

MODULE 3

Summary of the vulnerability of the banking sector conducted during the national risk assessment

Members of the working group:

- (Financial Supervision Authority, head of the working group)
- (Financial Intelligence Unit)
- (Ministry of Finance)
- (Eesti Pank/*Bank of Estonia*)
- (Estonian Banking Association)

The employees of Eesti Pank and Financial Supervision Authority also participated in the work of the working group.

Introduction:

The new recommendations of the Financial Action Task Force (FATF) (Recommendation 1), which entered into force in February 2012, require countries to systematically conduct national risk assessments of money laundering and terrorist financing, and unlike in the past, official risk assessment documents are no longer sufficient. It is therefore necessary to use a methodological approach and extend the limits of risk assessment beyond the institutional view, prepare a National Risk Assessment (hereinafter *NRA* or *national risk assessment*).

In order to prepare the NRA, the Government Committee for the Prevention of Money Laundering and Terrorist Financing decided at the meeting on 17 October 2012 to establish a separate working group (hereinafter *risk assessment working group*). The work of the risk assessment working group is led by the Ministry of Finance and its members are: representatives of the Ministry of Justice, Ministry of the Interior, Ministry of Foreign Affairs, Ministry of Finance, Tax and Customs Board, Internal Security Service, Police and Border Guard Board, Financial Intelligence Unit and Financial Supervision Authority. It was decided to

prepare the risk assessment in accordance with the World Bank methodology¹ (hereinafter: the methodology).

The aim of the module and brief description of its structure

The following is a brief summary of the impact assessment² (risk assessment) of the risk criteria and standard products for the banking sector. The assessment takes into account the data and circumstances for the years 2010 - 2012. In doing so, the estimates have not taken into account the results of Moneyval's IV evaluation report and other relevant changes that have entered into force after 2012 and which, by their nature, may affect the conclusions reached.

The risk assessment of the banking sector was based on the principles set out in the methodology. First, the various risk criteria³ and their vulnerability were assessed. The second part analyzed the impact of different standard banking products on the development of risk assessment in the banking sector.

The risk assessment of the sector addressed and assessed, inter alia, the following risk criteria:

- Applicable regulations - AML laws and regulations (preventive measures and supervision);
- Quality of AML supervision;
- Market pressure to meet AML standards;
- Commitment to good corporate governance;
- Applicable penalties for breach of due diligence;
- Enforcement of AML obligations;
- Bank staff integrity;
- Bank staff knowledge;
- Compliance function;
- Banks 'AML monitoring, data collection and record keeping systems;
- Identification infrastructure;
- Availability of independent information sources;
- Corporate and trust transparency.

The second part assessed the impact of specific products and the risks associated with the provision of related services, including separately:

¹ *Second Generation National Money Laundering Risk Assessment Tool.*

² The translation of the terms in the methodology may differ by working groups.

³ See footnote 1.

- Volume of product;
- Average transaction size of the product;
- Client profile of the product⁴;
- Other vulnerable features of the product;
- Existence of appropriate specific controls for the product.

The working group of the banking sector decided to change the initial list of products in the methodology⁵, as the standard products therein were not distinguishable in Estonian credit institutions in this way and to the extent necessary in the context of money laundering risk assessment.

The initial list of products offered in the methodology is provided in the working document of this module. The list of products used in the assessment has been provided for in section 2 of this document.

Summary of the impact analysis of the risk criteria and standard products in the banking sector. Rating.

1. Overall assessment of the vulnerability of the sector

When preparing the risk assessment of the banking sector, the members of the working group reached the opinion that the criteria assessed in the methodology have been applied in accordance with the standards, their impact on reducing potential money laundering risks is “high” (average rating ranged from 0.81 to 1.00)⁶.

1.1 Applicable regulations - AML laws and regulations (preventive measures and supervision)

According to the working group the banking sector is well covered by anti-money laundering and anti-terrorist financing regulations. The established regulations comply with the international and EU standards. The compliance of the norms applied in Estonia with the international standard has also been noted in the Moneyval Estonian evaluation reports of the Council of Europe Committee of Experts on the Prevention of Money Laundering and Terrorist Financing, where the respective assessments have been provided.

⁴ The client's risk primarily includes the risk of the client's country of origin, including whether it is a non-resident, person from the low tax rate or risk country (risk countries are according to the opinions of FATF, see: <http://www.fi.ee/index.php?id=12165>) person.

⁵ The intention to change the products included in the methodology was coordinated with the representatives of the World Bank at the seminar held in Tallinn. The main reason for changing the list of financial products was the wish to keep only those financial products that may have an impact in the Estonian context.

⁶ The estimates in this document are preliminary and may change in the course of further analysis.

In order to clarify the obligation arising from law, the Financial Supervision Authority has prepared the recommended guidelines on the implementation of measures to prevent credit and money laundering and terrorist financing. Due to the FATF recommendations that changed in 2012, the Financial Supervision Authority also updated its guidelines. The new guide entered into force on 1 January 2014.

The Regulation no. 10 “Requirements for the rules of procedure to be established by a credit and financial institution and their implementation and enforcement” (hereinafter: Regulation no. 10) and Regulation no. 11 “Criteria for low risk of money laundering and terrorist financing, where diligence measures may be applied in a simplified manner” issued by the Ministry of Finance on 3 April 2008 also handle the application of measures to prevent money laundering and terrorist financing. In addition to the above, the Financial Intelligence Unit has issued several instructions to obliged entities.

The Financial Supervision Authority exercises control over the implementation of measures aimed at preventing money laundering and terrorism by credit and financial institutions, which has set this issue as one of its priority activities. The Financial Supervision Authority has regularly mapped the shortcomings in the implementation of due diligence measures and analyzed their reasons. As a result of the respective analyses, the operational priorities for the following periods have been created and the emphases in the guidelines have been specified.

In the course of its supervisory activities, the Financial Supervision Authority has not identified any significant deficiencies in the implementation of measures to prevent money laundering and terrorist financing in credit and financial institutions. Moneyval has also not identified any significant shortcomings in the implementation of the respective standard in its evaluation reports, which is why the assessment of the applicable regulations (AML laws and regulations (preventive measures and supervision)) is high, i.e. 0.90.

1.2 Quality of AML supervision

The Financial Supervision Authority supervises the measures to prevent money laundering and terrorist financing in credit and financial institutions. The scope of supervision covers the activities from the processing of authorizations, assessment of the professional suitability of the managers of credit and financial institutions to the right to issue instructions on money laundering, issue precepts, prosecute misdemeanours and revoke authorizations.

