provisions appear comprehensive and in compliance with international standards.

926. Though the Estonian Constitution does in principle not allow for the extradition of Estonian citizens, there are a number of exceptions of this general rule. However, with regard to criterion 39.2b) there are no explicit provisions within 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. In Estonia, such a situation may occur when there is a case outside the scope of the EAW and no other int. arrangements exist. Though Estonian authorities explained that if extradition of Estonian nationals is refused they would be considered for prosecution in Estonia, this is not the same as required by criterion 39.2b), particularly is missing that such requests should be submitted *without undue delay* to competent Estonian authorities.

927. A decision on extradition for a money laundering and for terrorist financing offences would depend on whether the offence for which a person was wanted was punishable as money laundering, respectively terrorist financing in Estonia – thus e.g. money laundering committed in conspiracy or financing individual terrorist act may not be extraditable; though this presumably should be in practice no major obstacle as the Ministry of Justice which is the central authority for the processing of requests for extradition and mutual assistance and also the courts interpret the element of dual criminality very broadly.

928. The evaluation team was not provided with statistics showing the time in which Estonia responded to extradition requests. In the absence of such statistics it is not possible to determine whether extradition requests are handled without undue delay.

6.4.3 Compliance with Recommendation 37 and 39 and Special Recommendation V

	Rating	Summary of factors relevant to Section 6.4 underlying overall rating
R.37	**LC**	• 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.
R.39	**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. • In the absence of detailed statistics it is not possible to determine whether extradition requests are handled without undue delay.
SR.V	**LC**	• The lack of a comprehensive domestic incrimination of financing of terrorism may impede the extradition possibilities of Estonia.

6.5 Other Forms of International Co-operation (R. 40 and SR.V)

6.5.1 Description and analysis

929. The **FIU** has been a member of Egmont Group since 2000 and it actively participates in its activities. The FIU uses the Egmont secure web site for information exchange and, fax, e-mail or mail can be used if needed. § 46 of the MLTFPA states that the FIU "*has the right to exchange information and enter into cooperation agreements with foreign agencies which perform the functions of a financial intelligence unit*". Even though the FIU can exchange information directly and spontaneously with other FIUs even without having an MoU in place, it has signed a number of MoUs (for a list see above para 344). In 2006, the joint platform of the EU Financial Intelligence Units was established on the EU level under the leadership of the European Commission with the aim of developing international cooperation between the EU FIUs. Since 2006 the FIU is also the national point of contact for Estonia in the CARIN network.

930. International cooperation within the **Estonian Police** is carried out on different levels. The Police Board coordinates international cooperation of the whole Estonian police, including cooperation with the EU. Three national police agencies (Central Criminal Police, CLEP and FSC) cooperate with police agencies and international organisations of other states. The Central Criminal Police is the body responsible for operative cross border cooperation. It houses the Interpol National Bureau, the Europol National Unit and the Sirene Bureau. The Central Criminal Police also has liaison officers abroad (Finland, Russia). Estonia became a member of Interpol in 1992 and of Europol in 2005. Police authorities may directly exchange information with police authorities of foreign countries using Europol or Interpol channels. Such exchanges of information between law-enforcement authorities is possible upon request and in relation to both money laundering and underlying predicate offences. International co-operation concerning investigations must be in accordance with the Code of Criminal Procedure.

931. According to § 47 of the Financial Supervision Authority Act (FSAA), the **FSA** is empowered to exchange information with its foreign counterparts "*for the performance of its duties and exchange of information*". In this context, § 47(2) FSAA specifies that the FSA has the right to send and exchange confidential information which is necessary for the performance of its foreign counterparts' functions. Furthermore, the FSAA stipulates that information sent, received or exchanged in this manner is deemed to be confidential and can be used only for supervisory purposes. §47 (7) FSAA stipulates that the FSA "*has the right to use the competence and rights granted thereto by [the FSAA] and other legislation in order to fulfil the request of a foreign financial supervision authority submitted for the receipt of information, restriction of a right or performance of another act or activity if, in the opinion of the foreign financial supervision authority, this is essential for the performance of its supervision activities.*"

932. The Estonian FSA has concluded Memoranda of Understanding with the supervisory authorities of Finland, Sweden, Denmark, Germany, Switzerland, the Netherlands, Cyprus, Latvia and Lithuania. The evaluators were advised that most of the said MoUs contain articles promoting cooperation on financial crime and/or money laundering issues. At the time of the on-site visit, a draft MoU was under negotiation with the Bank of Russia[64]. The MoUs signed by the FSA with its foreign counterparts allow the exchange of information both spontaneously as well as upon request. All MoUs concluded by the FSA contain, as a rule, a list of contact persons, who can be contacted directly to safeguard the most efficient flow of information. Moreover, the FSA Act (§ 47) provides for the exchange of information with a foreign supervisory authority upon receipt of a reasoned request and, at the same time, allows the provision of spontaneous information at the FSA's initiative.

933. The Estonian FSA advised that joint on-site inspections (covering inter alia AML/CFT preventive issues) of financial institutions were carried out with the financial supervisory authorities of Finland, Sweden, Latvia and Lithuania.

Statistics

934. The FIU keeps statistics in an Excel-format concerning requests received from and sent to other FIUs. These statistics provide a breakdown concerning the countries involved. In conclusion, in 2004 the FIU received 91 requests from 23 countries and sent 30 requests, in 2005 the FIU received 81 requests from 26 countries and sent 64 requests, and in 2006 the FIU received 113 requests from 34 countries and sent 45 requests. However, it has to be noted that the figures provided to the evaluation team were not always harmonised and sometimes there were differences. Although the Estonian authorities indicated that the average time for responding to foreign requests is less than 30 days (and in emergency cases can be processed within 48 hours), the evaluators were not provided with statistics indicating the time of response and it is unclear whether this statement is based on figures or estimation.

935. The FSA does not keep statistics concerning its information exchange with foreign supervisory bodies. Representatives of the FSA explained that this is not done because there is a permanent exchange of information based on the terms specified in the various Memoranda of Understanding. It was explained that the majority of requests are related to licensing procedures, including information on fit and proper status of senior management and owners, origin of funds and relevant procedures as well as results of external and internal audit reports.

6.5.2 Recommendations and comments

936. The FSA should keep comprehensive statistical information on the exchange of information with foreign counterparts (including spontaneous exchange of information).

6.5.3 Compliance with Recommendation 40 and SR.V

	Rating	Summary of factors relevant to Section 6.5 underlying overall rating
R.40	**C**	
SR.V	**C**	

[64] The MoU with the Russian Central Bank was signed in August 2008. This MoU, which is available on the website of the FSA (http://www.fi.ee/failid/MoU_EFSA_and_Bank_of_Russia.pdf), also includes articles on the exchange of information concerning anti-money laundering and counter terrorist financing issues.

7 OTHER ISSUES

7.1 Resources and Statistics

Remark: *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 contains the boxes showing the rating and the factors underlying the rating.*

Recommendation 30

7.1.1 Resources - Compliance with Recommendation 30

	Rating	Summary of factors underlying rating
R.30	**LC**	• The number of staff of the FIU seems insufficient with regard to its supervision duties. • The Police do not have enough resources (human and technical) to deal satisfactorily with economic crimes. • The TCB do not have enough resources (human and technical). • Supervisory authorities lack the manpower required to carry out comprehensive on-site supervision regarding all obligated persons.

Recommendation 32

7.1.2 Statistics - Compliance with Recommendation 32

	Rating	Summary of factors underlying rating
R.32	**LC**	• The statistics on MLA are not kept on the predicate offences. • The evaluation team was not provided with statistics showing the time in which Estonia responded to extradition requests. • No statistical information was available on the exchange of information by the FSA with foreign counterparts.

IV. TABLES

Table 1: Ratings of Compliance with FATF Recommendations
Table 2: Recommended Action Plan to improve the AML/CFT system

Table 1. Ratings of Compliance with FATF Recommendations

For each Recommendation there are four possible levels of compliance: Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC). In exceptional circumstances a Recommendation may also be rated as not applicable (N/A). These ratings are based only on the essential criteria, and defined as follows:

Compliant	The Recommendation is fully observed with respect to all essential criteria.
Largely compliant	There are only minor shortcomings, with a large majority of the essential criteria being fully met.
Partially compliant	The country has taken some substantive action and complies with some of the essential criteria.
Non-compliant	There are major shortcomings, with a large majority of the essential criteria not being met.
Not applicable	A requirement or part of a requirement does not apply, due to the structural, legal or institutional features of a country *e.g.* a particular type of financial institution does not exist in that country.

Forty Recommendations	Rating	Summary of factors underlying rating[65]
Legal systems		
1. Money laundering offence	**LC**	• Unclear if money laundering may be convicted without a prior or simultaneous conviction for the predicate offence. • Conspiracy to commit money laundering is insufficiently covered in legislation.
2. Money laundering offence Mental element and corporate liability	**C**	
3. Confiscation and provisional measures	**LC**	• 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 applies to only part of the designated offences (among which neither money laundering nor terrorist financing offences are included). • Instrumentalities used or intended to be used in the commission of a crime are not subject to value

[65] These factors are only required to be set out when the rating is less than Compliant.

		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.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**LC**	• The provisions allowing the sharing of information between financial institutions where this is required by R. 7, R. 9 and SR VII are drafted in a complicated way and leave some discretion and uncertainty in interpretation which may hamper their practical application.
5. Customer due diligence	**LC**	• The obliged entities are allowed to rely on CDD information received *inter alia* from a credit institution which has been registered or whose place of business is in a country (outside the European Economic Area) where requirements equal to those provided in the MLTFPA are in force. There is no guidance available for financial institutions on which countries satisfactorily fulfil these requirements. • Concerning beneficial ownership, the language in the law is not clear as to whether it also covers instances when a natural person acts for another natural person. • The Estonian approach to address "*high risk of money laundering or terrorist financing*" sets the level to apply enhanced CDD measures to a higher level than "*higher risk*" in terms of the Methodology. The categories which require enhanced CDD measures seem insufficient and there is also no guidance on the existing categories. • The MLTFPA allows for the application of simplified CDD measures in case of credit or financial institutions located in a contracting state of the European Economic Area or a third country, which in the country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision. At present, no guidance from the Estonian supervisory bodies exists specifying which third countries fulfil these criteria. • There is not yet guidance from the Minister of Finance specifying the requirements for rules of procedure of the obliged entities dealing with situations in which a business relationship begins prior to full CDD. • The MLTFPA does not require termination of the business relationship in instances in which a request for additional documentation arising only from ongoing due diligence remains unfulfilled.

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. • 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 explicitly requires understanding the respondent bank's business. • There is no clear legal requirement to obtain approval from senior management before establishing new correspondent relationships. • 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). • 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	**PC**	• There are no specific provision in the law which address financial institutions to have policies in place or take such measures as may by needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.
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. • Concerning criterion 9.4, there has been no guidance issued by the Estonian authorities to advise financial institutions on 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. • 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 a third party.
10. Record keeping	**LC**	• There is no requirement in law or regulation to keep documents longer than five years if requested by a competent authority.
11. Unusual transactions	**PC**	• Financial institutions are not required to examine the background and the purpose of complex/unusual large transactions and thus to keep a record of the written findings which will be accessible for competent authorities/auditors.

12. DNFBP – R.5, 6, 8-11	**PC**	• The same concerns in the implementation of Recommendations 5, 6, 8 – 11 apply equally to DNFBP (see section 3 of the report). • There are no Regulations/Directives to DNFBP laying down requirements for internal control procedures for managing AML/CFT risks. • Though DNFBP are required under § 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 DNFBP should take to mitigate the risks for non-face-to face relationships and transactions. • Casinos are required to identify but not to verify the name of a client who pays or receives in a single transaction or several related transactions an amount exceeding 30 000 EEK (1 917.34 EUR) or the equivalent in another currency.

13. Suspicious transaction reporting	**LC**	• Not all kind of attempted transactions are clearly covered by the reporting obligations.
		• There is no reporting obligation in case of:
		  • financing of an individual terrorist;
		  • collecting of funds for the purpose of terrorist financing;
		  • the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist;
		  • those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC).
		• Savings and loan associations as well as the insurance sector sent no STRs so far which is presumably caused by a lack of understanding or awareness of their reporting obligations.

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 the on site visit, were based on a Regulation of the Minister of Finance issued under the previous law. • Financial institutions are not required to have guidance in their internal rules concerning the detection of unusual and suspicious transactions. • Limited requirements concerning screening

		procedures for new employees. • Financial institutions are not required to include in their training of employees current AML/CFT techniques methods and trends.
16. DNFBP – R.13-15 & 21	**PC**	• The same deficiencies in the implementation of Recommendations 13, 15 and 21 in respect of financial institutions apply equally to DNFBP. • Lawyers and real estate dealers as well as accountants and auditors have sent only a very small number of STR so far.
17. Sanctions	**PC**	• The general provisions of the Credit Institution Act used by the FSA do not provide a clear basis to issue precepts regarding those violations of AML/CFT obligations which are not directly sanctionable by §§ 57 ff of the MLTFPA. • The sanctioning regime utilizing precepts according to §§ 103 ff of the Credit Institutions Act places sanctions at one remove, in that a precept first needs to be issued before formal sanctions, e.g. penalty payments or suspension of a license, can be imposed based on a finding of a violation of the precept. • The FIU does not have powers to withdraw or suspend registration of financial institutions in case they fail to comply with AML/CFT requirements.
18. Shell banks	**LC**	• The CrIA does not clearly prohibit the establishment or continuous operation of shell banks in Estonia which are operated from outside of the European Economic Area (EEA).
19. Other forms of reporting	**C**	
20. Other DNFBP and secure transaction techniques	**C**	

21. Special attention for higher risk countries	**NC**	• There are no obligations in law or regulation or other enforceable means requiring financial institutions to
		  • give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations.
		  • to examine and monitor such transactions, if they do not have an apparent economic or visible lawful purpose, and have written findings available to assist competent authorities and auditors.
		• There are no specific provisions on application of counter- measures where a country continues not to apply or insufficiently applies the FATF Recommendations.

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. • 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. • 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**	• There are no legal provisions to explicitly 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 function. • For financial institutions which are not supervised by the Estonian FSA pursuant to § 2 of the FSA Act no registration no registration requirements apply [66].
24. DNFBP - Regulation, supervision and monitoring	**PC**	• Lack of fit and proper checks to beneficial owners and managers of casinos. • Not all trust and company service providers required to be registered. • Lawyers acting outside the Bar Association (independent legal professionals) are not subject to effective supervision by the FIU. • Lack of adequate mechanisms for supervision by the Estonian Bar Association and Chamber of Notaries. • Lack of sufficient supervisory staff in the FIU.
25. Guidelines and Feedback	**PC**	• In the light of the changes of the Estonian AML/CFT system because of coming into force of the new MLTFPA, the guidelines issued by the FSA seem already out of date. • The FIU has not yet issued guidelines explaining the legal requirements and preventive measures described therein to its supervised entities. • Insufficient guidance to DNFBP by supervisory bodies (FIU, Bar Association, Chamber of Notaries).
Institutional and other measures		
26. The FIU	**C**	
27. Law enforcement authorities	**C**	
28. Powers of competent	**C**	

[66] see FN 49.

authorities		
29. Supervisors	**LC**	• There is no explicit provision empowering the FIU to compel the off-site production of records from supervised entities for supervisory purposes absent a suspicion of money laundering or terrorist financing.
30. Resources, integrity and training	**LC**	• The number of staff of the FIU seems insufficient with regard to its supervision duties. • The Police do not have enough resources (human and technical) to deal satisfactorily with economic crimes. • The TCB do not have enough resources (human and technical). • Supervisory authorities lack the manpower required to carry out comprehensive on-site supervision regarding all obligated persons.
31. National co-operation	**LC**	• There seems to be no much formal co-ordination (in terms of formal agreements, sharing of information etc.) between the supervisory bodies.
32. Statistics	**LC**	• The statistics on MLA are not kept on the predicate offences. • The evaluation team was not provided with statistics showing the time in which Estonia responded to extradition requests. • No statistical information was available on the exchange of information by the FSA with foreign counterparts.
33. Legal persons – beneficial owners	**LC**	• There is limited control over the implementation of obligations of legal persons to submit updated information on ownership and control to the commercial register. • Requirements that limited liability companies maintain share registers and shareholder registers are not supervised. • The legal framework does not ensure adequate, accurate and timely information on the beneficial ownership and control of legal persons.
34. Legal arrangements – beneficial owners	**NA**	
International Co-operation		
35. Conventions	**LC**	*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 "collecting of funds". • No specific criminalisation of the 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 are not covered.
36. Mutual legal assistance (MLA)	**LC**	• The shortcomings of the money laundering and the terrorist financing offence may limit mutual legal assistance based on dual criminality.
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. • 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. • Establishment of an asset forfeiture fund was not considered. • 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. • 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	**C**	
Nine Special Recommendations		
SR.I Implement UN instruments	**PC**	• 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.
SR.II Criminalise terrorist financing	**PC**	• Financing of an individual terrorist is not criminalised. • The terrorist financing offence does not cover "collecting of funds". • Current law does not specifically criminalise the