Pursuant to § 64 (2) of the Money Laundering and Terrorist Financing Prevention Act the Financial Supervision Authority exercises supervision over compliance with the requirements for money laundering prevention by credit and financial institutions that are subject to its

supervision under the Financial Supervision Authority Act. Pursuant to clause 17 (1) 12) of the Credit Institutions Act, an authorization can be revoked if “the credit institution engages in money laundering, or violates the procedure established by legislation for the prevention of money laundering or terrorist financing”. In exercising supervision, the Financial Supervision Authority proceeds from a risk-based approach. On the one hand, the Financial Supervision Authority performs threat analysis, where the factors affecting the activities of the supervised entity are under assessment. On the other hand, a subject-specific vulnerability analysis is performed to assess the risks associated with the respective due diligence measures, internal procedures and business specifics. When comparing and assessing these components, the Financial Supervision Authority applies appropriate supervisory measures.

The management board of the Financial Supervision Authority approves the supervisory priorities and the action plan every year, incl. in particular, it is proceeded from the risks associated with the activities of the institutions that are systemically important and have a greater impact in the relevant field.

Various structural units (divisions) of the Financial Supervision Authority are involved in the prevention of money laundering and terrorist financing, including different divisions with a task based on their operational specifics. A separate structural unit within the Financial Services Supervision Division is responsible for the supervision of the respective area, 3 to 4 employees of which are involved in the supervision of the prevention of money laundering and terrorist financing on a daily basis. In addition, the Regulation and Reporting Division collects and analyzes reports. The Capital Supervision Division analyzes the activities of obliged entities, conducts the Fitness and Propriety procedure for managers and assesses operational risks. The Market Surveillance Division deals with the analysis of market abuses. However, the Legal Department provides secondary opinions on the legality of the processes carried out in the Financial Supervision Authority.

The following is an overview of the Financial Supervision Authority's anti-money laundering activities in 2010-2012.

2010-2012									
	Total number of on-site inspections carried out	Number of inspections having identified AML/CFT infringements	Written warning*	Fines		Removal of manager/compliance officer (where applicable)**	Withdrawal of license (where applicable)	Other (please specify and add further columns as applicable)	Number of sanctions taken to court (if applicable)
				Number	Amount (EUR)				
FINANCIAL SECTOR									
Credit institutions	1	1	1	N/A	N/A	N/A	N/A	1 (precept)	N/A
Branches of foreign credit institutions	1	1	1	N/A	N/A	N/A	N/A	1 (precept)	N/A

Investment firms	3	3	3	N/A	N/A	N/A	N/A	3 (precept)	N/A
Fund Management Companies	0	0	0	N/A	N/A	N/A	N/A	N/A	N/A
Life Insurance	1	1	1	N/A	N/A	N/A	N/A	1 (precept)	N/A
PSP-s	2	2	1	N/A	N/A	N/A	1	1 (precept)	N/A
E-money SP	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TOTAL	8	8	7	N/A	N/A	N/A	1	7	N/A

*) *Written warning or note that indicates the shortcomings detected.*

**) *There has been several resigning of key persons (compliance officers, contact persons, heads of client management units etc.) from the obliged entities in result of other supervisory activities (precepts and notes).*

The Financial Supervision Authority has the right to apply administrative coercion in the event of violation of measures to prevent money laundering and terrorist financing in order to ensure the elimination of identified deficiencies and punishment of persons. In addition to the data presented in the table above, several employees in the respective field in credit institutions have been dismissed from the office for insufficient compliance or violation of due diligence measures identified by the Financial Supervision Authority. In the course of processing authorisations, the Financial Supervision Authority has failed to issue authorisations to several persons whose business reputation does not meet the requirements.

However, Moneyval has questioned the adequacy of the resources allocated to the evaluation of anti-money laundering and anti-terrorist financing measures and the supervisory capacity to impose financial penalties for identified deficiencies in III evaluation report and the subsequent progress report. */...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 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 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/.*

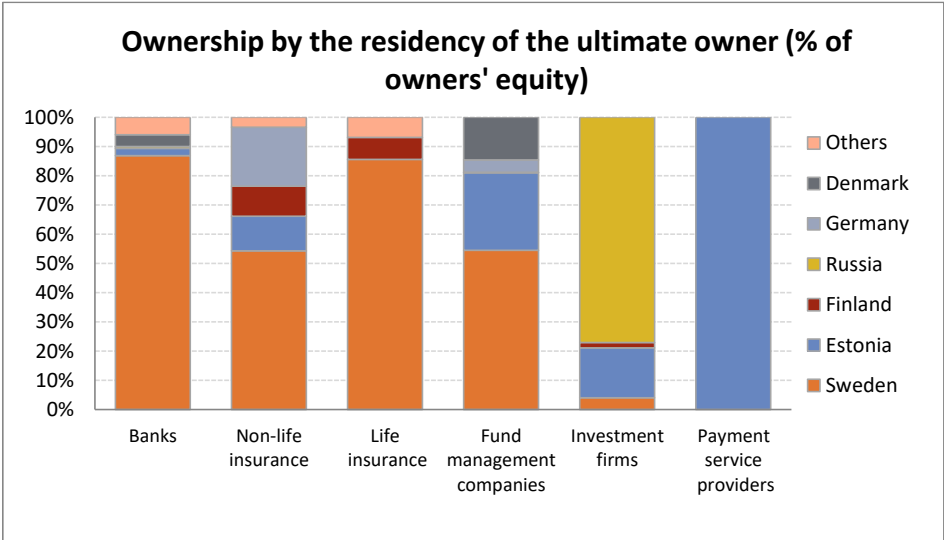
Taking into account the relevant comments of Moneyval, the relevant provisions of § 57-62 of the Money Laundering and Terrorist Financing Prevention Act were amended in 2009 to allow the Financial Supervision Authority to apply financial penalties for identified violations. The review of the supervisory activities of the Financial Supervision Authority indicates that no financial penalties have been applied.

In view of the above, the assessment of the quality of AML supervision is “medium/high”, i.e. 0.75.

1.3 Market pressure to meet AML standards

The credit and financial institutions operating in Estonia are primarily characterized by their connection with owners or parent companies of Scandinavian origin.

The attached illustration shows the distribution of ownership structure by country of origin.



Due to the fact that the majority of credit and financial institutions are a part of a larger Scandinavian financial group, they will inevitably have to take into account national regulatory and supervisory implications and common anti-money laundering and anti-terrorist financing policies and procedures for cross-border financial groups.

The standards in the legislation of the Scandinavian countries are known to comply with the provisions of the FATF and EU III Anti-Money Laundering Directive 2005/60/EC, and the standard of the due diligence applied in these countries is one of the highest in the world, so the service providers should take this into account.

The Financial Supervision Authority has entered into co-operation agreements with the financial supervision authorities of neighbouring countries, which oblige the parties to inform each other of any problems that have arisen. The cooperation and exchange of information in the field of money laundering and terrorist financing have worked well. This is especially noticeable in case of the branches operating in Estonia, where supervision is carried out in co-operation with the supervisory authority of the country of origin, which is why possible violations are disclosed to the supervisory authorities of both countries. Reputation is gaining weight in the competition between credit institutions as well as neighbouring countries, which is why no service provider wants to come under the scrutiny of the supervisory authority of the country in which it operates or any other country. It is noteworthy that no credit institution operating in Estonia has been banned from transactions by its clients by the US Office of

Foreign Assets Control (OFAC) of the US Department of the Treasury due to transactions that may be related to the transactions with illegally acquired property.

At the same time the Financial Supervision Authority has established that the level of reputational risks in credit institutions differs, some service providers take higher risks based on their economic interests at the expense of serving high-risk customers. However, it has not been established that the uneven application of due diligence measures has been abused.

In view of the above the assessment of the market pressure to meet AML standards is “high”, i.e. 0.85.

1.4 Commitment to good corporate governance

For the purposes of the Money Laundering and Terrorist Financing Prevention Act and Credit Institutions Act, the members of the management board of credit institutions are responsible for the management of the company, establishment of the respective internal procedures and implementation of the respective control mechanisms. In addition to the general principles of management and risk management, the legislation also provides for the obligation to establish an internal audit institution and to implement a compliance function in all business processes. The activities of credit and financial institutions are subject to audit.

§ 29 and § 30 of the Money Laundering and Terrorist Financing Prevention Act set out detailed requirements for both internal security measures and rules of procedure. The Chapter 3 of Regulation no. 10 sets out the requirements for the rules of procedure to be established by the credit and financial institutions, internal control rules for the control of their compliance and specifies the requirements for their implementation.

Pursuant to § 48 (2) of the Credit Institutions Act only the persons who have the necessary expertise, skills, experience, education, professional qualifications and an impeccable business reputation may be elected or appointed managers of a credit institution. The section 3 stipulates that a person whose earlier activities have caused the bankruptcy or compulsory liquidation or revocation of the activity licence of a company, or from whom the right to engage in economic activity has been taken away pursuant to law, or whose earlier activities as a manager of a company have shown that he or she is not capable of organising the management of a company such that the interests of the shareholders, members, creditors and clients of the company are adequately protected, or whose earlier activities have shown that he or she is not suitable to manage a company for other good reasons shall not be elected or appointed manager of a credit institution or a member of the supervisory board or management board of the parent company of a credit institution or a company belonging to the same consolidation group as the parent company.

The section 4 stipulates that the managers and staff members of a credit institution are required to act with the prudence and competence expected of them and according to the requirements for their posts in line with the interests of the credit institution and the clients thereof. The section 5 stipulates that the managers and staff members of a credit institution are required to give priority to the economic interests of the credit institution and the clients thereof over their own personal economic interests. The assessment of the suitability and compliance of the managers of a credit institution is also regulated by Regulation no. 24 of Eesti Pank of 15 October 1999 "Procedure for submission of data confirming compliance and declaration of economic interests of the persons specified in the Credit Institutions Act".

In addition to the above provisions, the good corporate governance code includes general principles for the members of the supervisory as well as management board, issued in cooperation between the Financial Supervision Authority and the stock exchange. This document does not directly refer to the compliance with money laundering requirements, but according to general principles, the members of the supervisory board and management board should comply with legislation, avoid conflicts of interest, be independent, manage risks properly, etc. The rules and regulations of the stock exchange state that this is a good practice, the observance of which should be declared in the reports.

The above principles for the head of a credit institution ensure that the management board includes persons who are sufficiently qualified to perform their work, have a clear understanding of the duties and general management of the company. At the same time the Financial Supervision Authority controls these cases when the company enters the market and does so on an ongoing basis during Fitness and Propriety proceedings. In the course of the Fitness and Propriety proceedings, the Financial Supervision Authority has also identified the violations of the requirements for managers, which is why it has applied administrative coercion, including issued precepts to recall the head of a credit institution.

The Financial Supervision Authority continuously evaluates the activities of credit institutions, including the evaluation of operational policies as well as the mechanisms of formation and suitability of the entire management and decision-making processes. In addition, the group-wide policies and principles established by the owners of credit institutions, mainly from Scandinavian countries, applied in day-to-day operations should be taken into account here. At the same time, the differences arising from Estonia's geopolitical environment and the resulting temptations to earn income in areas that are inherently riskier should be considered. In the course of its supervisory activities the Financial Supervision Authority has identified different attitudes of the managers of a credit institution in the commitment to good corporate governance practices, which is reflected in the concentration of certain types of risks in these credit institutions.

In view of the above, the assessment of the wish of credit institution managers to commit to good corporate governance is “high”, i.e. 0.85.

1.5 Penalties applied for breach of due diligence measures

Penalties for money laundering offenses are provided in subchapter 5 of the Penal Code, including for money laundering in § 394. For failure to comply with identification requirement in § 395, for failure to report suspicious transaction, submission of incorrect information in § 396. In addition, pursuant to § 372, an activity without an activity license or a prohibited economic activity is deemed to be a criminal offense.

It is also important to assess the possible penalties for money laundering offenses:

- The offence provided for in § 394 (1) of the Penal Code is punishable by a pecuniary punishment or up to five years' imprisonment. In reality a maximum of 1 year's imprisonment has been imposed for offence of section 1.
- The maximum possible punishment for violation of § 394 (2) of the Penal Code is 2 to 10 years' imprisonment. In practice, a breach of section 2 is usually punishable by 2 to 4 years' imprisonment. If the person has no previous convictions, the imprisonment is generally not enforced, but a probation period (usually 2-4 years) is imposed. In case of legal persons, both relatively small financial penalties and compulsory dissolution were identified. As a rule, however, legal persons cannot be punished.

Compared to the penalties for other offenses, the penalties for money laundering are rather lenient (e.g. in case of § 394 (2) (committing money laundering by a group, at least twice, on a large-scale basis or by a criminal organization), the minimum penalty is 2 years' imprisonment).

Although Estonia has sufficient measures in place to prosecute individuals, the state's penal policy in relation to the prevention of money laundering and terrorist financing is disproportionate to the crime committed, as money laundering offenses are not covered by "financial crime with serious damage". Money laundering crimes are not indicated as a priority area in the development directions of the criminal policy of the Riigikogu until 2018.

Given the complexity of money laundering crime proceedings and the relatively small number of sanctions applied, the assessment of the effectiveness of the applicable penalties (Penalties) is “medium/high”, i.e. 0.75.

1.6 Enforcement of AML obligations

Penalties for money laundering offenses are provided in subchapter 5 of the Penal Code, including for money laundering in § 394. For failure to comply with identification requirement

in § 395, for failure to report suspicious transaction, submission of incorrect information in § 396. In addition, pursuant to § 372, an activity without an activity license or a prohibited economic activity is deemed to be a criminal offense.