		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 are not covered.
SR.III Freeze and confiscate terrorist assets	**PC**	• Estonia does 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) does not cover funds controlled by a designated person or persons acting on their behalf or at their direction (as it is required by UNSCR 1267 and UNSCR 1373). • Estonia does 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 are aware of the procedures to be followed in order to implement the UNSC Resolutions.
SR.IV Suspicious transaction reporting	**LC**	• There is no reporting obligation in case of: – financing of an individual terrorist; – collecting of funds for the purpose of terrorist financing; – the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist; – those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC). • Not all kind of attempted transactions are clearly covered by the reporting obligations. • In the absence of detailed statistics before 2008 it is difficult to evaluate the effectiveness of the system.
SR.V International co-operation	**LC**	• The shortcomings of the domestic legislation intended to cover the financing of terrorism may limit mutual legal assistance based on dual criminality. • The lack of a comprehensive domestic incrimination of financing of terrorism may impede the extradition possibilities of Estonia.
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	**PC**	• No review of the adequacy of relevant laws and regulations to prevent the abuse of NPOs for financing of terrorism has been undertaken. • Authorities do not conduct outreach or provide guidance on terrorist financing to the NPO sector. • There is no supervision or monitoring of the NPO sector as envisaged by the Interpretative Note to SR VIII. • There are no particular mechanisms in place for a prompt sharing of information among all relevant competent authorities when there is suspicion that a particular NPO is being exploited for terrorist financing purposes. • No special points of contact or distinguished procedures to respond to international requests for information regarding particular NPOs.
SR.IX Cross Border declaration and disclosure	**PC**	• There are no legal provisions ensuring that there is under the circumstances of Special Recommendation IX at any time a designated competent authority which is authorised to stop or restrain currency or bearer negotiable instruments when there is a suspicion of money laundering or terrorist financing. • There are no legal provisions ensuring that there is under the circumstances of Special Recommendation IX at any time a designated competent authority to seize cash when there is a suspicion of money laundering or terrorist financing. • As the disclosure system has been established only in mid 2007, there are not yet comprehensive statistics available. Thus, it is not yet possible to assess the effectiveness of the system. • EC regulation No. 1889/2005 and relevant national legislation do not cover the transfer of cash or bearer negotiable instruments between Estonia and another EU member state[67].

[67] see FN 28.

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 & 2)	• It should be made clear in the law or by way f guidance and training that the prosecution of money laundering does not require a prior or simultaneous conviction for the predicate offence. • Estonia should introduce the full concept of conspiracy for the money laundering offence.
2.2 Criminalisation of Terrorist Financing (SR.II)	• It is recommended to amend the legal text criminalising terrorist acts and the provision criminalising terrorist financing in a way that they would be broad and detailed enough to cover, besides the financing of terrorist organisations, also all terrorist acts as required by the UN Conventions and the financing of individual terrorists. These provisions should also: – clearly cover the various elements required by SR.II, in particular the collection of funds by any means, directly or indirectly, and their use in full or in part for terrorist financing purposes; – clarify that it is not necessary that funds were actually used to carry out terrorist acts or be linked to a specific terrorist act.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• Laundered property, where money laundering is the only offence being proceeded with, should be covered by the Estonian mandatory confiscation regime; • Confiscation of instrumentalities used or intended to be used should be mandatory and apply for all the designated offences; • instrumentalities used or intended to be used in the commission of a crime should be subject to value confiscation; • Estonia should introduce 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).
2.4 Freezing of funds used for terrorist financing (SR.III)	• Estonia should implement a national mechanism to give effect to requests for freezing assets and designations from other jurisdictions and to enable freezing funds of EU internals (citizens and residents). • A national de-listing process should be established as part of these measures. • The definition of "funds" (as taken from the EU Regulations) does not explicitly cover funds owned 'directly or indirectly' by designated persons or those controlled directly or indirectly by designated persons; this

	should be amended and be brought in compliance with the requirements of UNSCR 1267 and UNSCR 1373. • Apart from banks, no other financial institutions or DNFBP are aware of the procedures to be followed in order to implement the UNSC Resolutions. Thus, Estonian authorities should consider providing clear and practical guidance to financial institutions and other entities concerning their responsibilities under the freezing regime. • Estonia should introduce clear provisions regarding the procedure for unfreezing 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.
2.5 The Financial Intelligence Unit and its functions (R.26)	• Though the rating for Recommendation 26 is compliant it has to be noted that the only concern which has the abstract potential to become a problem for the FIU is that it does not have its own budget. Though this does not appear to be a problem at present, a separate budget would certainly strengthen its independence.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• No recommended action.
2.7 Cross Border Declaration & Disclosure	• Estonia should establish an effective regime to stop or restrain currency or bearer negotiable instruments when there is a suspicion of money laundering or terrorist financing at the border (criterion IX.3 a). • There are no provisions authorising Customs to seize cash simply in the case of a suspicion of money laundering or terrorist financing. In such a situation Customs could either inform the FIU which could immediately issue a precept that the money has to be frozen or Customs could initiate criminal proceedings and inform prosecutors to get an order from the investigative judge to seize the cash. When it comes to nighttimes, weekends and public holidays, this system is not fully operational. Estonia should establish an effective system which allows that there is at any time the possibility to seize cash when there is a suspicion of money laundering or terrorist financing (in the evaluators view the easiest way to do so would be to authorise Customs to seize cash in the case of a suspicion of money laundering or terrorist financing). • EC Regulation No. 1889/2005 and relevant national legislation do not cover the transfer of cash or bearer negotiable instruments between Estonia and another EU member state[68].

[68] see FN 28.

3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	• The obliged entities are allowed to rely on CDD information received *inter alia* from a credit institution who 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 the MLTFPA are in force. In the absence of further guidance on this issue, Estonian authorities should at least issue guidance regarding the question of which countries satisfactorily fulfil these requirements. • Concerning beneficial ownership, the law leaves some discretion in interpretation whether it also covers instances when a natural person acts for another natural person. Estonian authorities should make it clear in the law that beneficial ownership does not only refer to the first natural person in the chain but that it (also) covers natural persons who ultimately control other natural persons. • Concerning criterion 5.6, § 13 (1) 4) MLTFPA requires "*acquisition of information about a business relationship and the purpose of a transaction*". This provision could only indirectly be sanctioned (that failure to observe these requirements indicate a failure of the institution's internal controls). Estonia should introduce a direct sanctioning regime for this provision. • The Estonian approach to address "*high risk of money laundering or terrorist financing*" sets the level to apply enhanced CDD to a higher level than "*higher risk*" in terms of the Methodology. While "high risk" is at the upper end of a level of risk, "higher risk" refers only to a situation more risky than average. Furthermore, in the categories of § 19 MLTFPA non-resident customers and private banking do not appear as higher risk situations which would require enhanced CDD measures. Estonia should change the term of "high risk" to "higher risk" and consider adding non-resident customers and private banking to the categories which require enhanced CDD measures. Furthermore, the authorities should provide financial institutions with guidance on the existing categories of high risk. • § 18 MLTFPA allows for the application of simplified CDD measures in case of credit or financial institutions located in a contracting state of the European Economic Area or a third country, which in the country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision. At present, no guidance from the Estonian supervisory bodies exists specifying which third countries fulfil these criteria. Though simplified CDD is not mandatory under the Methodology but in case of applying

	such a system, the requirements of criterion 5.10 have to be met which is not the case in Estonia[69]. • The MLTFPA requires all obligated persons to have rules of procedure which ensure that the legal CDD requirements as set out in the MLTFPA are followed. Though not explicitly mentioned, the Estonian authorities are of the opinion that this language covers also all instances in which a business relationship begins prior to full CDD. The Minister of Finance is obliged to issue a decree specifying further requirements for such rules of procedure. Such guidance was not yet in existence at the time of the on-site visit and should be done as soon as possible[70]. • The MLTFPA should clearly require financial institutions to terminate a business relationship and notify the FIU in instances in which a request for additional documentation arising only from ongoing due diligence remains unfulfilled (part of criterion 5.16). • The exemption concerning politically exposed persons that "*a person who, by the date of entry into a transaction, has not performed any prominent public functions for at least a year, or the family members or close associates of such person are not considered a politically exposed person*" (§ 20 (1) MLTFPA) is not in line with the Methodology and should be removed. • Concerning effective implementation of Rec. 6, at least one of the smaller local banks did not, at the time of the on-site visit, 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). Estonian authorities should address this shortcoming by focused supervision on these issues and consider issuing guidance in this regard. • There should be a clear requirement in the law which obliges financial institution to understand the respondent bank's business. • Estonia should introduce a clear legal requirement for financial institutions to obtain approval from senior management before establishing new correspondent relationships. • In case of correspondent banking, financial institutions should be required to document not only the respective CDD responsibilities of each institution but the whole range of AML/CFT responsibilities (e.g. notification). • Estonia should introduce specific provisions in the law which address the risk of misuse of technological developments in money laundering or terrorist financing schemes.

[69] A list of equivalent third countries has been established in the meanwhile.

[70] The relevant Regulation of Minister of Finance was published in the State Gazette and became effective on April 11, 2008.

3.3 Third parties and introduced business (R.9)	• The obligated persons should be clearly required to ensure that timely reproduction of the necessary documentation from third parties is possible. • Concerning criterion 9.4, Estonian authorities should issue guidance 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. • Estonian authorities should clarify that also in the circumstances of § 14 (4) MLTFPA the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.
3.4 Financial institution secrecy or confidentiality (R.4)	• The provisions allowing the sharing of information between financial institutions where this is required by R. 7, R. 9 and SR VII should be revised: the language should be simplified to facilitate their application in practice and further guidance should be provided[71].
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• The MLTFPA (particularly § 63) needs to be amended that sanctions also apply to credit institutions and currency exchange bureaux when they breach the provisions of the said Regulation. • Measures need to be taken to ensure full awareness of by credit institutions and payment service providers of the requirements of Regulation (EC) No 1781/2006. Moreover, both the FSA and the FIU should elaborate an appropriate monitoring mechanism to ensure its proper implementation. • Neither the FSA nor the FIU have informed credit institutions and payment service providers of their obligations arising from Regulation (EC) No. 1781/2006. For the sake of a proper implementation of this EU Regulation (and consequently SR VII), it is necessary to raise awareness with its requirements concerning fund transfers. Furthermore on-site inspections and other off-site monitoring techniques should aim at ascertaining and evaluating implementation of this EU Regulation by credit institutions and payment service providers. The supervisory tools used by the FSA and the FIU should encompass the monitoring of compliance with the EU Regulation by both credit institutions and other financial business entities involved in money remittances.
3.6 Monitoring of transactions and relationships (R.11 & 21)	• Financial institutions should be required by law, regulation or other enforceable means to investigate the background and purpose of complex/unusual large transactions and to keep a record of the written findings which will be then accessible for competent authorities and auditors. • Estonia should introduce obligations in law or regulation or other enforceable means requiring financial institutions to

[71] This has already been done to a certain extent concerning countries which can be considered as equivalent to "*a contracting state of the European Economic Area*"; see FN 30.

	– give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations. – to examine and monitor such transactions, if they do not have an apparent economic or visible lawful purpose, and have written findings available to assist competent authorities and auditors. • Estonia should introduce specific provisions on application of counter- measures where a country continues not to apply or insufficiently applies the FATF Recommendations.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	• It should be clarified in the MLTFPA, that all attempted transactions have to be reported. • The definition of financing of terrorism as provided for by § 5 of the MLTFPA is linked with the definition as provided for by § 237^3 PC (the terrorist financing offence) and thus it has the same limitations as the terrorist financing offence and there is no reporting obligation in case of: – financing of an individual terrorist; – collecting of funds for the purpose of terrorist financing; – the provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist; – those conducts of Art 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions which are not covered in the Estonian terrorist offence (§ 237 PC). It is recommended that the reporting obligation will be broadened and brought into line with SR. IV. • Savings and loan associations as well as insurance sector sent no STRs so far. This shows that there is presumably either a lack of understanding or awareness of anti-money laundering obligations of these entities. The FIU should provide more guidance and training to these entities that they better understand their reporting obligations.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• The MLTFPA requires obligated persons to establish written rules of procedure for the application of due diligence measures, including assessment and management of the money laundering and terrorist financing risk, collection of information and storage of data, reporting of suspicious transactions as well as rules for checking adherence thereto. However, the MLTFPA follows a system that further details of these internal rules have to be established by the Minister of Finance; at the time of the on-site visit and two months subsequently, no such regulation came into force and effect[72]. • Financial institutions should be required to have guidance

[72] see FN 45.

	in their internal rules of procedure concerning the detection of unusual and suspicious transactions. • It is recommended that the legal requirements for regular training of employees extend to cover new developments in AML/CFT matters, including information on current ML/TF techniques, methods and trends. • Estonian authorities should introduce requirements imposing an obligation on credit and financial institutions to put in place screening procedures when hiring employees beyond the ones established regarding audit employees and members of management as per the relevant articles of CrIA, IAA, Investment Funds Act and the Securities Market Act. • The MLTFPA requirements for the implementation of AML/CFT measures by foreign branches and subsidiaries of credit and financial institutions should extend beyond customer due diligence and record keeping measures. • Credit and financial institutions should be required to pay particular attention to foreign branches and subsidiaries operating in countries which do not or insufficiently apply FATF Recommendations. • Provision should be made that where minimum requirements of the host and home countries differ, branches and subsidiaries in host countries should be required to apply the higher standard to extent that local (i.e. host country) laws and regulations permit.
3.9 Shell banks (R.18)	• The CrIA provides safeguards only concerning the establishment or continuous operation of shell banks which are operated from the European Economic Area (EEA). This restriction to the EEA should be removed and the CrIA should prohibit the establishment or continuous operation of shell banks regardless from which country they are operated (though it is clear that the Estonian FSA's practice and policy is not to license shell banks).
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	• Estonia should create legal provisions clearly stating that criminal records bar applicants from becoming beneficial owners of a significant or controlling interest in a financial institution. • Estonia should introduce an effective registration regime for financial institutions which are not supervised by the Estonian FSA pursuant to § 2 of the FSA Act[73]. • The Estonian FIU should be empowered to compel the off-site production of records from supervised entities for supervisory purposes absent a suspicion of money laundering or terrorist financing. • The FIU should be given the power to withdraw or suspend the registration of a financial institution falling under its supervision in case it fails to comply with AML/CFT requirements. • The indirect sanctioning system of the MLTFPA via precepts of the FSA for provisions of the MLTFPA which

[73] see FN 49.

	are not covered by a specific sanctioning provision of the MLTFPA itself (which is the case for a number of important CDD measures) does not amount to a dissuasive, proportionate and (for all circumstances) effective sanctioning regime. This indirect sanctioning system should be revised and replaced by a direct sanctioning regime providing sanctions in the MLTFPA for all relevant AML/CFT obligations. • In the light of the changes of the Estonian AML/CFT system because of coming into force of the new MLTFPA, the guidelines issued by the FSA seem already out of date. The FSA should update its own guidelines in the light of the requirements of the new MLFTPA[74]. • The FIU should issue guidelines explaining the legal requirements and preventive measures described therein to its supervised entities.
3.11 Money value transfer services (SR.VI)	• The FIU should establish a programme of on-site inspections of all payment service providers for checking compliance with their AML/CFT obligations.
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• As the relevant provisions of the MLTFPA apply both to financial institutions and DNFBP in the same way, the comments and observations made for credit and financial institutions under Recommendation 5, 6, 8, 9, 10 and 11 equally apply for DNFBP (with the exception of criterion 8.2 of the FATF Methodology). Thus the Recommendations there are also valid concerning DNFBP. • § 30 (6) MLTFPA applies only to financial institutions but not to DNFBP. The evaluators recommend that also DNFBP should be required through means of secondary legislation (i.e. Minister of Finance's regulation) to set up comprehensive internal control mechanisms for managing AML/CFT risks having regard to the sort, scope and complexity of their activities. • Though DNFBP are required under § 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 DNFBP should take to mitigate the risks for non-face-to face relationships and transactions. Estonian authorities should issue such guidance. • Casinos should be required not only to identify but also to verify the name of a client who engage in financial transactions equal or above the threshold given by criterion 12.1 of 3 000 USD/EUR; though not required by