Pursuant to the aforementioned sections of the Penal Code, penalties have been imposed in accordance with the database of court decisions as follows:

Overview of money laundering penalties

	2008	2009	2010	2011	2012	2013 (9 months)
Number of court decisions	4	10	16	16	16	7
Number of persons convicted	8	11	51	65 (incl. 8 legal persons in three different cases)	45 (all natural persons)	18 (all natural persons)

The decisions made on the basis of § 394 and § 372 of the Penal Code dominate the most. No convictions have been made since 2006 on the basis of § 395 and § 396 of the Penal Code.

One of the possible reasons why the number of convictions for money laundering offenses may seem relatively low is that a conviction for money laundering requires proof of a predicate offense, which in many cases has proved difficult to prove in cross-border offenses. When analyzing the court judgments that have entered into force, it can be seen that in about half of the cases in 2010-2012 men of straw and/or associations were used to commit money laundering. The convicts themselves are often the members of the management board of these same front companies. The companies have been accused of money laundering infrequently.

Given the relatively small size of the Estonian financial sector and the efficient operations of supervisory authorities, it can be assumed that the breaches of due diligence will sooner or later be identified and appropriate sanctions will be imposed. The court-imposed sanctions are also available to both supervisory authorities and market participants, see https://www.riigiteataja.ee/kohtuteave/maa_ringkonna_kohtulahendid/main.html, which means that it can be assumed that the awareness of possible sanctions is high.

Due to the above the assessment of enforcement of AML obligations is "high", i.e. 0.85.

1.7 Bank staff integrity

Employee loyalty is generally set out in internal rules. The employee is required to be loyal to the employer, including the principles of processing professional information and personal data of clients have been separately stipulated.

Pursuant to § 48 (4) of the Credit Institutions Act the managers and staff members of a credit institution are required to act with the prudence and competence expected of them and according to the requirements for their posts in line with the interests of the credit institution and the clients thereof. Pursuant to § 55 of the Credit Institutions Act the management board is required to ensure that all staff members of the credit institution are aware of the provisions of legislation relating to their duties of employment and of the principles provided for in the documents approved by the directing bodies of the credit institution;

The market participants generally detect employee frauds through internal controls and internal security measures. The reports of detected internal fraud are submitted to the Financial Supervision Authority.

The Financial Supervision Authority has stipulated in its new recommended guidelines the following: "An obliged entity will manage and avoid conflicts of interest with internal rules where the bases for remuneration of managers and employees would encourage them to give up or make concessions in complying with legislation and the guidelines." This obligation also comes from clause 2.2.3 of the Financial Supervision Authority's recommended guide "Good corporate governance", according to which the bases for remuneration of the management board are clear and transparent. The supervisory board regularly discusses and reviews the bases for remuneration of the management board. When deciding on the remuneration of the management board, the supervisory board proceeds from the assessment of the activities of the members of the management board.

The obligation of an employee to act loyally to the employer is provided for in § 15 (1) of the Employment Contracts Act, this obligation essentially includes the obligation to act in good faith within the meaning of § 6 of the Law of Obligations Act. The Employment Contracts Act also imposes an obligation on the employee to avoid competition and maintain secrecy. It can therefore be stated that, although there is no corresponding obligation to lay down rules of internal procedure concerning, inter alia, the situation in which an employee is prevented from cooperating with offenders, the relevant special laws indirectly provide guidelines to prevent such a situation.

The obligation of confidentiality of employees usually arises from the employment contract and internal rules, but also from the internal rules for the prevention of conflicts of interest, the employee's job description, ethical principles and work organization rules. Both business secrets and bank secrets are treated as confidential.

Due to the above, the assessment of bank staff integrity is “high”, i.e. 0.85.

1.8 Bank staff knowledge

The Money Laundering and Terrorist Financing Prevention Act and Regulation no. 10 stipulate the obligation to train employees. Pursuant to § 14 (6) of the Money Laundering and Terrorist Financing Prevention Act, the management board of a legal person that is an obliged entity, the manager of a branch that is an obliged entity or, upon their absence, the obliged entity must ensure that the employees whose employment duties include the establishment of business relationships or the making of transactions are provided with training in the performance of the duties and obligations arising from the Money Laundering and Terrorist Financing Prevention Act. In training, information, inter alia, on the modern methods of money laundering and terrorist financing and the related risks should be given.

§ 27 (3) of Regulation no. 10 provides that an employee of a credit and financial institution has the right to receive the training necessary for the performance of tasks related to the prevention of money laundering and terrorist financing. In addition, an employee whose duties include establishing business relationships or entering into transactions shall be introduced to the applicable rules of procedure and internal control rules upon taking up employment and thereafter as necessary, but not less frequently than once a year.

The Financial Supervision Authority, in cooperation with the Financial Intelligence Unit, has regularly organized information days to raise the awareness of employees in the respective field of the norms for the prevention of money laundering and terrorist financing and the principles of their implementation. Information days have taken place about 1-2 times a year. In addition, the meetings of the anti-money laundering committee of the Banking Association are held approximately once a month, which also deal with issues related to the topic, which are later passed on during the internal trainings of credit institution employees.

According to the representatives of credit institutions, the topic of money laundering prevention is a part of instructing new employees, and the persons involved in the topic undergo a corresponding supplement once a year. According to the Financial Supervision Authority the regularity and content of trainings of credit institutions, according to the purpose of the training, are at a good level.

Due to the above the assessment of the bank staff knowledge is “high”, i.e. 0.95.

1.9 Compliance function

The Money Laundering and Terrorist Financing Prevention Act stipulates the obligation to establish a compliance officer institution. Pursuant to § 31 of this act the organizational structure of a credit institution must be suitable for fulfilling the requirements arising from law and ensure the subordination of the compliance officer directly to the management board of the credit or financial institution. The contact person must have the necessary competence, resources and access to relevant information in all structural units of the credit institution in order to perform the tasks provided by law.

In addition, the obliged entity pursuant to § 29 (1) of the Money Laundering and Terrorist Financing Prevention Act shall establish in writing the rules of procedure for the application of due diligence measures, including money laundering and terrorist financing risk assessment and management, data collection and storage, rules of procedure for reporting and informing management and the internal control rules for monitoring compliance.

The institution of the compliance officer is an important link in collecting information on suspicious and unusual transactions in the credit institution and forwarding the relevant information to the Financial Intelligence Unit.

The procedure for notifying the Financial Intelligence Unit is provided in § 32 of the Money Laundering and Terrorist Financing Prevention Act. In order to identify suspicious or unusual transactions, the Financial Intelligence Unit has issued new guidelines in 2013 on the characteristics of transactions suspected of money laundering and on the characteristics of transactions suspected of terrorist financing. At the same time, the Minister of the Interior has established a form by a regulation that helps obliged entities to make notifications. This has created sufficient opportunities for obliged entities, including credit institutions, to fulfil the notification obligation provided for in § 32 of the Money Laundering and Terrorist Financing Prevention Act.

The credit institutions have sent suspicious notifications to the Financial Intelligence Unit:

2012 - 2185

2011 - 2400

2010 - 2627

The Financial Supervision Authority has assessed the activities of the compliance officer in the course of various supervisory procedures, the ability of the compliance officer's institution to perform the tasks assigned to it by law, its independence and the use of information collected on suspicious and unusual transactions. According to the Financial Intelligence Unit, the function of the compliance officer in credit institutions is well-functioning, a reliable relationship has been established, which supports the bilateral exchange of information.

Considering the given circumstances, the assessment of the compliance function is “high”, i.e. 0.95.

1.10 Banks’ AML monitoring, data collection and record keeping systems

The corresponding sections of the Money Laundering and Terrorist Financing Prevention Act and Regulation no. 10 stipulate the obligation of the obliged entity, including the credit institution, to keep data and to monitor and screen transactions in order to identify the politically exposed persons and subjects of international sanctions.

The subchapter 2 of the Money Laundering and Terrorist Financing Prevention Act sets out in detail the requirements for data collection and storage, including the storage of documents and data on the basis of which a natural or legal person is identified (§ 23 and 24), registration of transaction data (§ 25) and general data retention obligation (§ 26).

Chapter 2, subchapter 2 of Regulation no. 10 provides for a code of conduct on the collection and storage of data, including the storage of data used for identification (§ 17).

In addition to the above obligations, credit institutions shall implement measures for the monitoring and subsequent analysis of transactions, including transaction monitoring and screening, that enable them to identify suspicious or unusual transactions. In addition to identifying suspicious and unusual transactions, credit institutions are required to identify the subjects of international sanctions or persons subject to enhanced due diligence when conducting transactions. To search for the subjects of an international sanction, credit institutions use the FIU's search engine for the subject of an international sanction as well as the corresponding lists directly from the original source. The website of the Financial Supervision Authority also contains a reference to the search engine of the subject of international sanctions of the European Union available on the computer network and a reference to all established international sanctions. In order to identify the politically exposed persons, credit institutions use various databases available on the computer network, including World-Check, Dow Jones, Bloomberg, Google, etc.

In case of credit institutions the supervisory procedure has not established that the politically exposed person or the subject of an international sanction has not been identified.

The corresponding sections of the Money Laundering and Terrorist Financing Prevention Act and Regulation no. 10 stipulate the obligation of the obliged entity, including the credit institution, to keep data and to monitor and screen transactions in order to identify the politically exposed persons and subjects of international sanctions and comply with the notification obligation.

The procedure for notifying the FIU is provided in § 32 of the Financial Intelligence Unit. In order to identify suspicious or unusual transactions, the FIU has issued new guidelines in 2013 on the characteristics of transactions suspected of money laundering and on the characteristics of transactions suspected of terrorist financing. At the same time, the Minister of the Interior has established a form by a regulation that helps obliged entities to make notifications.

Credit institutions have sent significantly more suspicious notifications to the FIU than other obliged entities, see the attached table:

Statistical information on reports received by the FIU, 2012				
Monitoring entities, e.g.	Reports about transactions above threshold	reports about suspicious transactions		
		Suspicion unspecified	ML	FT
Commercial banks	20	4	2185	7
Insurance companies	0	1	1	0
Notaries	86	4	35	2
Currency exchange	3916	2	553	409
Broker companies	0	0	0	0
Securities' registrars	0	4	2	0
Lawyers	4	5	0	0
Accountants/auditors	20	1	0	0
Company service providers				
Others (please specify and if necessary, add further rows)				
money remittance	0	1	318	0
Loan providers	0	0	0	0
Leasing providers	0	0	3	0
Payment services provider	575	8	1397	1313
Non-cash payment services providers	0	0	0	0
Traders	169	3	17	0
Real estate agents	0	0	0	0
Organizers of gambling	571	1	9	1
Bailiffs	1	0	1	0
Other legal counsellors	0	0	1	0
Trustees in bankruptcy	0	5	0	0
State agencies	14	227	11	0
Foreign authorities	0	220	1	0
Other	5	24	0	0
Total	5381	510	4534	1732

The Financial Supervision Authority has assessed the systems applied in credit institutions for monitoring transactions, and the conditions for storing transaction data have also been

repeatedly discussed. In the opinion of the Financial Supervision Authority, the transaction monitoring systems of credit institutions and the conditions for data storage comply with the norms established by legislation.

In view of the above, the assessment of banks' AML monitoring, data collection and record keeping systems is "high", i.e. 0.90.

1.11 Identification infrastructure

The Money Laundering and Terrorist Financing Prevention Act stipulates general identification obligations, incl. pursuant to § 13 the obliged entity pays increased attention to the activities and circumstances of a person participating in a transaction or official activity, a person using professional services or a client that indicate money laundering or terrorist financing or terrorist financing is likely, including complex, high-value and unusual transactions that do not have a reasonable economic purpose. Pursuant to § 19 (1), the obliged entity shall apply due diligence measures at least: 1) upon establishment of a business relationship; 2) upon making or mediating occasional transactions outside a business relationship where a transaction with a value of over 15,000 euros or an equivalent sum in another currency is made, 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; 3) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in this act; 4) when there is doubt as to the sufficiency or truthfulness of documents or data previously gathered in the course of identification of a person, verification of submitted information or updating the relevant details.

Pursuant to § 13 (1) of the Money Laundering and Terrorist Financing Prevention Act, an obliged entity shall apply the following due diligence measures to perform the obligation specified in § 12 of the Money Laundering and Terrorist Financing Prevention Act in economic, professional or professional activities: 1) identification of a customer or a person participating in an occasional transaction and verification of the submitted information based on information obtained from a reliable and independent source; 2) identification and verification of the identity and right of representation of the representative of a natural or legal person; 3) identification of the beneficial owner, including the collection of information on the ownership and control structure of the legal person, trust, partnership or other such contractual entity, on the basis of pre-contractual information or other information obtained from a reliable and independent source; 4) obtaining information on the business relationship and the purpose and nature of the transaction; 5) continuous monitoring of the business relationship, including monitoring of transactions performed during the business relationship, regular verification of the data used for identification, updating of relevant documents, data

and information and, if necessary, identification of the source and origin of the funds used in the transaction.

Pursuant to § 14 (1) of the Money Laundering and Terrorist Financing Prevention Act, an obliged entity will apply the due diligence measures specified in § 13 (1) 1) -4) before establishing a business relationship or entering into a transaction, unless otherwise provided in this act. Pursuant to § 14 (3) of the Money Laundering and Terrorist Financing Prevention Act, the obliged entity must apply the due diligence measures specified in § 13 (1) of the Money Laundering and Terrorist Financing Prevention Act, but may choose an appropriate scope for the application of due diligence measures, depending on the nature of the business relationship or transaction or the level of risk of the person involved in the transaction or professional activity, the person using the professional service or the client.