[74] The FSA advised that its guidelines „Additional measures for prevention of money laundering and terrorist financing in credit and financial institutions" were adopted on 22 October 2008 and published on its website.

	the Methodology, it may be easier simply to amend the law by using the existing (lower) threshold of the MLTFPA which is 30 000 EEK (1 917.34 EUR).
4.2 Suspicious transaction reporting (R.16)	• The same deficiencies in the implementation of Recommendations 13, 15 and 21 in respect of financial institutions apply equally to DNFBP and the Recommendations there concerning financial institutions are also valid in the context of Recommendation 16. • Some DNFBP seem less aware of their obligations; e.g. lawyers, real estate dealers as well as accountants and auditors sent only a very small number of STR so far. Further outreach to these entities that they better understand their reporting obligations is necessary (though it has be noted that the Estonian FIU already provided a number of training seminars to these entities).
4.3 Regulation, supervision and monitoring (R.24-25)	• Beneficial owners and managers of casinos should be subject to fit and proper checks at the time of licensing, transfer of ownership or taking up employment. • The Law should require the registration of all persons providing trust and company services irrespective of whether or not the provision of such services constitute their primary professional or economic activity. • The Estonian Bar Association is responsible for the AML/CFT supervision of their members only. As it is not compulsory for a practising lawyer (independent legal professionals) to be a member of the Bar Association, they fall only under the supervision of the FIU which did not supervise them so far. The FIU should identify how many of such lawyers exist (e.g. by a mandatory registration requirement) and should supervise them (alternatively it could be made mandatory for these lawyers to become members of the Bar Association and that they are supervised by the Bar Association). • The Chamber of Notaries and the Estonian Bar Association should establish monitoring and supervisory mechanisms for checking compliance of their members with the AML/CFT obligations. • The FIU, the Chamber of Notaries and the Estonian Bar Association should prepare and issue guidelines assisting obligated entities in complying with their AML/CFT obligations.
4.4 Other non-financial businesses and professions (R.20)	• No recommended action.
5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• The control over the implementation of obligations of legal persons to submit updated information on ownership and control to the commercial register should be enhanced. • The requirements that limited liability companies maintain share registers and shareholder registers should be supervised. • The legal framework should be improved to ensure

	adequate, accurate and timely information on the beneficial ownership and control of legal persons.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	• No recommended action.
5.3 Non-profit organisations (SR.VIII)	• Estonian authorities should review the adequacy of relevant laws and regulations to prevent the abuse of NPOs for financing of terrorism. • Estonian authorities should conduct outreach or provide guidance on terrorist financing to the NPO sector. • Estonian authorities should supervise or monitor the NPO sector as envisaged by the Interpretative Note to SR VIII. • Mechanisms should be introduced for a prompt sharing of information among all relevant competent authorities when there is suspicion that a particular NPO is being exploited for terrorist financing purposes. • Estonia should establish special points of contact or distinguished procedures to respond to international requests for information regarding particular NPOs.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	• So far there seems to be no much formal co-ordination (in terms of formal agreements, sharing of information etc.) between the supervisory bodies. To improve the national cooperation in the AML/CFT area, supervisory authorities and, in particular, the FSA and the FIU should devise a formal agreement through a Memorandum of Understanding or other means for cooperation and coordination on supervisory matters.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• Estonia should implement all the provisions of the relevant international conventions it has ratified, particularly it should be made clear in the law or by way of guidance and training that the prosecution of money laundering does not require a prior or simultaneous conviction for the predicate offence. • It is recommended to amend the legal text criminalising terrorist acts and the provision criminalising terrorist financing in a way that they would be broad and detailed enough to cover, besides the financing of terrorist organisations, also all terrorist acts as required by the UN Conventions and the financing of individual terrorists. • These provisions should also: – clearly cover the various elements required by SR.II, in particular the collection of funds by any means, directly or indirectly, and their use in full or in part for terrorist financing purposes; – clarify that it is not necessary that funds were actually used to carry out terrorist acts or be linked to a specific terrorist act. • The requirements of the UN Conventions should be reviewed to ensure that Estonia is fully meeting all its obligations under them. Particularly Estonia should

	• introduce a national mechanism to freeze the funds of EU internals. • broaden the definition of funds (as it is provided for in the EU Regulations, which currently does not explicitly cover funds owned 'directly or indirectly' by designated persons or those controlled directly or indirectly by designated persons); • introduce a national procedure for the purpose of considering delisting requests..

6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• Arrangements for coordinating seizure and confiscation action with other countries should be established.
	• Consideration should be given
	  • to establishment of an asset forfeiture fund as well as
	  • to sharing of confiscated assets with other countries when confiscation is a result of coordinated law enforcement action.
	• More statistical data (e.g. nature of mutual assistance requests; whether it was granted or refused; the time required to handle them; type of predicate offences related to requests) is needed to show the effectiveness of the system.

6.4 Extradition (R.39, 37 & SR.V)	• Estonia should introduce specific 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. • More statistical data (e.g. the time required to handle requests) is needed to show the effectiveness of the system.
6.5 Other Forms of Co-operation (R.40 & SR.V)	• No recommended action.
7. Other Issues	

7.1 Resources and statistics (R. 30 & 32)	• The supervisory authorities should be provided with more manpower to carry out the supervisory tasks accorded to them by law, particularly regarding on-site supervision.
	• The Police should be provided with more resources (human and technical) to deal satisfactorily with economic crimes.
	• The resources (human and technical) of the TCB should be improved.
	• Estonia should keep in addition to the already maintained statistics also comprehensive statistics concerning the following issues:
	  – statistics in MLA concerning the predicate offences;
	  – statistics showing the time in which Estonia responded to extradition requests;
	  – statistics concerning the exchange of information of the FSA with foreign counterparts.

Table 3. Authorities' Response to the Evaluation (if necessary)

Relevant Sections and Paragraphs	Country Comments

V. COMPLIANCE WITH THE THIRD EU AML DIRECTIVE

Estonia is a member country of the European Union since 2004. It has implemented *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: "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* in 2008.

The following sections describe the major differences between the Directive and the relevant FATF 40 Recommendations plus 9 Special Recommendations. Following an analysis of the findings of the evaluation and conclusions on compliance and effectiveness, recommendations and comments are made as appropriate.

1.	**Self Laundering**
Directive	Self laundering is not explicitly addressed by the Directive but is not excluded from its scope.
FATF R. 1	Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.
Key elements	Is self laundering provided for?
Description and Analysis	Self laundering is not explicitly addressed in the Estonian money laundering offence (§ 394 Penal Code). During the first evaluation round the Estonian law did not allow for the prosecution of money laundering in cases where the person committed the predicate offence ("self-laundering"). Due to the different opinions expressed by Estonian authorities, the second round evaluators strongly advised that the issue of "own proceeds" is put beyond doubt in legislation. During the third round evaluation there was unanimity amongst prosecutors and judges that self-laundering is prosecutable in Estonia. Examples of the court practice were brought to the attention of evaluators which convincingly showed that there is no obstacle to prosecute persons who committed the predicate offence themselves. Persons charged with a predicate offence were charged also with money laundering offence when they have committed both the offences.
Conclusion	Estonia is in compliance with the Directive and FATF Rec. 1.
Recommendations and Comments	No recommendations.

2.	**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.
Description and Analysis	Estonia introduced criminal liability of legal persons in 2002. § 14 of the Penal Code (which is in the general part of the Penal Code) clarifies that criminal liability of legal persons is only possible in cases where this is specifically provided for by law: *(1) In the cases provided by law, a legal person shall be held responsible for an act which is committed by a body or senior official thereof in the interest of the legal person.* *(2) Prosecution of a legal person does not preclude prosecution of the natural person who committed the offence.* *(3) The provisions of this Act do not apply to the state, local governments or to legal persons in public law.* Criminal liability for legal persons for money laundering is provided for in § 394(3) and (4) PC: *(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.* All the terrorist (financing) offences are punishable by a pecuniary punishment or a compulsory dissolution if committed by a legal person (§§ 237(2), 237^1(2), 237^2 (2)) PC. These provisions formally fulfil the requirements of criterion 2.3 and II.4, but there are some deficiencies with regard to the requirements of Art. 37 of the Directive: § 14 PC requires as a prerequisite "*an act which is committed by a body or senior official thereof in the interest of the legal person*". It was understood that "*body*" refers to the general meeting, the management or supervisory board of a company. Thus, it can be concluded that the requirements of Art. 39 para 3 lit. b) and c) of the Directive are covered (which refer to "*an authority to take decisions on behalf of the legal person*" and "*an authority to exercise control within the legal person*"). However, this seems not to cover Art. 39 para 3 lit. a) of the Directive ("*a power of representation of the legal person*"). Furthermore § 14 PC requires that one can link the criminal act with a particular person (arg. ex "*committed by a body or senior official thereof*"). This requirement may be particularly difficult in the circumstances of Art. 39 para 4 of the Directive which requires that "*legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 3 has made possible the commission of the infringements referred to in paragraph 1 for the benefit of a legal person by a person under its authority*". Concerning the extension of corporate liability beyond the ML offence even to infringements which are based on national provisions adopted pursuant to the Directive, it has to be noted that chapter 7 of the MLTFPA provides for sanctions in case of violations of the obligations stipulated by the MLTFPA. Whenever relevant, these provisions also allow for sanctions of legal entities. However, the same difficulties as

	described in the report concerning the sanctioning of natural persons (i.e. not all obligations of the MLTFPA covered; the indirect sanctioning via precepts of the FIU is considered insufficient) applies.
Conclusion	Estonia has not fully implemented Art. 39 of the Directive.
Recommendations and Comments	To be fully in compliance with Art. 39 of the Directive, Estonia should: • revise its provisions of the Penal Code to make sanctions possible for legal entities in the situations envisaged by Art. 39 para 3 lit. a) and Art. 39 para 4 of the Directive. • amend the sanctioning regime of the MLTFPA to introduce a direct sanctioning regime (not via precepts of the FIU) for the obligated entities in case of all relevant obligations arising from the MLTFPA.

3.	**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.
Description and Analysis	§ 15 (2) MLTFPA requires credit and financial institutions "*to open an account and keep an account only in the name of the account holder*". As a consequence it can be concluded that it is prohibited to open anonymous accounts, accounts in fictitious names or numbered accounts. The private sector representatives met by the evaluators were well aware of this restriction.
Conclusion	Estonia is in compliance with both the Directive and the FATF Recommendations.
Recommendations and Comments	No recommendations.

4.	**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 15 000 EUR 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 of 15 000 EUR covered?
Description and Analysis	§ 12 (2) 2) of the MLFTPA requires CDD measures to be undertaken when carrying out occasional transactions amounting to 200 000 Estonian EEK (12 782.32 EUR) or more. This threshold is well below the requirement of the Directive.
Conclusion	Estonia is in compliance with the Directive.
Recommendations and Comments	No recommendations.

5.	**Beneficial Owner**
Art. 3(6) of the Directive	The definition of 'Beneficial Owner' establishes minimum criteria 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	The country follows which approach in its definition of "beneficial owner"?
Description and Analysis	§ 8 of the MLFTPA narrowly tracks the provisions of Art. 3 Nr. 6 of the Directive.
Conclusion	Estonia is in compliance with the Directive.
Recommendations and Comments	No recommendations.

6.	**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 Article 3(1) or (2) of the Directive. Article 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. (Methodology para 20; Glossary to the FATF 40 plus 9 Rec.)
Key elements	Does the country implement Article 4 of Commission Directive 2006/70/EC?
Description and Analysis	Estonia has decided not to make use of the option made available by Art. 2 (2) of the Directive.
Conclusion	Estonia has decided not to make use of the option made available by Art. 2 (2) of the Directive.
Recommendations and Comments	No recommendations.

7.	**Simplified CDD**
Art. 11 of the Directive	By way of derogation from the relevant Article 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 be subject to the full range of CDD measures yet, there are instances where reduced or simplified measures can be applied.
Key elements	Establish the implementation and application of Article 3 of Commission Directive 2006/70/EC which goes beyond criterion 5.9.
Description and Analysis	§ 17 of the MLFTPA defines simplified CDD measures, which can be applied if the conditions in § 18 of the MLFTPA are met. § 18 of the MLFTPA mirrors the requirements of Art. 3 of Commission Directive 2006/70/EC (with the exception of the requirement of non-anonymity, which follows from § 15 (2) of the MLFTPA). Some § 18 (5) of the MLFTPA allows the Ministry of Finance to enact a regulation which establishes further criteria for low risk. The Estonian Minister of Finance Regulation No 11 of 3 April 2008 does so and goes beyond criterion 5.9. Estonia allows, but does not require its financial institutions to apply

	simplified CDD vis-à-vis financial institutions from other EU member states.
Conclusion	Estonia is only partially in compliance with the Directive as it leaves it to the discretion to the financial institutions to apply simplified CDD measures vis-à-vis financial institutions from other EU member states (and does not make it mandatory).
Recommendations and Comments	Estonia should make simplified CDD mandatory vis-à-vis financial institutions from other member states (except for instances where this is explicitly prohibited by the Directive).

8.	**PEPs**
Art. 3 (8), 13 (4) of the Directive	The Directive defines PEPs broadly in line with FATF 40 (Article 3(8)). It applies enhanced CDD to PEPs residing in another Member State or third country (Article 13(4)). Directive 2006/70/EC provides a wider definition of PEPs (Article 2) and removal of PEPs after one year of ceasing to be entrusted with prominent public function (Article 2(4)).
FATF R. 6 and Glossary	Definition similar to Directive but applies to individuals entrusted with prominent public function in a foreign country.
Key elements	Did the country implement Article 2 of Commission Directive 2006/70/EC, in particular Article 2(4), and does it apply Article 13(4) of the Directive?
Description and Analysis	§ 20 (1) of the MLFTPA defines Politically Exposed Persons in the ambit of Estonian law and excludes persons who have ceased executing a prominent public function for more than a year. § 21 (1) of the MLFTPA makes such transactions subject to enhanced due diligence, while § 21 (2) of the MLFTPA additionally mandates the requirements of Art. 13 (4) of the Directive.
Conclusion	Estonia is in compliance with the Directive.
Recommendations and Comments	No recommendations.

9.	**Correspondent banking**
Art. 13 (3) of the Directive	Concerning correspondent banking, Article 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 the country apply Art. 13(3) of the Directive?
Description and Analysis	Estonian authorities explained that § 22 MLTFPA (correspondent banking) is the *lex specialis* to § 18 MLTFPA (simplified CDD). Thus it can be concluded, that § 22 of the MLFTPA limits the application of Enhanced Customer Due Diligence (ECDD) to correspondent banking relationships with institutions from non-EU member countries. § 18 MLTFPA allows to apply simplified CDD in relation to correspondent banking relationships with institutions from EEA member countries only.
Conclusion	Estonia applies Art. 13(3) a), b) and e) of the Directive to EEA member countries only. However, Estonia does not fully apply 13 (3) c) and d) of the Directive. There is no clear requirement to obtain senior management approval for establishing a correspondent banking relationship (matters of Agency aside) nor are the participating banks required to define the division of all AML/CFT related matters regarding the correspondent accounts.

Recommendations and Comments	Estonia should require 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 arrangement.

10.	**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 Article 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.
Description and Analysis	§ 15 (2) MLTFPA forbids financial institutions from providing services which can be used without prior identification and verification of the customer; this provision expressly requires such institutions "*to open an account and keep an account only in the name of the account holder*". § 15 (3) MLTFPA prohibits credit and financial institutions "*to enter into a contract or make a decision on opening an anonymous account or savings bank book*". Apart from that, the MLFTPA does not directly address the issue of products or transactions that might favour anonymity, except for outlawing non-face-to-face opening of accounts for financial institutions and mandating ECDD for other designated persons who established a business relationship without a face-to-face identification and verification. § 30 of the MLFTPA establishes requirements regarding certain transactions. It does not deal with products or technologies except in § 30 (4) 5), "means of communications", which establishes that institutions must have rules in place to deal with the use of telecommunications. § 30 (6) of the MLFTPA establishes the authority of the Minister of Finance to enact regulation in this regard. § 22 of the "Requirements for the Rules of Procedure established by credit and financial institutions and for their implementation and verification of compliance" (Minister of Finance Regulation No 10 of 3 April 2008) establishes that special attention should be paid to any "circumstances" that differ from what is known about a client's behavior, arguably including both products and transactions. Estonian financial institutions were required to bring their internal rules in line with these Rules of Procedure by 1 November 2008 at the latest. However, this does not specifically target products or transactions that target anonymity.
Conclusion	Estonia has not fully implemented Art. 13 (6) of the Directive.
Recommendations and Comments	Estonia should require its financial institutions and DNFBP to pay special attention to products and transactions which favour anonymity.