By taking into account the aforementioned norms of the Money Laundering and Terrorist Financing Prevention Act, it can be said that in Estonia, at the level of legislation, it is provided which information should be used to establish the identity of the customer and be collected about the person participating in the transaction. The provisions of this act also comply with the European Union directives and international standards.

Most credit institutions use a web portal to communicate with their customers, where identification is done through various authentication systems. One of the most common electronic means of identification is the use of an ID card. An Estonian ID card is an identity card issued by the Republic of Estonia, i.e. an identity document. The most important electronic operations performed with an ID card are personal identification and digital signing. Every Estonian citizen of at least 15 years of age permanently staying/living in Estonia should have an ID card.

Estonian legislation provides for the identification structure of the customer or person involved in the transaction in accordance with European Union legislation and international standards, thus the assessment of the identification infrastructure is “high”, i.e. 0.85.

1.12 Availability of independent information sources

Pursuant to § 14 (1) of the Money Laundering and Terrorist Financing Prevention Act, the obliged entity will apply the due diligence measures specified in § 13 (1) 1)-4) of the Money Laundering and Terrorist Financing Prevention Act each time before establishing a business relationship or concluding a transaction. In Estonia, the legislation has precisely defined which information should be collected regarding the customer or the person participating in the transaction. The provisions of this act also comply with European Union directives and

international standards. Pursuant to § 89 (2) 1) of the Credit Institutions Act the credit institution has the right to verify the validity of the identity documents on which the identification is based. Upon checking the validity of identity documents, a credit institution has the right to obtain personal data from the respective databases of the state agencies issuing the documents.

In Estonia information on the validity of identity documents is publicly and electronically available to all market participants. In addition, business register is available electronically in Estonia, where everyone has free access to limited information. There is a charge for the full information request. The Estonian Business Register also provides access to the European Business Register. These business registers enable to obtain information on the management structure of a potential customer or person participating in the transaction. The market participant can also make inquiries in the Central Register of Securities, where it is possible to obtain information on the beneficial owners of Estonian companies. The Credit Register provides information on the payment behaviour of a customer or a person participating in a transaction, international databases on PEPs and subjects of international sanctions. In addition, everyone has access to public sources of information, such as Google and others.

An obliged entity can verify the authenticity of identity documents on the basis of information published on the website of the Police and Border Guard Board. The verification of power of attorney can be performed by notaries, if the power of attorney must be legalized or supplied with apostille. Thus, it can be said that there is sufficient regulation in Estonia and practical possibilities are also ensured so that the obliged entity can collect data or verify the submitted data from independent sources.

Due to the above, it can be said that market participants generally receive information on the reliability and financial behaviour of customers or persons involved in transactions from public databases, business register, population register, internet searches, group databases, international sanctions lists (in addition, original confirming documents are required from the customers). Reliability can also be established by interviewing customers or the person involved in the transaction.

In practice, credit institutions use a number of relevant databases, such as WorldCheck, Dow Jones, Bloomberg and others.

Estonia has a suitable system in place to verify the data submitted or collected from independent sources, which is why the assessment of the availability of independent information sources) is “high”, i.e. 0.90.

1.13 Corporate and trust transparency

According to § 13 of the Money Laundering and Terrorist Financing Prevention Act the obliged entity pays increased attention to the activities and circumstances of a person participating in a transaction or official activity, a person using professional services or a client that indicate money laundering or terrorist financing or terrorist financing is likely, including complex, high-value and unusual transactions that do not have a reasonable economic purpose.

Pursuant to § 13 (1) 3) of the Money Laundering and Terrorist Financing Prevention Act the obliged entity shall identify the beneficial owner, including the collection of information on the ownership and control structure of a legal person, trust, partnership or other such contractual legal entity, in order to perform the obligation specified in § 12 of the Money Laundering and Terrorist Financing Prevention Act in economic, professional or trade activities, on the basis of information provided during the pre-contractual negotiations or other information obtained from a reliable and independent source.

§ 9 of the Money Laundering and Terrorist Financing Prevention Act provides for the definition of "beneficial owner". According to section 1 of that provision, beneficial owner means a natural person who exercises control over a transaction, operation or other person or in whose interests, for the benefit of whom or in whose name a transaction or operation is made. Pursuant to section 11 a beneficial owner is also a natural person who ultimately owns or controls the company in at least one of the following ways: 1) owns more than 25 percent of the shares through direct or indirect ownership or control; including in the form of bearer shares or units; 2) by otherwise controlling the management of the legal person.

The instructions of the Financial Supervision Authority specify the circumstances related to the identification of the beneficial owner. Normally, a person is found to identify the beneficial owner who owns 25 per cent of the shares, stocks or voting rights through direct or indirect ownership or control, including in the form of bearer shares or units.

At the same time, in the course of supervisory procedures, the Financial Supervision Authority has established that the obliged entities have not been able to identify the beneficial owner who controls the management of the company "in another way". The latter is also confirmed by the fact that according to the inquiries made from the database of court decisions, men of straw, managers as men of straw, front companies and undertakings were used in committing offence of § 394 of the Penal Code in five out of twenty decisions in 2010, six out of sixteen decisions in 2011 and six out of twelve decisions in 2012.

The identification of the beneficial owner depends to a large extent on the availability of data based on supervisory findings. In case of complex ownership structures, it is difficult to identify the beneficial owner through the direct or indirect holding or control of shares, stocks or

voting rights, including in the form of bearer shares or units. In this case, it is also difficult to identify the beneficial owner who otherwise controls the management of the legal person. However, in case of complex ownership structures, verification in another way is one of the main ways to identify the beneficial owner.

Despite the compliance of the norms set out in the Money Laundering and Terrorist Financing Prevention Act with international standards, credit institutions are not always able to identify the actual beneficiaries and persons who otherwise control the activities of the legal entity.

Due to the above, the assessment of the corporate and trust transparency is “medium/high”, i.e. 0.75.

Summary

The analysis of the impact of risk criteria affecting credit institutions revealed that the criteria discussed in the methodology have a significant impact on reducing money laundering and anti-terrorist financing risks, including high willingness of credit institutions to apply anti-money laundering standards and due diligence measures, the diligence and knowledge of the employees are in accordance with the established legislation and correspond to the associated risks. Credit institutions have applied high corporate governance practices, which ensure the responsibility of management for the implementation of applied due diligence measures. The measures to identify the management and ownership structure of the companies were also found to be satisfactory. The legal technical measures implemented in the sector for the identification and independent verification, processing and storage of the submitted data meet the objectives provided in the standard.