11.	**Third Party Reliance**
Art. 15 of the Directive	The Directive allows to rely for CDD performance on third parties from EU Member States or third countries under certain conditions and categorised by profession and qualified.
FATF R. 9	Allows reliance for CDD performance by third parties but does not

	categorise obliged entities and professions.
Key elements	What are the rules for procedures for reliance on third parties? Are their special conditions, categories etc.?
Description and Analysis	Estonian obligated persons are entitled to rely on "*information received by the obligated person in a format which 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 who 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*" (§ 14 (4) MLTFPA). To fully understand the scope of this provision it is necessary to look at the definition of "credit institution" as given by the MLTFPA: § 6 (1) of the MLTFPA refers for the definition of a *credit institution* to the definition as provided for by the Credit Institutions Act (CrIA) which defines in its § 3 a credit institution as "*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*". Furthermore, the MLTFPA understands credit institutions as the branch of a foreign credit institution registered in the Estonian commercial register (§ 6 (1) 2) MLTFPA).
Conclusion	In limiting the possible reliance on third parties to information of some further defined Credit Institutions ("*a credit institution registered in the Estonian commercial register or from a branch of a foreign credit institution or from a credit institution who 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*"), Estonia does not make use of all the possibilities as provided for by Art. 15 ff of the Directive: e.g. it is not allowed to rely on currency exchange offices and money transmissions offices under the circumstances described by Art. 15 (2) of the Directive. Thus it can be concluded that Estonia's approach is considerably more restrictive than allowed for by the Directive and that Estonia is in compliance with the Directive.
Recommendations and Comments	No recommendations.

12.	**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 1. do not apply concerning auditors and tax advisors; 2. apply for accountants when they prepare for or carry out transactions for their client concerning the following activities: • buying and selling of real estate; • managing of client money, securities or other assets; • management of bank, savings or securities accounts; • organisation of contributions for the creation, operation or management of companies; • creation, operation or management of legal persons or arrangements, and buying and selling of business entities (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 12.1d).
Description and Analysis	§ 3 (1) MLTFPA provides that it, inter-alia, applies to ▪ auditors and provides of accounting services (par.7) ▪ providers of accounting and tax advice services (par. 8) Chapter 2 of the MLTFPA (§§ 23-26) which deals with record keeping requirements applies to all obligated entities, including auditors, accountants and tax advisors.
Conclusion	The MLTFPA does not make any exemption to maintenance and preservation of records to auditors', tax advisors and accountants who are required to abide to the same obligations as all other entities covered by the law.
Recommendations and Comments	No recommendations.

13.	**High Value Deals**
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 15 000 EUR or more.
FATF R. 12	The application is limited to dealing in precious metals and precious stones.
Key elements	The scope of the Directive is broader.
Description and Analysis	The MLTFPA applies (§ 3 (1) (5)) to traders for the purpose of the Trading Act if a cash payment of no less than 200 000 EEK or an equal amount in another currency is made to the trader, regardless of whether the financial obligation is performed in a lump sum or in several related payments, unless otherwise provided by law. Estonian authorities advised that the phrase "unless otherwise provided by law" used in § 3 (1) (5) MLTFPA refers foremost to § 14 (2) MLTFPA which provides 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 shall be identified and verified as soon as the exceeding of the specified amount becomes evident.
Conclusion	The MLTFPA is in compliance with the Directive.
Recommendations and Comments	No recommendations.

14.	**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 2 000 EUR or more. This is not required if they are identified at entry.
FATF R. 16	The identity of customer has to be established and verified when they engage in financial transactions equal to or above 3 000 EUR.
Key elements	In which situations customers of casinos have to be identified? The Directive transaction threshold is lower.
Description and Analysis	§ 16 MLTFPA requires that organisers of games of chance (i.e. casinos and gambling houses) shall identify and verify the data specified in § 23(3) MLTFPA (i.e. residential address, profession or area of activity and information on PEP status) regarding all persons who pay or receive in a single or several related transactions an amount exceeding 30 000 EEK (around 2 000 MLTFPA) or the equivalent amount in another currency. In addition, § 23 MLTFPA requires obligated entities 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 MLTFPA is in compliance with the Directive.
Recommendations and Comments	No recommendations.

15. Reporting of accountants, auditors, tax advisors, notaries and other independent legal professionals via a self-regulatory body to the FIU	
Art. 23 (1) of the Directive	Option for accountants, auditors and tax advisors, and for notaries and other independent legal professionals to report through a self-regulatory body that 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	§ 32 MLTFPA requires all obligated persons to report directly to the FIU.
Conclusion	Estonia does not allow any of the obligated entities to report through a self-regulatory body; thus, Estonia does not make use of this option given by the EU Directive.
Recommendations and Comments	No recommendations.

16. Reporting obligations	
Art. 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 (Article 22). Obliged persons have to refrain from carrying out a transaction knowing or suspecting it to be related to money laundering or terrorist financing and to report to the FIU which can stop the transaction. If to refrain is impossible or could frustrate an investigation, the obliged persons are required to report to the FIU (Article 24).
FATF R. 13	Imposes 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? Is there a legal framework addressing Art 24 of the Directive?
Description and Analysis	§ 32 (1) MLTFPA describes the reporting obligations of financial institutions in case of a suspicion of money laundering or terrorist financing: "*If, upon performance of economic or professional activities or when carrying out an official act, an obligated person identifies an activity or circumstances which might be an indication to money laundering or terrorist financing or in case the obligated person has reason to suspect or knows that it is money laundering or terrorist financing, the obligated person shall immediately notify the Financial Intelligence Unit thereof.*" This language makes it clear, that the reporting obligation is triggered by a suspicion of money laundering and also when there is a suspicion of terrorist financing. According to § 32 (5) MLTFPA, "*an obligated person has the right to postpone a transaction or official act*" in the event a reporting obligation arises as described in § 32 (1) MLTFPA. The transaction has to be carried out, • if the postponement of the transaction may cause considerable harm, or • if it may impede catching the person who possibly committed

	money laundering or terrorist financing. In such an event the Financial Intelligence Unit shall be notified thereafter.
Conclusion	Estonia is in compliance with Article 22 of the Directive and FATF Recommendation 13. However, it has to be noted that Estonia is not fully in compliance with Article 24 of the Directive which requires a mandatory obligation for the obliged entities to refrain from carrying out a transaction knowing or suspecting it to be related to money laundering or terrorist financing. Instead § 32 (5) MLTFPA gives the obligated entities only the *right* to postpone a transaction. Moreover, the Directive provides only certain exceptions from this obligation (Art. 24: when it is impossible or it is likely to frustrate efforts to pursue the beneficiaries of a suspected ML or TF operation) but it does not allow to carry out a transaction "*if the postponement of the transaction may cause considerable harm*".
Recommendations and Comments	To fully implement Art. 24 of the Directive, Estonia should introduce a *mandatory* obligation for obligated entities to refrain from carrying out a transaction knowing or suspecting it to be related to money laundering or terrorist financing. Concerning exceptions from this obligation, Estonia should remove the possibility for obligated entities to carry out a transaction "*if the postponement of the transaction may cause considerable harm*".

17.	**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 the pendant to Art. 26 of the Directive)
Key elements	Is Art. 27 of the Directive implemented?
Description and Analysis	§ 35 MLTFPA provides a comprehensive protection of financial institutions, their directors, officers and employees concerning civil (arg. e "*not [...] be liable for damage*") and criminal (arg. e "*not deemed infringement of the confidentiality requirement provided by law or contract*") liability because of breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. However, this covers only the requirements of FATF Rec. 14 but Art. 27 of the Directive goes beyond as it provides for an obligation for Member States to protect employees of reporting institutions from being exposed to *threats* or *hostile actions*. Estonian authorities could refer in this regard only to general provisions of the Penal Code: • § 120 - Threat („*A threat to kill, cause health damage or cause significant damage to or destroy property, if there is reason to fear the realisation of such threat, is punishable by a pecuniary punishment or up to one year of imprisonment.*") • § 121 – Physical Abuse („*Causing damage to the health of another person, or beating, battery or other physical abuse which causes pain, is punishable by a pecuniary punishment or up to 3 years' imprisonment.*") However, if threats or hostile actions do not fulfil the requirements of the above mentioned criminal offences (which will usually be the case in

	situations when there are only "hostile actions"), no further protection applies as neither the MLTFPA nor the sectoral laws contain such specific provisions.
Conclusion	Estonia has not implemented Art. 27 of the Directive.
Recommendations and Comments	Estonia should take appropriate measures in order to protect employees of the institutions or persons covered by the Directive who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to *threats* or *hostile action*.

18.	**Tipping off (2)**
Art. 28 of the Directive	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 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 which circumstances apply tipping off obligations? Are there exceptions?
Description and Analysis	§ 34 of the MLTFPA establishes the confidentiality requirements of persons with a notification obligation: "*An obligated person, a structural unit and 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 or initiation of criminal proceedings under § 40 or 41. 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 after fulfilment of the precept made by the Financial Intelligence Unit.*" This provision covers in a comprehensive way the requirements of criterion 14.2. Concerning the coverage of Art. 28 of the Directive one difference has to be noted: while the "tipping off" obligation in Estonia is also extended in cases of "*initiation of criminal proceedings under § 40 or 41*", the Directive requires more as it refers only to ML or TF *investigations*. As there may be ML/TF investigations which are prior to criminal proceedings, some situations may not be covered.
Conclusion	Estonia has not fully implemented Art. 28 of the Directive.
Recommendations and Comments	To fully implement Art. 28 of the Directive, Estonia should extend the "tipping off"-requirements to situations of ML/TF investigations (Estonia may consider to do so by amending § 34 MLTFPA and replacing "*initiation of criminal proceedings under § 40 or 41*" with the term "*money laundering or terrorist financing investigations*".

19.	**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 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 Article 34(2) of the EU Directive.
Key elements	Is there an obligation as provided for by Art. 34 (2) of the Directive?
Description and	§ 13(2) MLTFPA requires credit and financial institutions to apply the

Analysis	due diligence measures specified in Division 1 of the Law 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 this Act. It is noted that the MLTFPA does not provide a definition of "a third country" and is, therefore, uncertain as to whether it goes broader than the EU Directive to include in the "third countries" the EEA countries as well.
Conclusion	The MLTFPA is in compliance with the Directive. though it may be desirable to clarify the term "third countries".
Recommendations and Comments	Though the MLTFPA is in compliance with the Directive, it may be desirable to clarify the term "third countries".

20.	**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 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 are financial institutions obliged to do in such circumstances?
Description and Analysis	§ 13(2) 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	-

21.	**Supervisory Bodies**
Art. 25 (1) of the Directive	The Directive imposes obligation on supervisory bodies to inform 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 Dir. implemented?
Description and Analysis	§ 49 MLTFPA imposes an obligation on supervisory authorities (other than the FIU) to notify the FIU whenever in the course of their supervisory activities detect a situation the elements of which refer to a justified suspicion of money laundering or terrorist financing. It is unclear what is meant by the words "justified suspicion" which triggers, as per the Law, a reporting obligation by supervisory authorities. It is noted that § 32(1) MLTFPA which deals with the notification duty of obligated entities speaks about "indication of money laundering or terrorist financing" and "reason to suspect or know that is money laundering or terrorist financing".
Conclusion	The MLTFPA restricts the reporting obligation of supervisory authorities to cases of "justified suspicion" only and, thus, does not require reporting to the FIU of all facts discovered that could relate to money laundering or terrorist financing as envisaged by the EU Directive.
Recommendations and Comments	The MLTFPA should be suitability amended to bring its provisions in line with Article 25(1) of the EU Directive.

22.	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 circumstances can be broadly inferred from Recommendations 23 and 26 – 32.
Key elements	Are credit and financial institutions required to have such systems in place and effectively applied?
Description and Analysis	§ 26 MLTFPA requires credit and financial institutions to "*preserve the original copies or copies of the documents specified in §§ 23 and 24, which serve as the basis for identification and verification of a person, and the documents serving as the basis for establishment of a business relationship no less than five years after termination of the business relationship.*" § 26 (3) of the MLFTPA also states that an "*obligated person shall preserve the documents and data specified in sections (1) and (2) in a manner which allows for an exhaustive and immediate reply to enquiries from the Financial Intelligence Unit or other investigative bodies*"[75]. The few larger international banks, as a matter of common practice, use electronic systems in this regard. The FIU advised that whatever systems were used in the small local banks, there had never been problems with slow responses. The obligations stipulated by § 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 Financial Intelligence Unit 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	-

23.	Extension to other professions and undertakings
Art. 4 of the Directive	The Directive imposes a *mandatory* obligation on Member States to ensure extension of its provisions to other professionals and undertakings whose activities are likely to be used for money laundering or terrorist financing.
FATF R. 20	Requires countries only to consider such extensions.
Key elements	Has the country effectively implemented Art. 4 of the Directive? Is this based on a risk assessment?
Description and Analysis	§ 3 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 Article 2(1) of the EU Directive as well as pawnbrokers. The latter is the only class of professionals covered by the MLTFPA which goes beyond the EU Directive's requirements. Estonian authorities advised that these entities were included as they appear "in the Glossary of the FATF Recommendations as an area of activity of a higher risk of money laundering." However, it seems that Estonian authorities did not

[75] Emphasis added.

	undertake a risk assessment establishing which other professionals and undertakings could likely be used for money laundering or terrorist financing.
Conclusion	Without a thorough risk assessment of Estonian authorities establishing which other professionals and undertakings could likely be used for money laundering or terrorist financing, it is impossible to say whether Art. 4 of the Directive has been effectively implemented.
Recommendations and Comments	To be fully in compliance with Art. 4 of the Directive, Estonia should undertake a risk assessment establishing which other professionals and undertakings could likely be used for money laundering or terrorist financing.

24.	**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 does the country address the issue of equivalent third countries?
Description and Analysis	Neither the MLFTPA nor the regulations based on it define equivalent third countries[76].
Conclusion	-
Recommendations and Comments	-

[76] The list of equivalent third countries was adopted in the EU Committee on the Prevention of Money Laundering and Terrorist Financing on 18 April 2008 (*Common Understanding Between Member States on Third Country Equivalence Under the Anti-Money Laundering Directive (Directive 2005/60/EC*)). The list and Estonian translation has been made available on the web-pages of the Ministry of Finance, FSA and FIU.

VI. LIST OF ANNEXES

Annex 1. List of acronyms used

CCP	Code of Criminal Procedure
CDD	Customer Due Diligence
CETS	Council of Europe Treaty Series
CFT	Combating the financing of terrorism
CrIA	Credit Institutions Act
CTR	Cash Transaction Report(s)
DNFBP	Designated Non-Financial Businesses and Professions
EAW	European Arrest Warrant
EBA	Estonian Banking Association
ECRSA	Estonian Central Register of Securities Act
EEK	Currency code for "Estonian Kroon"
ETS	European Treaty Series [since 1 January 2004: CETS = Council of Europe Treaty Series]
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FN	Footnote
FSA	Financial Supervision Authority
GPCCA	General Part of the Civil Code Act
IN	Interpretative Note
IAA	Insurance Activities Act
ISA	International Sanctions Act
IT	Information Technology
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MoJ	Ministry of Justice
MOU	Memorandum of Understanding
MLTFPA	Money Laundering and Terrorist Financing Prevention Act
NCCT	Non-cooperative countries and territories
NPA	Non-profit associations
NPAA	Non-profit Associations Act
NPO	Non-profit organisation
PC	Penal Code
PEP	Politically Exposed Person(s)
SEPPA	Substitutive Enforcement and Penalty Payment Act
SPB	Security Police Board
SRO	Self-Regulatory Organisation
STR	Suspicious transaction report(s)

SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCB	Tax and Customs Board

Annex 2. Details of all bodies met on the on-site mission – Ministries, other government authorities or bodies, private sector representatives and others

Ministry of Finance

Ministry of Justice

Prosecutor's Office General

Financial Supervision Authority

Bank of Estonia

Ministry of Foreign Affairs

Estonian Central Register of Securities + Tallinn Stock Exchange (OMX)

Police Board

Law enforcement agencies including police and other relevant investigative bodies

Organization on drug agencies, intelligence or security services, IT crime, etc.

Estonian Gambling Operator Association(EGOA)

Real Estate Association (REA)

Representative of the Currency Exchange Bureaus

Casino Supervisory body

Bar association (BA)

Chamber of Notaries (CoN)

Estonian Board of Auditors (EBA)

Tax and Custom Authority

Supreme Court

Ministry of Economic Affairs and Communications

Annex 3. Money Laundering and Terrorist Financing Prevention Act

Chapter 1
GENERAL PROVISIONS
Division 1 Purpose and Scope of Application of Act

§ 1. Purpose of Act
The purpose of this Act is to prevent the use of the financial system and economic space of the Republic of Estonia for money laundering and terrorist financing.

§ 2. Scope of application of Act
(1) This Act regulates:
1) the application of due diligence measures by obligated persons for the prevention of money laundering and terrorist financing;
2) monitoring the implementation of the Act by obligated persons;
3) the bases of activities of the Financial Intelligence Unit;
4) the liability of obligated persons for non-compliance with the requirements of this Act.
(2) The provisions of the Administrative Procedure Act apply to administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

§ 3. Application of Act
(1) This Act applies to the economic and professional activities and professional practice of the following persons:
1) credit institutions;
2) financial institutions;
3) organisers of games of chance;
4) persons who carry out or intermediate immovable property transactions;
5) traders for the purposes of the Trading Act, if a cash payment of no less than 200,000 kroons 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;
6) pawnbrokers;
7) auditors and providers of accounting services;
8 providers of advisory services in the areas of accounting and taxation;
9) providers of trust and company services.
(2) This Act applies to notaries public, attorneys, bailiffs, trustees in bankruptcy, interim trustees in bankruptcy and providers of other legal services if they act in the name and on the account of a customer in financial or immovable property transactions. This Act also applies to the specified persons if they instruct the planning or execution of a transaction or perform an official act, which concerns:
1) the purchase or sale of immovables, enterprises or companies;
2) the management of the customer's money, securities or other property;
3) the opening or managing of bank or securities accounts;
4) the acquisition of funds necessary for the foundation, operation or management of companies;
5) the foundation, operation or management of trusts, companies or other similar entities.
(3) For the purposes of this Act "cash" means cash within the meaning of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community. The provisions regarding cash are also applicable to performance of financial obligations using a precious metal, which is measured in bars or other units.

Division 2 Definitions

§ 4. Money laundering
(1) Money laundering means:

1) concealment or maintenance of the confidentiality of the true nature, origin, location, manner of disposal, relocation or right of ownership or other rights of property acquired as a result of a criminal activity or property acquired 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 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 is also 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.

§ 5. Terrorist financing
Terrorist financing means financing terrorism crimes as provided in § 273^3 of the Penal Code.

§ 6. Credit and financial institutions
(1) For the purposes of this Act, a credit institution is:
1) a credit institution within the meaning of the Credit Institutions Act;
2) the branch of a foreign credit institution registered in the Estonian commercial register.
(2) For the purposes of this Act, a financial institution is:
1) a financial institution within the meaning of the Credit Institutions Act;
2) providers of currency exchange services;
3) providers of payment services;
4) providers of services of alternative means of payment;
5) an insurer engaged in life assurance within the meaning of the Insurance Activities Act (hereinafter insurer);
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) an electronic money institution within the meaning of the Electronic Money Institutions Act;
11) a branch of a foreign service provider registered in the Estonian commercial register providing a service specified in clauses 1)-10).
(3) For the purposes of this Act, a currency exchange service is the exchange of the official currency of one country for the official currency of another country within the economic or professional activities of an undertaking.
(4) A provider of services of alternative means of payment is a person who in its economic or professional activities and through a communications, transfer or clearing system purchases, sells or intermediates 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 Credit Institutions Act.

§ 7. Trust and company service provider
A provider of trust and company services is a natural or legal person whose primary economic or professional activity lies in providing a third party with at least one of the 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 the arrangement of assumption of this position by another person;
3) enabling the 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 arrangement 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 the arrangement of representation of a shareholder by another person, except in the case of companies whose securities have been listed in a regulated securities market and with respect to whom disclosure requirements complying with European legislation or equal international standards are applied.

§ 8. Beneficial owner

(1) A beneficial owner is a natural person who, taking advantage of his or her influence, exercises final control and in whose interests or favour or on whose account a transaction or act is performed. A beneficial owner is a natural person who ultimately owns the company or exercises ultimate control over the management of a company:

1) by owning over 25 percent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares;

2) by otherwise exercising control over the 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, or who exercises significant 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 the 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 in whose interests mainly the legal person, civil law partnership or another contractual legal arrangement is set up or operates.

(4) Clause (1) 1) does not apply to companies whose securities have been listed in a regulated stock exchange.

§ 9. Property

For the purposes of this Act, property is any object as well as the right of ownership of such an object or documents certifying the rights related to the object, including electronic documents and the benefit received from the object.

§ 10. Obligated person

An obligated person is a person specified in subsection 3 (1) or (2).

§ 11. Business relationship

(1) For the purposes of this Act, a business relationship is a relationship of an obligated person, which:

1) arises upon conclusion of long-term contract in economic or professional activities;

2) is not based on a long-term contract, but which may reasonably be expected to last for a certain term and during which an obligated person repeatedly enters into separate transactions in the framework of its economic or professional activities or professional practice.

(2) For the purposes of this Act, a customer is a person who has a business relationship with the obligated person.

Chapter 2
DUE DILIGENCE
Division 1 Due Diligence Measures

§ 12. Obligation to apply due diligence measures

(1) In economic or professional activities or professional practice an obligated person shall pay special attention to the activities of a person or customer participating in a transaction or official act and to circumstances which refer to money laundering or terrorist financing or to the probable connection with money laundering or terrorist financing, including to complex, high value and unusual transactions which do not have reasonable economic purpose.

(2) An obligated person shall apply due diligence measures at least:

1) upon establishment of a business relationship;

2) upon concluding or intermediating transactions on an occasional basis, while the value of the transaction exceeds 200,000 kroons or an equal amount in another currency, regardless of whether the financial obligation is performed in a lump-sum or in several related payments, unless otherwise provided by law;
3) upon suspicion of money laundering or terrorist financing, regardless of any avowals, exemptions or limits specified by law;
4) in the event of insufficiency or suspicion of the correctness of the documents or data gathered earlier in the course of identification and verification of a person or updating the respective data.

§ 13. Due diligence measures
(1) To perform the obligation provided in § 12 an obligated person applies in economic or professional activities or professional practice the following due diligence measures:
1) identification of a customer or a person participating in a transaction on the basis of the documents and data submitted by him or her and verification of the submitted information on the basis of the information acquired from a reliable and independent source;
2) identification and verification of the representative of a natural or a legal person and the identification and verification of the right of representation;
3) identification of the beneficial owner, including gathering information on the ownership and control structure of a legal person, trust, civil law partnership or other contractual legal arrangement on the basis of the information provided in pre-contractual negotiations or obtained from another reliable and independent source;
4) acquisition of information about the purpose and nature of the business relationship and transaction;
5) constant monitoring of a business relationship, including monitoring transactions concluded during the business relationship, regular verification of the data used for identification, updating relevant documents, data and information and, if necessary, identification of the source and origin of funds used in the transaction.
(2) Credit and financial institutions apply the due diligence measures in an agency, branch or 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 this Act. If the legislation of the third country does not allow application of equal measures, the credit or financial institution shall immediately notify the competent supervisory authority thereof and apply additional measures for prevention of money laundering or terrorist financing risks.

§ 14. General application of due diligence measures
(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.
(2) 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 shall be identified and verified as soon as the exceeding of the amount provided by clause 12 (2) 2) becomes evident.
(3) An obligated person shall apply all due diligence measures specified in subsection 13 (1), but may choose the appropriate scope of application of the due diligence measures depending on the nature of the business relationship or transaction or the risk level of the person or customer participating in the transaction or official act.
(4) Upon application of the due diligence measures specified in clauses 13 (1) 1)-3), an obligated person has the right to rely on the information received in a format which can be reproduced in writing from a credit institution or from a branch of a foreign credit institution registered in the Estonian commercial register or from a credit institution who 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.

§ 15. Specifications for the application of due diligence measures by credit and financial institutions
(1) Upon opening an account in a credit or financial institution or upon the first use of another service by a person with whom the credit or financial institution has no business relationship, the person

participating in the transaction or using the service shall be identified while being present at the same place with the person or his or her representative.
(2) A credit and financial institution must not provide services which can be used without identification or verification of the person participating in the transaction. A credit and financial institution is obligated to open and keep the account only in the name of the account holder.
(3) For a credit and a financial institution it is prohibited to enter into a contract or make a decision on opening an anonymous account or savings bank book. A transaction in violation with the prohibition is void.
(4) A credit and financial institution may exceptionally, at the request of the person participating in the transaction, open an account before full application of due diligence measures on the condition that the account is debited after full application of the due diligence measures specified in clauses 13 (1) 1)-4) and the first payment relating to the transaction is made through the same person's account which has been opened in a credit institution that operates in a contracting state of the European Economic Area or in a state where requirements equal to those provided for in this Act are in force.
(5) An insurer and an insurance broker may verify the identity of a beneficiary under a life assurance contract after establishment of the 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.
(6) Upon the performance of currency exchange services the provider of currency exchange services is obliged to identify and verify all persons participating in the transaction if the amounts exchanged in cash either in a single transaction or related transactions exceed 100,000 kroons or an equal amount in another currency.
(7) Upon provision or intermediation of a payment service, the provider of payment services is obliged to identify all customers who initiate or receive money transfers through the provider of payment services.
(8) A provider of services of alternative means of payment is obliged to:
1) identify each customer upon establishment of a business relationship and entering into a transaction while being present at the same place with the customer, if the value of the transactions of the customer exceeds 15,000 kroons 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 and the represented data.

§ 16. Specifications for the application of due diligence measures by other obligated persons
(1) An organiser of games of chance is obligated to 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 30,000 kroons or an equal amount in another currency.
(2) Identification of persons and application of other due diligence measures by a notary public shall be based on the Notarisation Act and the Notaries Act with the specifications provided by this Act.
(3) A notary public, bailiff, trustee in bankruptcy, auditor, attorney and another legal service provider may identify and verify the identity of a customer, the 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 financing money laundering or terrorist financing is low.
(4) In the case specified in subsection (3) the application of due diligence measures must be completed as soon as possible after the first contact and before performing any binding acts.

§ 17. Application of simplified due diligence measures
(1) Upon fulfilment of the conditions provided for in § 18, an obligated person may, in the case of a low risk of money laundering or terrorist financing, apply the due diligence measures specified in subsection 13 (1) pursuant to a simplified procedure and determine the appropriate scope of the measures depending on the nature of the business relationship or the risk level of the transaction and of the person or the customer participating in the transaction or in the official act.
(2) Simplified due diligence measures are not applied if there is a suspicion of money laundering or terrorist financing.

(3) An obligated person is obliged to gather sufficient amount of information to identify whether a transaction performed in economic or professional activities and the person or customer participating in a transaction or an official act are in compliance with the requirements provided by subsections 18 (1)-(4).

§ 18. Conditions of the application of simplified due diligence measures

(1) An obligated person may apply simplified due diligence measures if a person or a customer participating in an official act or a transaction concluded in economic or professional activities is:
1) a legal person governed by public law founded in Estonia;
2) a governmental authority or another authority performing public functions in Estonia or in another contracting state of the European Economic Area;
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 provided by this Act and whose securities are traded in a regulated securities market in one or several contracting states of the European Economic Area;
5) a credit or financial institution, a credit or financial institution located in a contracting state of the European Economic Area or a third country, which in the country of location is subject to requirements equal to those provided by this Act and the performance of which is subject to state supervision.
(2) An obligated person may apply the simplified due diligence measures with regard to the beneficial owners of an official account opened by a notary public or bailiff of a contracting state of the European Economic Area or a 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 bailiff has and preserves information about the identity of the beneficial owner.
(3) An insurer and an insurance broker may apply simplified due diligence measures if:
1) a life assurance contract is made whereby the annual assurance premium does not exceed 15,000 kroons or a single premium does not exceed 35,000 kroons;
2) a pension insurance contract which does not provide for the right of withdrawal or cancellation and which cannot be used as loan collateral is concluded;
3) a transaction is concluded 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 the participant in the scheme.
(4) An obligated person may apply simplified due diligence measures in a transaction if:
1) a written long-term contract has been concluded with a customer;
2) a payment is made through the account of a person or customer participating in a transaction, which has been opened in a credit institution or the 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 by this Act are in force;
3) 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 200,000 kroons.
(5) The criteria of the low risk of money laundering or terrorist financing with regard to certain persons or transactions in the case of which simplified due diligence measures may be applied shall be established by a regulation of the Minister of Finance.

§ 19. Application of enhanced due diligence measures

(1) If the nature of a situation involves a high risk of money laundering or terrorist financing, an obligated person shall apply enhanced due diligence measures.
(2) An obligated person must apply the enhanced due diligence measures specified in subsection (3) if:

1) a person or customer participating in a transaction or official act performed in economic or professional activities has been identified and verified without being present at the same place as the person or customer;
2) upon identification or verification of a person suspicion arises of the truthfulness of the data or authenticity of the documents submitted or of the identification of the beneficial owner or the beneficial owners;
3) a person or customer participating in a transaction or an official act performed in economic or professional activities is a person specified in subsection 21 (1).
(3) In the events specified in subsections (1) and (2) an obligated person shall apply at least one of the following enhanced due diligence measures:
1) identification and verification of a person on the basis of additional documents, data or information, which originate from a reliable and independent source or from a credit institution or the branch of a credit institution registered in the Estonian commercial register or 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 this 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 the 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.
(4) In the events specified in subsections (1) and (2) an obligated person shall apply the due diligence measures specified in clause 13 (1) 5) more frequently than usually.
(5) An obligated person is responsible for proper application of the due diligence measures.

§ 20. Politically exposed person
(1) A politically exposed person is a natural person who performs or has performed prominent public functions, also the family members and close associates of such a person. A person who, by the date of entry into a transaction, has not performed any prominent public functions for at least a year, or the family members or close associates of such a person are not considered politically exposed persons.
(2) For the purposes of this Act, a person performing prominent public functions is:
1) a head of state, head of government, minister, and deputy or assistant minister;
2) a member of parliament;
3) a justice of a supreme, constitutional or another court of which the judgments can be appealed only in exceptional circumstances;
4) a member of the supervisory board of a state audit institution or the central bank;
5) an ambassador, chargé d'affaires and senior officer of the Defence Forces;
6) a member of a management, supervisory or administrative body of a state-owned company.
(3) The provisions of clauses (2) 1)-5) include positions of the European Union and other international organisations.
(4) A family member of a person performing prominent public functions is:
1) his or her spouse;
2) a partner equal to a spouse under the law of the person’s country of residence or a person who as of the date of entry into the transaction had shared the household with the person for no less than a year;
3) his or her children and their spouses or partners within the meaning of clause 2);
4) his or her parent.
(5) A close associate of a person performing prominent public functions is:
1) a natural person who has a close business relationship with a person performing prominent public functions or with whom a person performing prominent public functions is the joint beneficial owner of a legal person or contractual legal arrangement;

2) a person who as a beneficial owner has full ownership of a legal person or contractual legal arrangement, which is known to have been set up for the benefit of the person performing prominent public functions.

§ 21. Transactions with politically exposed persons of other Member States and third countries

(1) Upon establishment of a business relationship or entry into a transaction or performance of an official act with a politically exposed person of a contracting state of the European Economic Area or a third country or his or her family member or close associate, an obligated person shall apply the enhanced due diligence measures provided for in § 19.

(2) In the event specified in subsection (1), an obligated person shall also implement the following requirements:

1) apply appropriate risk-based internal procedures for making a decision on establishment of a business relationship or on conclusion of a transaction;

2) the management board of the obligated person or a person or persons authorised by the management board shall decide on establishment of business relationships;

3) upon establishment of a business relationship or upon the conclusion of a transaction, appropriate measures for identification of the origin of the money or other property used are taken;

4) continuously apply the due diligence measures specified in clause 13 (1) 5).

§ 22. Correspondent relationships of credit and financial institutions

(1) A credit and financial institution shall apply 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:

1) the trustworthiness and reputation of the credit institution of the third country and the effectiveness of the supervision exercised over the credit institution on the basis of the information accessible to the public;

2) the control systems of the credit institution of the third country for prevention of money laundering and terrorist financing.

(2) The contract serving as the basis for opening a correspondent account or the rules of procedure of the credit institution must 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:

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;

2) upon the submission of the data acquired in the course of identification of the customer on an enquiry and verification of the submitted information.