However, it was found that there was room for efficiency gains for a number of criteria, e.g. it was found that penalties and the effectiveness of due diligence enforcement could be higher, so the impact of this criterion was assessed at 0.75. The impact of any of the criteria was not assessed as low.

2. Assessment of the vulnerability of the products and services offered in the sector

To assess the vulnerability of products and services offered in the banking sector, the approach set out in the methodology was used, according to which the impact of the volume of individual services or products, the average size of transactions and the risk of the customer performing it was assessed. In addition, the risks arising from the specifics of these products and the specific supervisory measures applied were assessed.

The initial list of products provided in the methodology was changed during the seminar at the proposal of the members of the working group, as the products offered in the methodology were not distinguishable in Estonian credit institutions in this way and to the extent necessary in the context of money laundering risk assessment. A questionnaire was prepared for credit institutions to evaluate the products and services offered in the sector. In order to reduce the administrative burden on the sector, the respective questionnaire was sent to only five credit institutions: AS SEB Pank, AS Swedbank, AS Eesti Krediidipank, Danske Bank A/S Estonian branch and Nordea Bank Finland PLC Estonian branch. The aggregate data of these five credit institutions make up about 95% of the volume of services in the respective sector.

In addition to the data received from credit institutions, the databases of the Financial Supervision Authority and Eesti Pank⁷ were also used in preparing the risk assessment to assess the services and transaction volumes of credit institutions.

The following products or services were assessed to evaluate the vulnerability of products and services offered in the banking sector:

- a) Private banking = individuals with a customer-based balance of liquid assets of at least EUR 100,000 (incl.) at the end of the year or more;
- b) Retail deposits = individuals whose balance of customer-based liquid assets at the end of the year were less than EUR 100,000;
- c) Deposits of legal persons = legal persons whose customer-based balance of deposits (eg current account, overnight deposit, term deposit, current deposit, guarantee deposit, investment deposit, etc.) at the end of the year was at least EUR 100,000 (incl.) or more;
- d) Trust and asset management services⁸;
- e) Credit products for retail customers;
- f) Credit products for small and medium size businesses;
- g) Negotiable instruments;
- h) Trade finance;
- i) Correspondent accounts;
- j) Electronic banking;
- k) Cash payments;
- l) Initiated international payments;
- m) Incoming international payments;

⁷ In the course of the work, it became clear that in order to make inquiries and process the respective data, it is necessary to involve analysts from the Financial Supervision Authority and Eesti Pank, whose participation was not taken into account in the planning of activities.

⁸ Asset management data obtained from banking statistics according to the parameters of the asset management product and differs from the data of “wealthy clients” received from credit institutions. The categories of asset management and wealthy clients are relatively similar, so consideration should be given to merging them in the future to avoid repeating the effects of similar risks.

n) Cash exchange⁹.

3.1. Assessment of the vulnerability of main products and services offered in the banking sector¹⁰

The vulnerability of products offered in the banking sector was assessed simultaneously in 2010-2012 (hereinafter the observed period) by years. This approach makes it possible to compare the indicators obtained for 2012 with the corresponding assessments of previous years.

3.1.1. Private banking

The valuation of the volume of deposits of wealthy clients was based on private clients of credit institutions whose customer-based balance of liquid assets at the end of the year was at least EUR 100,000 or more. The total number of such customers was 4000-4400. To assess the impact of the volume of services, the share of deposits of such customers was compared with the volume of resources of credit institutions. (Consideration was also given to finding a corresponding ratio to the volume of assets or deposits).¹¹

As a result of the analysis, it was found that the assets of wealthy individuals held in the credit institutions make up a significant part of the resources of banks (2010: approx. 45%; 2011: approx. 42%; 2012: approx. 19%). The share of the volume of assets in the respective segment was used as a basis for assessing the risks of the volume of services.

To assess the risk of the size of an individual transaction of a wealthy customer, the size of the average deposit in a retail banking (less wealthy individual) deposit was assessed. It turned out that the average deposit of a wealthy client exceeds the deposit of a retail client up to 1000 times¹². Considering the volume of the product and the average size of the transaction, the overall risk level was assessed as high for all years (0.81 - 1.00).

The assessment of the risk of the wealthy client (the risk of the client's country of origin) was based on the share of non-resident clients, which formed the volume of assets of the wealthy client segment as follows:

2010: about 480 million euros, i.e. about 7% of the resource volume (490 customers, i.e. 11.2% of the number of customers);

⁹ See footnote 2.

¹⁰ The assessment of the vulnerability of main products and services offered in the banking sector is presented in a working document. The text provides some examples that may not be exhaustive in this context.

¹¹ The choice of appropriate metrics and ratios needs to be clarified in further research.

¹² As for wealthy customers, the average transaction volume is expected to be higher than for retail customers.

2011: about 3152 million euros, i.e. about 56% of the resource volume (536 customers, i.e. about 13.6% of the number of customers);

2012: about 403 million euros, i.e. about 16% of the volume of the resource (598 customers, i.e. 13.6% of the number of customers).

In total, the share of the assets of 4-8 customers from the low-tax region¹³ was 2-12% of the assets of non-resident customers. The growth of other non-resident wealthy clients was about 20-40 persons per year. There were no politically exposed persons (PEPs) among the customers.

Given the relatively small share of customers from low-tax areas, the level of risk based on customer residency (excluding 2011) was assessed as low (0.00 - 0.20).

Given the high level of due diligence measures applied to wealthy clients in credit institutions, including the application of applied due diligence measures according to the client's risk, the application of increased measures to non-residents, other related risks were assessed as low (0.00 - 0.20).

3.1.2.Retail deposits

The segment of retail deposits consisted of persons whose customer-based balance of liquid assets at the end of the year was less than EUR 100,000.

The assessment was based on the volume of assets of the respective sector from the volume of resources of credit institutions, taking into account, inter alia, the share of non-residents and customers registered in low-tax areas. The volume of assets of less wealthy private customers accounted for 23-28% of the volume of resources (approximately 15,000 million euros) in the consolidated balance sheet, respectively. Assessing the ratio of the average deposit balance of the respective sector to the average salary¹⁴ (the average deposit does not exceed 2 x average salary), the risks related to the volume of services were assessed as low (0.00 - 0.21).

The share of non-resident customers in the volume of assets of the less wealthy customers segment amounted to 78-95 million euros, i.e. or approximately 2% in the period under review. The share of customers from risk countries, including low-tax countries (number of customers 133-172), was less than 1% of the volume of non-resident customers and there

¹³ The share of non-residents among wealthy clients is low, therefore the risk assessment is low. However, it is known that non-resident wealthy customers generally use the legal entity form to hold assets and use services.

¹⁴ http://et.wikipedia.org/wiki/Eesti_keskmine_palk

were no PEPs, therefore the risks related to the customer's origin were also assessed as low (0.00 - 0.21).