(3) A credit and financial institution is prohibited to open and hold a correspondent account in a credit institution, which meets at least one of the following conditions:

1) the actual place of management or business of the credit institution is located outside its receiving state and the credit institution is not part of the consolidation group or group of undertakings of a credit or financial institution which is subject to sufficient supervision;

2) an account for a credit institution corresponding to the characteristics specified in clause 1) has been opened in the credit institution;

3) there are deficiencies in the trustworthiness of the executives of the credit institution and in the assessment of the measures for the prevention of money laundering and terrorist financing according to respective international standards or the circumstances provided for in this section, which are used as a basis for assessment.

(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) is void.

(5) Subsections (3) and (4) are applied to correspondent relationships with an institution and undertaking whose principal and permanent activity lies in concluding transactions similar to the transactions provided for in subsection 6 (1) of the Credit Institutions Act.

Division 2 Collection and Preservation of Data

§ 23. Documents and data serving as basis of identification of natural persons

(1) An obligated person shall identify a natural person and verify the person on the basis of a document specified in subsection 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 subsection 4 (1) of the Identity Documents Act. In addition to an identity document, the representative of a person participating in a transaction shall submit a document certifying the right of representation in the required format.

(2) A copy shall be made of the page of the identity document submitted for identification which contains the personal data and a photograph. In addition, upon identification and verification of the persons specified in subsection (1), an obligated person shall register the following personal data:

1) the name and the representative's name;

2) the personal identification code or, in case of absence of a personal identification code, the date and place of birth;

3) the name and number of the document used for identification and verification, its date of issue and the name of the agency that issued the document;

4) the name of the document, used for identification and verification of the right of representation, its date of issue and the name of the issuer.

(3) On the basis of the information received from the person specified in subsection (1), an obligated person shall register his or her address of the place of residence and the profession or the area of activity. If a person or customer participating in a transaction concluded in economic or professional activities is a natural person of a contracting state of the European Economic Area or a third country, the obligated person shall register the information whether the person performs or has performed any prominent public functions or is a close associate or a family member of a person performing prominent public functions.

(4) At the request of an obligated person, a person or customer participating in a transaction performed in economic or professional activities shall submit documents and provide relevant information required for the application of the due diligence measures specified in subsection 13 (1).

(5) A representative of a legal person of a foreign country 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 replacing legalisation (apostille), unless otherwise prescribed by an international agreement.

(6) If the document or data specified in subsections (1) and (3) cannot be received, documents certified or authenticated by a notary public or authenticated officially may be used for verification of the identity of a person.

(7) A person or customer participating in an economic or professional transaction or an official act shall, at the request of an obligated person, confirm the authenticity of the submitted information and documents received from the application of the due diligence measures by his or her signature.

§ 24. Documents and data serving as basis of identification of legal persons

(1) An obligated person shall identify a legal person and its passive legal capacity and verify the obtained information. A legal person registered in Estonia or a branch of a foreign company registered in Estonia shall be identified on the basis of an extract of a registry card of the relevant register and a foreign legal person is 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.

(2) The document submitted to enable identification shall at least contain:

1) the business name or the 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 that issued the document.

(3) On the basis of the documents specified in subsection (1) 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 replacing it and their authorisation in representing the legal person;
2) the area of activity of the legal person;
3) means of communications´ numbers;
4) the data of the beneficial owners of the legal person.
(4) If an obligated person has information that a politically exposed person of another contracting state of the European Economic Area or third country may be related to a person or customer participating in a transaction entered into in economic or professional activities, the circumstances specified in subsection 23 (3) shall be registered on the basis of the information received from the representative of the legal person in addition to the data specified in subsection (3).
(5) An extract of the registry card does not have to be submitted if an obligated person has access to the data of the commercial register and the register of non-profit associations and foundations or the corresponding register of a foreign country via the computer network.
(6) If the document or data specified in subsections (1) and (3) 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.

§ 25. Registration of the data of the transaction
(1) Upon identification and verification of a person, an obligated person shall register the date or period of time of the conclusion of the transaction and a description of the content of the transaction.
(2) A credit and financial institution shall register the following data about a transaction:
1) upon opening an account, the account type, account number, currency and significant characteristics of the securities or other property;
2) upon the deposit of property, the deposit number and the market value of the property on the date of depositing or a detailed description of the property if the market value of the property cannot be determined;
3) upon renting or using a safe deposit box or a safe in a bank, the number of the safe deposit box or safe;
4) upon making a payment to the customer relating to shares, bonds or other securities, the type of the securities, the monetary value of the transaction, the currency and the account number;
5) upon the conclusion of a life assurance contract, the account number debited to the extent of the first premium;
6) upon making a disbursement under a life assurance contract, the account number that was credited to the extent of the amount of disbursement;
7) in the case of the payment mediation service, the data, the communication of which is compulsory under Regulation (EC) No. 1781/2006 of the European Parliament and Council, of the payer accompanying the transfers of funds;
8) in the case of providing services of alternative means of payment, the name of the payer and recipient, the personal identification code, and upon absence thereof, the date and place of birth or a unique feature on the basis of which the payer can be identified;
9) in the case of another transaction, the transaction amount, the currency and the account number.

§ 26. Preservation of data
(1) An obligated person shall preserve the original documents or copies of the documents specified in §§ 23 and 24, which serve as the basis of identification and verification of a person, and the documents serving as the basis of establishment of a business relationship no less than five years after the termination of the business relationship.
(2) An obligated person shall preserve the documents prepared relating to the transaction on any data medium and the documents and data serving as the basis of the notification obligations specified in subsections 32 (1) and (2) for no less than five years after the conclusion of the transaction or the performance of the notification obligation.
(3) An obligated person shall preserve the documents and data specified in sections (1) and (2) in a manner which allows for an exhaustive and immediate reply to enquiries from the Financial Intelligence Unit or other investigative bodies or from a court pursuant to legislation.

Division 3 Management of Risks Relating to Money Laundering and Terrorist Financing

§ 27. Refusal from transaction and termination of business relationship

(1) An obligated person is prohibited to establish a business relationship or to enter into a transaction specified in clause 12 (1) 2) if a person or customer participating in the transaction or the official act, regardless of a respective request, does not submit the documents or relevant information required to comply with the due diligence measures specified in clauses 13 (1) 1) to 4) or if, on the basis of the documents submitted, the obligated person suspects that it may be money laundering or terrorist financing.

(2) An obligated person has the right to refuse concluding a transaction if a person or customer participating in the transaction or the official act, regardless of a respective request, does not submit the documents or relevant information required for identification of the circumstances specified in clauses 13 (1) 1) to 4) or data and documents certifying the legal origin of the property constituting the object of the transaction or if, on the basis of the data and documents submitted, the obligated person suspects that it may be money laundering or terrorist financing.

(3) In a long-term contract serving as the basis of a business relationship, an obligated person shall stipulate the right to terminate it extraordinarily without following the term of advance notification, if a person or customer participating in a transaction concluded in economic or professional activities does not, regardless of a respective request, submit documents and relevant information or if the submitted documents and data do not eliminate the obligated person's suspicion that the purpose of the transaction or business relationship may be money laundering or terrorist financing.

(4) In the event of termination of a business relationship on the basis of subsection (3) of this section, a credit or financial institution may transfer the property of a customer only to an account opened in a credit institution or a branch of a credit institution registered in the Estonian commercial register or in a credit institution registered or having its seat in a contracting state of the European Economic Area or in a country, where requirements equal to those provided in this Act are in force. Provisions of subsection 720 (6) of the Law of Obligations Act do not apply relating to this subsection.

(5) The provisions of subsections (1) to (3) do not apply to notaries public, attorneys, bailiffs, trustees in bankruptcy or other legal service providers or to auditors and persons providing accounting or tax advice when evaluating the customer's legal position, defending or representing the customer in court, challenge or other such proceedings, including providing the customer with consultations regarding the initiation or avoidance of proceedings.

(6) An obligated person shall register the information about refusal to establish a business relationship or conclude a transaction and the circumstances of the termination of a business relationship and the information serving as the basis of the notification obligation arising from § 32 and shall preserve it pursuant to the procedure provided for in § 26.

§ 28. Outsourcing of activities related to economic or professional activities of obligated persons

(1) If an obligated person has outsourced an activity to a third party for the purpose of better performance of the obligations related to its economic or professional activities, it shall be deemed that the third party knows of all requirements arising from this Act. The obligated person who outsourced its activities is liable for infringement of the requirements.

(2) Outsourcing is permitted only if:

1) it does not harm the justified interests of the obligated person or the person participating in the transaction;

2) it does not impede the activities of the obligated person or the performance of the obligations provided in this Act;

3) it does not impede exercising state supervision over the obligated person;

4) the third party to whom the activities are outsourced has the required knowledge and skills and it is capable of fulfilling the requirements provided for in this Act;

5) the obligated person has the right and possibility to check the third party's performance of the requirements provided in this Act;

6) it is ensured that the documents and data collected for the fulfilment of the requirements arising from this Act are preserved pursuant to the procedure provided for in this Act and legislation adopted on the basis thereof.

(3) An obligated person notifies the competent supervisory authority of outsourcing its activities.

§ 29. Internal security measures

(1) An obligated person shall establish written rules of procedure for application of the due diligence measures provided in this Act, including the assessment and management of the risk of money laundering and terrorist financing, the collection and the preservation of data, and the performance of the notification obligation and the notification of the management, as well as rules of internal procedure for checking adherence thereto.

(2) The management board of a legal person considered an obligated person, the head of a branch of an obligated person or, upon absence of the former, an obligated person shall ensure the providing of regular training in the performance of obligations arising from this Act for employees whose duties include establishment of business relationships or conclusion of transactions.

(3) The management board of a credit and financial institution and the head of a branch of a foreign credit and financial institution registered in the Estonian commercial register appoints a person as the contact person of the Financial Intelligence Unit (hereinafter contact person).

(4) An obligated person who is not a credit or financial institution may appoint a contact person for the performance of the obligations related to prevention of money laundering and terrorist financing. Unless a contact person has been appointed, the obligations of a contact person shall be performed by the management board of a legal person, the head of a branch of a foreign company registered in the Estonian commercial register, or a sole proprietor.

(5) An employee or a structural unit may perform the functions of the contact person. If a structural unit performs the functions of the contact person, the head of the respective structural unit shall be responsible for the performance of the given functions. The competent supervisory authority shall be notified of the appointment of the contact person.

§ 30. Requirements for rules of procedure

(1) The rules of procedure established by an obligated person shall correspond to the type, scope and complexity of the economic or professional activities of the obligated person and set out the rules for application of due diligence measures at least in the events specified in subsection 13 (1).

(2) An obligated person shall regularly check whether the established rules of procedure are up-to-date and establish new rules of procedure where necessary.

(3) The rules of procedure shall:

1) describe transactions of a lower risk level and establish the appropriate requirements and procedure for entering into such transactions;

2) describe transactions of a higher risk level and establish the appropriate requirements and procedure for entering into and monitoring such transactions;

3) set out the rules of application of the due diligence measures specified in clause 13 (1) 5);

4) set out the requirements and procedure for preservation of the documents and data provided in Division 2 of this Chapter.

(4) The rules of procedure shall also contain instructions regarding how to effectively and quickly identify whether or not the person is:

1) a politically exposed person;

2) a person whose place of residence or seat is in a country where no sufficient measures for the prevention of money laundering and terrorist financing have been applied;

3) a person with regard to whose activities there is prior suspicion that the person may be involved in money laundering or terrorist financing;

4) a person with regard to whom international sanctions are imposed;

5) a person with whom a transaction is concluded via means of communications.

(5) The rules of procedure are introduced to all employees of an obligated person whose duties include establishment of business relationships or conclusion of transactions.

(6) The requirements for the rules of procedure to be established by credit and financial institutions, internal audit rules for checking the performance, and the application thereof shall be established by a regulation of the Minister of Finance.

§ 31. Contact person

(1) The organisational structure of a credit or financial institution shall be suitable for the performance of the requirements arising from this Act and ensure direct subordination of the contact person to the management board of the credit or financial institution.
(2) The management board of a credit and financial institution and the head of a branch of a foreign credit and financial institution registered in the Estonian commercial register shall ensure that the contact person has the competence, means and access to relevant information required for the performance of the functions provided in this Act in all structural units of the credit or financial institution.
(3) The functions of the contact person are:
1) analysis and organisation of gathering of information referring to unusual transactions or transactions with the suspicion of money laundering or terrorist financing in the activities of the obligated person;
2) notification of the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing;
3) periodic submission of written statements on implementation of the rules of procedure to the management board of the credit or financial institution or the head of the branch of the foreign credit or financial institution registered in the Estonian commercial register;
4) performance of other obligations, which are related to the fulfilment of the requirements of the Act by the credit or financial institution.
(4) The contact person has the right to:
1) make proposals to the management board of the credit or financial institution or the head of a branch of a foreign credit or financial institution registered in the Estonian commercial register for the amendment or modification of the rules of procedure containing requirements for prevention of money laundering and terrorist financing or the organisation of training specified in subsection 29 (2);
2) demand that the structural units of the obligated person eliminate within a reasonable term the deficiencies detected in the implementation of the requirements of the prevention of money laundering and terrorist financing.

Chapter 3
ACTION TAKEN IN CASE OF SUSPICION OF MONEY LAUNDERING OR TERRORIST FINANCING

§ 32. Notification obligation in case of suspicion of money laundering or terrorist financing
(1) If, upon performance of economic or professional activities or when carrying out an official act, an obligated person identifies an activity or circumstances which might be an indication to money laundering or terrorist financing or in case the obligated person has reason to suspect or knows that it is money laundering or terrorist financing, the obligated person shall immediately notify the Financial Intelligence Unit thereof.
(2) Subsection (1) shall also be applied in the events provided by subsections 27 (1) to (3).
(3) An obligated person, except a credit institution, notifies the Financial Intelligence Unit of any transaction where the financial obligation exceeding 500,000 kroons or an equal amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments. A credit institution notifies the Financial Intelligence Unit of any currency exchange transaction exceeding 500,000 kroons in cash, unless the credit institution has a business relationship with the person participating in the transaction.
(4) Notaries public and attorneys are not subject to the notification obligation arising from subsections (1) and (3) when evaluating a customer's legal position, defending or representing the customer in court, challenge or other such proceedings, including providing the customer with consultations regarding the initiation or avoidance of proceedings, regardless of whether the information has been received before, during or after proceedings.
(5) An obligated person has the right to postpone a transaction or an official act in the event specified in subsection (1). If postponement of a transaction may cause considerable harm, the transaction has to be concluded or if it may impede the apprehension of the person who possibly committed money laundering or terrorist financing, the transaction or the official act shall be carried out and the Financial Intelligence Unit shall be notified thereafter.

§ 33. Place and format of the performance of the notification obligation
(1) The information is forwarded to the Financial Intelligence Unit of the contracting state of the European Economic Area in whose territory the obligated person is located.
(2) A notification is communicated orally, in writing or in a format which can be reproduced in writing. If a notification was communicated orally, it shall be repeated the next working day in writing or in a format which can be reproduced in writing.
(3) The data used for identifying and verifying a person or, where necessary, copies of relevant documents may be appended to a notification.
(4) The format of the notification to be forwarded to the Financial Intelligence Unit and instructions for the preparation thereof shall be established by a regulation of the Minister of the Interior.

§ 34. Confidentiality obligation of the notifier
(1) An obligated person, a structural unit and 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 or initiation of criminal proceedings under § 40 or 41. 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 after fulfilment of the precept made by the Financial Intelligence Unit.
(2) The provisions of subsection (1) are also applied to the providing of information to third parties, unless otherwise provided in this Act.
(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 or management or internal control system as the obligated person in 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 who 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.
(4) Information exchanged pursuant to subsection (3) may be used only for the purpose of the prevention of money laundering and terrorist financing.
(5) The prohibition provided by subsection (1) is not applied if a notary public, attorney or auditor tries to convince a customer to refrain from illegal acts.

§ 35. Exempt from liability
(1) An obliged person, its employee, representative or a person who acted in its name is not, upon the performance of the obligations arising from this Act, liable for the damage arising from the failure to conclude a transaction or to conclude a transaction by the due date, if the damage was caused to the person participating in the transaction concluded in economic or professional activities in connection to the notification of the Financial Intelligence Unit of the suspicion of money laundering or terrorist financing in good faith, also for the damage caused to a person or customer participating in a transaction concluded in economic or professional activities in connection with the cancellation of a long-term contract on the basis of subsection 27 (3).
(2) The performance of the notification obligation in good faith arising from § 32 and the communication of the relevant data by an obligated person is not deemed infringement of the confidentiality requirement provided by law or contract and no liability provided by legislation or

contract is imposed on the person who performed the notification obligation for the disclosure of the information. An agreement derogating from this provision is void.

Chapter 4
FINANCIAL INTELLIGENCE UNIT

§ 36. Financial Intelligence Unit
(1) The Financial Intelligence Unit is an independent structural unit of the Central Criminal Police.
(2) The head of the Financial Intelligence Unit is appointed by the national police commissioner of the Police Administration on the proposal of the police chief of the Central Criminal Police for five years.
(3) The Police Board provides the Financial Intelligence Unit with sufficient funds for the performance of the functions provided by law.

§ 37. Functions of Financial Intelligence Unit
(1) The functions of the Financial Intelligence Unit are:
1) to gather, register, process and analyse information received pursuant to §§ 32 and 33 of this Act. In the course thereof, the significance of the information submitted to the Financial Intelligence Unit for the prevention, identification or investigation of money laundering, criminal offences related thereto and terrorist financing are assessed;
2) to inform the persons who submit information to the Financial Intelligence Unit of the use of the information submitted for the purposes specified in clause 1) of this section in order to improve the performance of the notification obligation;
3) tracing criminal proceeds and application of the enforcement powers of the state on the bases and within the scope provided by law;
4) to supervise the activities of obligated persons in complying with this Act, unless otherwise provided by law;
5) public disclosure of the information on prevention and identification of money laundering and terrorist financing, analysing the respective statistics, and preparing and publishing an aggregate overview at least once a year;
6) cooperation with obligated persons, investigative bodies and police institutions in the prevention of money laundering and terrorist financing;
7) training obligated persons, investigative bodies, prosecutors and judges in matters related to prevention of money laundering and terrorist financing;
8) organisation of foreign communication and exchange of information pursuant to § 46;
9) exercising supervision over the application of the measures specified in clauses 3 (1) 3) to 5) of the International Sanctions Act, unless otherwise provided by the Act or legislation of the European Union;
10) to conduct proceedings in matters of misdemeanours provided for in this Act.
(2) The Financial Intelligence Unit analyses and verifies information about suspicions of money laundering or terrorist financing, taking measures for preservation of property where necessary and immediately forwarding materials to the competent authorities upon detection of elements of a criminal offence.

§ 38. Administrative acts of the Financial Intelligence Unit
(1) The Financial Intelligence Unit issues precepts and other administrative acts in order to perform the functions arising from law.
(2) A precept issued on the basis of subsection 40 (1) of this Act does not set out the factual basis for the issue. The factual circumstances reasoning the precept are reflected in a separate document. The person whose transaction was suspended or the use of whose account was restricted by a precept has the right to examine the document presenting the factual circumstances. The Financial Intelligence Unit has the right to deny a request to examine a document if this would impede the prevention of money laundering or terrorist financing or hinder the truth from being ascertained in criminal proceedings.
(3) An administrative act of the Financial Intelligence Unit is signed by the head or deputy head of the Financial Intelligence Unit or by an official authorised by the head of the Financial Intelligence Unit.

Upon signature by an authorised official, the number and date of the document granting the right of signature and the place where the document can be reviewed is indicated next to the signature.
(4) In the event of failure to comply with an administrative act, the Financial Intelligence Unit may impose a coercive measure pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act. The upper limit for a penalty payment for failure to comply with the administrative act is 20,000 kroons for the first occasion and 80,000 kroons for each subsequent occasion.

§ 39. Guidelines of the Financial Intelligence Unit
(1) The Financial Intelligence Unit has the right to issue advisory guidelines to explain the legislation regulating the prevention of money laundering and terrorist financing.
(2) The Financial Intelligence Unit issues advisory guidelines regarding the characteristics of suspicious transactions.
(6) The Financial Intelligence Unit issues advisory guidelines regarding the characteristics of terrorist financing. The guidelines are coordinated with the Security Police Board beforehand.
(4) The guidelines of the Financial Intelligence Unit are published on the website of the Financial Intelligence Unit.

§ 40. Suspension of transaction, restriction of disposal of property and transfer of property to state ownership
(1) In the event of suspicion of money laundering or terrorist financing, the Financial Intelligence Unit may issue a precept suspending a transaction or imposing restrictions on the disposal of an account or other property constituting the object of the transaction for up to thirty days as of the delivery of the precept. In the case of property registered in the land register, ship register, traffic register or commercial 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 thirty days.
(2) Before expiry of the term specified in subsection (1) a transaction may be entered into or the restriction of disposal of an account of other property may be derogated from only upon the written consent of the Financial Intelligence Unit. During the time the restrictions on using the account are in force, the credit or financial institution does not execute any orders issued by the account holder for debiting the account.
(3) On the basis of a precept the Financial Intelligence Unit may restrict the disposal of property for up to 60 days for the purpose of ensuring its preservation if:
1) during verification of the source of the property in case there is a suspicion of money laundering, the owner or possessor of the property fails to submit evidence certifying the legality of the source of the property to the Financial Intelligence Unit within thirty days as of the suspension of the transaction or as of the imposition of restrictions on the use of the account;
2) there is suspicion that the property is used for terrorist financing;
(4) If in case of suspicion of money laundering the legality of the source of the property is verified before the term specified in subsection (3) of this section expires, the Financial Intelligence Unit is required to revoke the restrictions on the disposal of the property immediately. If criminal proceedings have been commenced in the matter, a decision shall be taken on the revocation of the restrictions on the disposal of the property from pursuant to the procedure provided by the Acts regulating criminal procedure.
(5) Disposal of property may be restricted for a term exceeding the term specified in subsection (3) if criminal proceedings have been commenced in the matter.
(6) The Financial Intelligence Unit or the investigative body may restrict the disposal of property until identification of the actual owner as well as upon termination of criminal proceedings if it has not proven possible to establish the actual owner of the property and if the possessor of the property asserts that the property does not belong to possessor and relinquishes possession thereof.
(7) The Prosecutor's Office or the investigative body may apply to an administrative court for permission to transfer property to state ownership if, within a period of one year as of establishment of the restrictions on the disposal of the property, it has not proven possible to establish the owner of the property and if the possessor of the property asserts that the property does not belong to him and relinquishes possession thereof. In the event where possession of movable property or immoveable

property is relinquished, the property shall be sold pursuant to the procedure provided in the Acts regulating the enforcement procedure and the amount received from the sale is transferred to the state. The owner of the property has the right to reclaim an amount equivalent to the value of the property within a period of three years from the date on which the property is transferred to state ownership.

§ 41. Requesting additional information

(1) To perform the functions arising from law the Financial Intelligence Unit has the right to receive information from the Financial Supervision Authority or state and local government authorities and, on the basis of precepts, from obligated persons regarding the circumstances, transactions or persons related to suspicion of money laundering or terrorist financing.

(2) The addressee of a precept is required to comply with the precept and to submit the requested information, including any information subject to banking or business secrecy, during the term prescribed in the precept. The information is submitted in writing or in a format which can be reproduced in writing.

(3) In order to prevent money laundering, the Financial Intelligence Unit has the right to obtain, pursuant to the procedure provided by legislation, relevant information, including information collected by surveillance, from any surveillance agency. If the Financial Intelligence Unit wishes to forward information collected by surveillance and which was submitted by a surveillance agency to other agencies, the Financial Intelligence Unit must obtain written consent from the agency which submitted the information.

(4) On the basis of a precept the Financial Intelligence Unit has the right to receive information from third parties to identify the circumstances which are relevant to the prevention of money laundering or terrorist financing, including accounting documents on any data medium from a third party whose connection to the investigated transactions became evident in the course of the inspection or analysis.

(5) This section does not apply to an attorney, except in cases where the notification submitted by the attorney to the Financial Intelligence Unit does not meet the established requirements, the required documents are not attached to the notice or the attached documents do not meet the requirements.

§ 42. Interbase cross-usage of data

In order to perform the functions arising from law, the Financial Intelligence Unit has the right to make enquiries and receive data from state and local government databases and databases maintained by persons in public law, pursuant to the procedure provided by the legislation.

§ 43. Restrictions on the use of information

(1) Only the officials of the Financial Intelligence Unit shall have access to and the right to process the information in the Financial Intelligence Unit database.

(2) In order to prevent or identify money laundering or terrorist financing or criminal offences related thereto and in order to facilitate pre-trial investigation thereof, the Financial Intelligence Unit is obligated to forward significant information, including information subject to tax and banking secrecy to the prosecutor, the investigative body and the court.

(3) Information registered in the Financial Intelligence Unit shall only be forwarded to the authority engaged in the pre-trial procedure, the prosecutor or a court in connection with criminal proceedings on the basis of a written request of the preliminary investigation authority, the Prosecutor's Office or the court or on the initiative of the Financial Intelligence Unit if the information is significant for the prevention, establishment or investigation of money laundering, terrorist financing or a criminal offence related thereto.

(4) The Financial Intelligence Unit may notify the Financial Supervision Authority of infringement of the requirements established by this Act by a credit or financial institution.

(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.

(6) The procedure for the registration and processing of the information gathered by the Financial Intelligence Unit shall be established by a regulation of the Minister of the Interior.

§ 44. Requirements for officials of Financial Intelligence Unit
(1) Only a person with impeccable reputation, required experience and abilities, and high moral qualities may be appointed as an official of the Financial Intelligence Unit.
(2) Officials of the Financial Intelligence Unit are required to maintain the confidentiality of information received 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.

§ 45. Cooperation between Financial Intelligence Unit and Security Police Board
(1) The Financial Intelligence Unit and the Security Police Board shall cooperate in investigation of transactions suspected of terrorist financing through mutual official assistance and exchange of information.
(2) The Director General of the Security Police Board shall appoint a contact person who has an equal right to the 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.
(3) The contact person of the Security Police Board shall be subject to the provisions of subsections 37 (1) 1), 6) and 7), § 41, subsections 43 (1) to (5) and subsection 44 (2).
(4) The contact person of the Security Police Board has the right to exercise supervision specified in § 48 jointly with the Financial Intelligence Unit.

§ 46. International exchange of information
The Financial Intelligence Unit has the right to exchange information and enter into cooperation agreements with foreign agencies which perform the functions of a financial intelligence unit.

Chapter 5
SUPERVISION

§ 47. Supervisory authorities
(1) The Financial Intelligence Unit exercises supervision over fulfilment of the requirements arising from this Act and legislation adopted on the basis thereof by the obligated persons, unless otherwise provided in this section.
(2) The Financial Supervision Authority exercises supervision over fulfilment of the requirements arising from this Act by credit and financial institutions which are subject to supervision by the Financial Supervision Authority under the Financial Supervision Authority Act.
(3) The board of the Estonian Bar Association (hereinafter the Bar Association) exercises supervision over fulfilment of the requirements arising from this Act and legislation adopted on the basis thereof by the members of the Bar Association on the basis of the Bar Association Act, taking into account the provisions of this Chapter.
(4) The Ministry of Justice exercises supervision over fulfilment of the requirements arising from this Act and legislation adopted on the basis thereof by notaries public on the basis of the Notaries Act, taking into account the provisions of this Chapter. The Ministry of Justice may delegate supervision to the Chamber of Notaries.
(5) The Financial Supervision Authority, the board of the Bar Association and the Ministry of Justice and the Chamber of Notaries shall cooperate with the Financial Intelligence Unit pursuant to the objectives of this Act.

§ 48. Rights of the supervisory authority
(1) The supervisory authority has the right to inspect the place or the seat of business of obligated persons. The supervisory authority has the right to enter the building and the 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 the documents and data media from the obligated person, and monitor the work processes;

2) receive oral and written explanations from the obligated person, members of its directing body or employees.

§ 49. Rights of the supervisory authority

(1) If upon exercising supervision the Financial Supervision Authority, the board of the Bar Association, the authorised officials of the Ministry of Justice or the Chamber of Notaries detect a situation of which the elements refer to a 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).

(2) The Financial Supervision Authority, the board of the Bar Association and the Ministry of Justice obliged to submit to the Financial Intelligence Unit by April 15 information about:

1) supervisory operations conducted in the previous calendar year;

2) violations detected upon exercising supervision and punishments imposed in the previous calendar year based on types of obligated persons.

§ 50. Reporting of the inspection results

(1) The supervisory authority shall prepare a report on the inspection results, which is communicated to the inspected person within one week after the inspection.

(2) The inspection report shall contain the following data:

1) the name of the inspection operation;

2) the official title and given name and surname of the compiler of the inspection report;

3) the place and date of the compiling of the inspection report;

4) reference to provisions serving as the basis for inspection;

5) the given name and surname and the official title of the representative of the inspected person or the possessor of the building or room who attended the inspection;

6) the given name and surname and the official title of another person who attended the inspection;

7) the time of the beginning and the end and the conditions of the inspection;

8) the process and results of the inspection along with the required details.

(3) The compiler of the inspection report signs it. The inspection report remains with the supervisory official, a copy shall be given to the inspected person or their representative.

(4) The inspected person has the right to submit written explanations within 30 days after receiving the inspection report.

§ 51. Data protection supervision

The Data Protection Inspectorate exercises supervision over the legality of the processing of the information registered in the Financial Intelligence Unit.

Chapter 6
REGISTRATION IN THE REGISTER OF ECONOMIC ACTIVITIES

§ 52. Registration obligation

(1) The following persons (hereinafter in this Chapter service providers) are required to register themselves in the register of economic activities (hereinafter in this Chapter register) before commencing operations in the corresponding area of activity:

1) financial institutions which are not subject to supervision by the Financial Supervision Authority pursuant to § 2 of the Financial Supervision Authority Act;

2) providers of trust and company services;

3) providers of currency exchange services;

4) providers of payment services;

5) providers of alternative means of payment services;

6) pawnbrokers.

(2) The provisions of the Register of Economic Activities Act apply to the registration procedure together with the specifications arising from this Act.

§ 53. Registration application

(1) The service provider shall submit a registration application to the authorised processor of the register. The registration application shall contain:
1) the name, registry code, address and other contact details of the service provider;
2) the area of activity;
3) the address or addresses of the place or places of service providing or the address of the website used for providing the service;
4) the name and contact details of the person in charge of providing the service with regard to all the places of service providing specified in clause 3);
5) the name, personal identification code or, upon absence thereof, the date and place of birth and the address of the place of residence of a member of the directing body of the service provider who is a legal person, unless the service provider is an undertaking registered in the commercial register;
6) the name, personal identification code or, upon absence thereof, the date and place of birth and the address of the place of residence of the beneficial owner of the service provider who is a legal person;
7) the date of submission of the application, and a signature;
8) the name, official title and contact details of the person who signed the application.
(2) If a service provider who is a legal person has not been registered in the Estonian commercial register, the registration application shall contain the name and personal identification code or registry code, upon absence thereof, the date and place of birth and place of residence of the owner of the service provider.

§ 54. Registration
(1) In addition to the provisions of the Register of Economic Activities Act, the prerequisite for registration is that it becomes evident from a reply to an enquiry made to the authorised processor of the penal register by the authorised processor of the register that there are no grounds for refusal from registration arising from § 55 in connection with the person specified in clauses 53 (1) 1), 5) and 6).
(2) In addition to the information provided by the Register of Economic Activities Act, the following shall be entered in the register:
1) the area of activity;
2) the address or addresses of the place or places providing the service or the address of the website used for providing the service;
3) the name and contact details of each person in charge of providing the service with regard to the places providing the service;
4) the name, personal identification code or, upon absence thereof, the date and place of birth and the address of the place of residence of a member of the directing body of the service provider who is a legal person;
5) the name, personal identification code or, upon absence thereof, the date and place of birth and the address of the place of residence of the beneficial owner of the service provider who is a legal person.
(3) Only the registered service provider, state authority or a person who must perform duties imposed on it by law or a legislation pursuant to law is entitled to access the data specified in clauses (2) 4) and 5) and receive extracts or make enquiries using the data security measures agreed on the registrar and via a data exchange system based on a computer network.

§ 55. Refusal to register
In addition to the provisions of the Register of Economic Activities Act the authorised processor of the register shall refuse to register if it becomes evident from a reply to an enquiry made to the penal register that a criminal conviction for a crime specified in §§ 237-237^3 or 394-396 of the Penal Code has entered into force with regard to the persons specified in clauses 53 (1) 1), 5) or 6) or subsection 53 (2) or with regard to whom a criminal conviction for another intentionally committed criminal offence has entered into force and the terms arising from subsection 25 (1) of the Penal Register Act have not expired.

§ 56. Deletion of the registration
In addition to the provisions of the Register of Economic Activities Act a registration shall be deleted if it becomes evident from a reply to an enquiry made to the penal register that a criminal conviction for a crime specified in §§ 237-237^{3} or 394-396 of the Penal Code has entered into force with regard to the persons specified in clauses 53 (1) 1), 5) or 6) or subsection 53 (2) or with regard to whom a criminal conviction for another intentionally committed criminal offence has entered into force.

Chapter 7
LIABILITY

§ 57. Failure to comply with the identification requirement
(1) Failure on the part of an employee of a credit or financial institution or on the part of another person or agency or an employee thereof to comply with the identification obligation provided in this Act is punishable by a fine of up to 300 fine units.
(2) The same act, if committed by a legal person, is punishable by a fine up to 500,000 kroons.

§ 58. Violation of the requirement to register and preserve data
(1) Violation of the requirement to register and preserve data provided in this Act is punishable by a fine up to 300 fine units.
(2) The same act, if committed by a legal person, is punishable by a fine up to 500,000 kroons.

§ 59. Failure to submit and late submission of mandatory information
Failure on the part of an employee of an obligated person to submit mandatory information provided for in this Act to the contact person or the manager, or intentional failure to submit such mandatory information on time, is punishable by a fine up to 300 fine units.

§ 60. Failure to report suspicion of money laundering or terrorist financing and submission of incorrect information
(1) Violation of the obligation to notify the Financial Intelligence Unit of suspicion of money laundering or terrorist financing, currency exchange transaction or another transaction where the financial obligation exceeds 500,000 kroons or an equal amount in another currency is performed in cash or submission of incorrect information by the manager, contact person or another employee of an obligated person is punishable by a fine up to 300 fine units or detention.
(2) The same act, if committed by a legal person, is punishable by a fine up to 500,000 kroons.

§ 61. Unlawful notification of the information submitted to the Financial Intelligence Unit
(1)Unlawful notification of a person or a beneficial owner of a person by the manager, contact person or another employee of an obligated person about a notification or data submitted to the Financial Intelligence Unit regarding the person or the precepts made by the Financial Intelligence Unit or criminal proceedings instituted regarding the person is punishable by a fine up to 300 fine units or detention.
(2) The same act, if committed by a legal person, is punishable by a fine up to 500,000 kroons.

§ 62. Failure to apply internal security measures
(1) Failure by the manager of an obligated person to establish rules of procedure for application of due diligence measures, assessment and management of the risk of money laundering and terrorist financing, gathering of information, preservation of data and performance of the notification obligation as well as failure to appoint the contact person by the manager of a credit or financial institution is punishable by a fine up to 300 fine units.
(2) The same act, if committed by a legal person, is punishable by a fine up to 500,000 kroons.

§ 63. Violation of the obligations of a payment service provider
(1) Failure to identify, verify or communicate information about a payer by the manager or employee of a payment services provider or a violation of other obligations of a payment service provider

established by Regulation (EC) No. 1781/2006 of the European Parliament and Council, of the payer accompanying the transfers of funds is punishable by a fine up to 300 fine units.
(2) The same act, if committed by a legal person, is punishable by a fine up to 500,000 kroons.

§ 64. Violation of the registration obligation
Violation of the obligation to register an application for the amendment of the registration data or the violation of the obligation to notify of the termination of the activities of the service provider established with regard to financial institutions not subject to supervision exercised by the Financial Supervision Authority, trust and company service providers, currency exchange service providers, payment service providers, providers of services of alternative means of payment and pawnbrokers is punishable by a fine up to 300 fine units.

§ 65. Proceeding
The misdemeanours specified in §§ 57-64 are subject to the provisions of the general part of the Penal Code and the Code of Misdemeanour Procedure.
(2) Extrajudicial proceedings concerning the misdemeanours provided for in §§ 57-64 of this Act shall be conducted by:
1) police prefecture;
2) the Financial Supervision Authority;
3) the Financial Intelligence Unit.

Chapter 8
IMPLEMENTING PROVISIONS

§ 66. Entry into force of the registration obligation of pawnbrokers, trust and company service providers and financial institutions
Chapter 6 of this Act shall enter into force with regard to pawnbrokers, trust and company service providers and financial institutions not subject to supervision exercised by the Financial Supervision Authority on 15 June 2008.

§ 67. Repeal of Money Laundering and Terrorist Financing Prevention Act
The Money Laundering and Terrorist Financing Prevention Act (RT I 1998, 110, 1811; 2007, 24, 127) is repealed.

§ 68. Amendment of Credit Institutions Act
The Credit Institutions Act (RT I 1999, 23, 349; 2007, 24, 127) is amended as follows:
1) subsection 88 (8) is worded as follows:
"(8) Credit institutions have the right and obligation to disclose information subject to banking secrecy to the Financial Intelligence Unit and the Security Police Board in the cases and to the extent prescribed in the Money Laundering and Terrorist Financing Prevention Act.";
2) subsection 89 2^3 is worded as follows:
"(2^3) The standard term by which a credit institution or a financial institution belonging to the same consolidation group as the credit institution reserves the right to amend the standard term specified in subsection 2^2 of this section shall be subject to the provisions of subsection 43 (2) of the Law of Obligations Act. Amendment of the standard term shall be deemed as unfair first of all if the amendment gives the credit institution or the financial institution belonging to the same consolidation group as the credit institution the right to process personal data to an extent which the data subject could not reasonably foresee given the purpose of the contract."

§ 69. Amendment of Security Authorities Act
Clause 21) is added to § 6 of the Security Authorities Act (RT I 2001, 7, 17; 2007, 16, 77) worded as follows:
"2^1) prevention and combating terrorism, terrorist financing and terrorist supporting, and collection and processing of information to that end;".

§ 70. Amendment of Taxation Act

Subsection 28 (9) of the Taxation Act (RT I 2002, 26, 150; 2007, 44, 316) shall be worded as follows:

"8) to the Financial Intelligence Unit for the prevention, detection and investigation of money laundering or terrorist financing or criminal offences related to money laundering or terrorist financing;".

§ 71. Amendment of Penal Code

Subsection § 334[1] (1) of the Penal Code (RT I 2001, 61, 364; 2007, 45, 320) shall be amended and worded as follows:

"(1) Failure to hand counterfeit money over to a police prefecture by an employee of Eesti Post, credit institutions or financial institutions provided for in the Credit Institutions Act, or providers of payment services or providers of currency exchange services specified in the Money Laundering and Terrorist Financing Prevention Act is punishable by a fine up to 300 fine units."

§ 72. Amendment of Notaries Act

The Notaries Act (RT I 2000, 104, 684; 2006, 7, 42) is amended as follows:

1) subsections 5 (1) and (2) are amended and worded as follows:

"(1) The Ministry of Justice exercises supervision over the professional activities of notaries public. The Ministry of Justice may involve the Chamber of Notaries in exercising supervision.

(2) The Ministry of Justice may delegate supervision over fulfilment of the requirements of the Money Laundering and Terrorist Financing Prevention Act and legislation adopted on the basis thereof as well as supervision over other single issues to the Chamber of Notaries. In the area of delegated supervision the Ministry of Justice may give instructions for exercising supervision and change the decisions approved by the Chamber of Notaries in these issues.";

2) clause 1^1) is added to subsection 44 (1) worded as follows:

"(1^1) monitor that notaries public fulfil the requirements of the Money Laundering and Terrorist Financing Prevention Act and legislation adopted on the basis thereof;"

3) clause 3^1) is added to subsection 44 (2) worded as follows:

"(3^1) exercise supervision over fulfilment by notaries public of the requirements of the Money Laundering and Terrorist Financing Prevention Act and legislation adopted on the basis thereof;".

4) clause 10) is added to subsection 44 (3) worded as follows:

"(10) implementation of the due diligence measures and rules of procedure provided in the Money Laundering and Terrorist Financing Prevention Act."

---

[1] 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 (OJ L 309, 25.11.2005, pp. 15-36);
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 (OJ L 214, 04.08.2006, pp. 29-34).

Annex 4. Penal Code - excerpt

The entire Penal Code is accessible at http://www.legaltext.ee/text/en/X30068K7.htm

Chapter 7

Other Sanctions

§ 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 belong to the offender at the time of the making of the judgment or ruling.
(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.
(4) In the absence of the permission necessary for the possession of an object or substance, such object or substance shall be confiscated.
(5) In the cases provided for in subsection (4) of this section, a device, object or substance may be confiscated if the person has committed at least an unlawful act.
(6) In the cases provided for in subsections (1), (2) and (4) of this section, the object used to commit a misdemeanour or the substance or object which was the direct object of a misdemeanour may be confiscated by the extra-judicial body prescribed by law.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 83[1]. Confiscation of assets acquired through offence
(1) A court shall confiscate of 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.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 83[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.
(4) Upon extended confiscation of assets acquired through criminal offence, the court shall take account of the provisions of subsection 83^1 (3) of this Code.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 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.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 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 (2of this Code.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)
(3) Before entry into force, the decision of an extra-judicial body or court concerning confiscation has the effect of a prohibition against disposal.
(12.06.2002 entered into force 01.09.2002 - RT I 2002, 56, 350)

Division 2
Offences Against State Power

§ 237. Acts of terrorism
(24.01.2007 entered into force 15.03.2007 - RT I 2007, 13, 69)
(1) Commission of a criminal offence against international security, against the person or against the environment, 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 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 five to twenty years' imprisonment, or life imprisonment.
(24.01.2007 entered into force 15.03.2007 - RT I 2007, 13, 69)
(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 § 83^2 of this Code.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 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 § 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.
(24.01.2007 entered into force 15.03.2007 - RT I 2007, 13, 69)

§ 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 § 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.
(24.01.2007 entered into force 15.03.2007 - RT I 2007, 13, 69)

§ 237^3. Financing and support of acts of terrorism
(1) Financing or supporting a criminal offence provided in §§ 237, 237^1, 237^2 of this Code in another manner 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.
(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 § 83^2 of this Code.
(24.01.2007 entered into force 15.03.2007 - RT I 2007, 13, 69)

Division 5
Offences Relating to Money Laundering

§ 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 § 83 of this Code, apply confiscation of an property which was the direct object of the commission of an offence provided for in this section.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)
(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 § 83^2 of this Code.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 395. Failure to comply with identification requirement
(1) Failure to comply with the identification requirement, a punishment for a misdemeanour has been imposed on the offender for the same act, is punishable by a pecuniary punishment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(28.06.2004 entered into force 01.07.2004 - RT I 2004, 54, 387)

§ 396. Failure to report suspicious transaction, submission of incorrect information

(1) Failure to report a suspicious transaction or a suspicion of terrorist financing or submission of incorrect information to the Financial Intelligence Unit, if a punishment for a misdemeanour has been imposed on the offender for the same act, is punishable by a pecuniary punishment or up to one year of imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(28.06.2004 entered into force 01.07.2004 - RT I 2004, 54, 387)

Annex 5. Code of Criminal Procedure - excerpt

The entire Code of Criminal Procedure is accessible at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X60027K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=kriminaalmenetlus

§ 34. Rights and obligations of suspects
(1) A suspect has the right to:
1) know the content of the suspicion and give or refuse to give testimony with regard to the content of the suspicion;
2) know that his or her testimony may be used in order to bring charges against him or her;
3) the assistance of a counsel;
4) confer with the counsel without the presence of other persons;
5) be interrogated and participate in confrontation, comparison of testimony to circumstances and presentation for identification in the presence of a counsel;
6) participate in the hearing of an application for an arrest warrant in court;
7) submit evidence;
8) submit requests and complaints;
9) examine the report of procedural acts and give statements on the conditions, course, results and report of the procedural acts, whereas record shall be made of such statements;
10) give consent to the application of settlement proceedings, participate in the negotiations for settlement proceedings, make proposals concerning the type and term of punishment and enter or decline to enter into an agreement concerning settlement proceedings.
(2) A conference specified in clause (1) 4) of this section may be interrupted for the performance of a procedural act if the conference has lasted for more than one hour.
(3) A suspect is required to:
1) appear when summoned by an investigative body, Prosecutor's Office or court;
2) participate in procedural acts and obey the orders of investigative bodies, Prosecutors' Offices and courts.

§ 40^1. Third party
(1) The body conducting the proceedings may involve a third party in the criminal proceeding if the rights or freedoms of the person which are protected by law may be adjudicated in the adjudication of the criminal matter or in special proceedings.
(2) A third party who is a legal person shall participate in a criminal proceeding through a member of the management board or the body substituting for the management board of the legal person and such member has all the rights of a third party.
(3) The provisions concerning civil defendant apply to third parties on participation in procedural acts, examination of criminal file and failure to appear when summoned by body conducting proceedings unless otherwise provided for in this Code.
(13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)

§ 142. Seizure of property
(1) The objective of seizure of property is to secure a civil action, confiscation or fine to the extent of assets. "Seizure of property" means recording the property of a suspect, accused, 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.
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329; 13.12.2006 entered into force 01.02.2007 - RT I 2007, 2, 7)
(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.
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329)
(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 twenty-four hours after the seizure and the 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.
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329)
(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 submitted for examination to the person whose property is to be seized or to his or her adult family member upon the performance of the procedural act. The person or family member shall sign the ruling to that effect.
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329)
(6) If necessary, an expert or specialist 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.
(8) An immovable may be 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. For the seizure of an immovable, a Prosecutor's Office shall submit an order on seizure to the land registry department of the location of such immovable in order for a prohibition on the disposal of the immovable to be made in the land register.
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329)
(9) A construction work which is a movable or a vehicle may be 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. For the seizure of a building which is a movable, a Prosecutor's Office shall submit an order on seizure to the register of construction works of the location of the building; for the seizure of a vehicle, the order shall be submitted to the motor vehicle register.
(19.05.2004 entered into force 01.07.2004 - RT I 2004, 46, 329; 19.04.2006 entered into force 25.05.2006 - RT I 2006, 21, 160)
(10) Property which pursuant to law must not be subject to a claim for payment shall not be seized.

§ 143. Report of seizure of property
(1) The report of seizure of property shall set out:
1) the names and characteristics of the seized objects and the number, volume or weight and value of the objects;
2) a list of property taken over or deposited into storage with liability;
3) lack of property to be seized if such property is missing.
(2) A list of seized property may be annexed to the report of seizure of property and a notation concerning the list is made in the report. In such case, the report shall not contain the information listed in clause (1) 1) of this section.

Annex 6. Links to other relevant legislation

- Bar Association Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30070K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=advokatuuriseadus

- Commercial Code
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X0001K16&keel=en&pg=1&ptyyp=RT&tyyp=X&query=%E4riseadustik

- Credit Institutions Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30042K10&keel=en&pg=1&ptyyp=RT&tyyp=X&query=krediidiasutuste+seadus

- E-money Institutions Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XX00001&keel=en&pg=1&ptyyp=RT&tyyp=X&query=e%2Draha

- Estonian Central Register of Securities Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30067K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=v%E4%E4rtpaberite

- Foundations Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X1014K6&keel=en&pg=1&ptyyp=RT&tyyp=X&query=sihtasutuste

- General Part of the Civil Code Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30082K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=tsiviilseadustiku

- Identity Documents Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30039K11&keel=en&pg=1&ptyyp=RT&tyyp=X&query=dokumentide

- Insurance Activities Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90004&keel=en&pg=1&ptyyp=RT&tyyp=X&query=kindlustustegevuse

- Investment Funds Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X80045&keel=en&pg=1&ptyyp=RT&tyyp=X&query=investeerimisfond

- Law of Obligations Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30085K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=v%F5la%F5igusseadus

- Non-profit Associations Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X1013K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=mittetulundus

- Notaries Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X50001K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=notariaadi

- Police Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X60006K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=politseiseadus

- Precious Metal Articles Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90024&keel=en&pg=1&ptyyp=U&tyyp=X&query=

- Prosecutor's Office Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X2050K10&keel=en&pg=1&ptyyp=RT&tyyp=X&query=prokuratuur

- Register of Economic Activities Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X80016&keel=en&pg=1&ptyyp=RT&tyyp=X&query=majandustegevuse

- Savings and Loan Associations Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30055K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=hoiu%2D

- Securities Market Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40057K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=v%E4%E4rtpaberitur

- The International Sanctions Act
  http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X70011K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=sanktsiooni

- Advisory Guidelines of the Financial Supervisory Authority: Requirements regarding the arrangement of operational risk management (established by resolution no. 63 of the Management Board of the Financial Supervisory Authority dated 18 May 2005 on the basis of § 57 (1) of the Financial Supervisory Authority Act)
  http://www.fi.ee/failid/20050518_nouded_OR_juhtimise_korraldamiseks_EN.pdf

- Previous MLTFPA (in force until 28 January 2008)
  http://www.legaltext.ee/text/en/X30024K4.htm