3.1.3. Deposits of legal persons

To assess the risks associated with deposits of legal persons, the persons whose deposits (e.g. current account, overnight deposit, term deposit, current deposit, guarantee deposit, investment deposit, etc.) had a customer-based balance at the end of the year of at least EUR 100,000 or more were assessed.

The assessment was based on the ratio of the deposit balance of the respective sector to the total volume of resources¹⁵. The balances of deposits of legal persons accounted for 37-52% of the resource volume of credit institutions in the period under review.

The share of the volume of assets in the respective segment was used as a basis for assessing the risks of the volume of services, which resulted in the average risk level of the volume of the product in the range low/medium (0.41 - 0.60).

To assess the impact of the average size of the transaction, the ratio of the average deposit balance of the respective sector to the deposit of retail banking (less wealthy individual) was assessed. In the observed period the ratio of the average deposit balance to the retail banking (less wealthy individual) deposit differed approximately 35 -38 times.

To determine the risk of the customer's origin, the share of non-residents in the deposits of legal persons was estimated, which was 26-36%, respectively, while the number of non-resident depositors was about 3.6-3.9% of the number of depositors. The share of customer deposits from high-risk countries accounted for 17-20% in the period under review, including the number of depositors from risk countries for about 1.5-1.7% of the number of depositors.

Based on this, the respective risk was assessed as medium or high according to the share of deposits of legal persons of non-residents and risk countries, remaining within the range of 0.61 - 0.80.

3.1.4. Trust and asset management services

The data on asset management services provided in banking statistics differ from the data obtained from credit institutions set out in clause 2.1.1. The main difference is the different

¹⁵ The comparison uses the banking statistics of Eesti Pank, which have been published: <http://statistika.eestipank.ee/?lng=et#treeMenu/FINANTSSEKTOR>.

definition of the product¹⁶. According to banking statistics, the volume of asset management services amounted to 350-456 million euros, i.e. about 3.0-4.7% of the volume of deposits. It is hereby important to note that the volume of asset management services is constantly decreasing. The share of non-residents accounted for about 1/5 of asset management customers, including the share of customers from risk countries for about 10-16%.

3.1.5. Credit products for retail customers

The loans to individuals accounted for about 50-51% of the loan portfolio of credit institutions. Given the due diligence measures involved in issuing loans to individuals, the risks associated with the volume of this product were assessed as relatively low. The share of non-residents and customers from risk countries among retail customers' credit products was also relatively low, which is why the level of risk related to the customer's origin was assessed as low within the range of 0.00 - 0.20.

3.1.6. Credit products for small and medium size businesses

The loans of companies, state and local government companies, financial institutions as non-credit institutions accounted for about 49 -50% of the volume of loan portfolio of credit institutions, including loans of non-residents 2%. Given the due diligence measures involved in lending to the sector, the risk in this area was assessed as relatively low. The share of non-residents and customers from risk countries among the credit products of customers in the respective segment was less than 0.3%, which is why the risk of the customer's country of origin was assessed as low (0.00 - 0.20).

3.1.7. About checks, see clause 3.1.8

3.1.8. Trade finance

Given the small volume of checks and trade finance transactions, the risks associated with the volume of these services were assessed as low. Considering the fact that the average amount of payment initiated in checks is approximately 5-6 times bigger than the payment initiated in cash, it can be assumed that the risks in this area are higher and the potential risk of money laundering with these instruments is higher. The overall risk level of the product was assessed as medium (0.41 - 0.60).

3.1.9. Correspondent accounts

¹⁶ For the sake of clarity, it should be limited to one indicator only and the definition of private banking provided in clause 2.1.1 should be used.

The assessment is based on the relative number of correspondent relationships. The branches of credit institutions operating in Estonia, including Danske and Nordea, use a minimum of correspondence, as foreign settlements are made through the parent company. In Eastern relations, only the so-called TOP 10 credit institutions with high reputation and international ratings are used. Therefore, the risks are assessed as low. The number of correspondent relations has not changed significantly during the period under review. The overall risk level of the product was assessed as low (0.00 - 0.20).

3.1.10. Non-cash payments

Non-cash payments make about 99% of the initiated payments, of which electronically initiated payment orders 95-96% and card payments about 2.1-2.4%. As to the electronically initiated payment orders, internet bank and telebank payment orders account for 71.2-77.3%, respectively. The mere fact that the vast majority of payments are initiated electronically cannot be a source of additional risk. Despite the technical due diligence measures applied to electronically initiated payments, according to FATF standards, the payments initiated through new technologies (e.g. mobile payments) are associated with higher risks, therefore the potential risk of money laundering in this type of transactions was assessed as average (0.41 - 0.60).

3.1.11. Cash payments

To assess the risk of cash payments, the ratio of such payments to the total amount of domestic and cross-border payments initiated was found. Given the relatively small share of payments initiated in cash, payments initiated in cash accounted for less than 1% of payments. At the same time, the amount of the average payment initiated in cash¹⁷ is about 1/3 of the average salary, which may be a significant amount in the context of private individuals, but still remains marginal considering the total amount of payments. It is not possible to determine residency for payments initiated in cash. Nor does residency add additional risks. Thus, the overall risk level of the product was assessed as low (0.00 - 0.20).

3.1.12. Initiated international payments

The assessment is based on the ratio of the number of initiated international payments to the number of all initiated payments, including domestic and cross-border payments. Such payments accounted for about 26-31% of the total number of initiated payments in the period under review. The average initiated international payment is about 30x higher than the

¹⁷ Here and throughout the analysis process as a whole, an average has been used to analyze the data provided in banking statistics. However, the median size that would characterize the average size of a typical payment and from which individual, e.g. +/- 5-10% oversized or micropayments have been eliminated has not been taken into account.

domestic payment. It should also be taken account of additional or enhanced due diligence measures applicable to international payments that are likely to reduce the risks involved.

In case of initiated international payments, it is not possible to determine the payer's residence. The assessment has taken into account the share of the respective payments in the risk countries, which may indicate the origin of the initiator of the payment and the risk associated with it. The main risk-increasing hazards stem from the limited ability to identify the payment targets. The overall risk level of the product was assessed as low/medium (0.21 - 0.40).

3.1.13. Incoming international payments

The ratio of the number of international payments to the number of initiated payments was about 0.9 -1.0. The ratio of the average incoming international payment to the average initiated international payment is about 1.0 -1.1, which is why the potential risks have been assessed as high as in case of initiated international payments. In principle, all same circumstances apply as for initiated international payments, so the overall risk level was assessed as low/medium (0.21 - 0.40).

3.1.14. Cash exchange

The assessment is based on the turnover of foreign exchange transactions against payments initiated in cash, which in the period under review amounted to approximately 20% in Estonia before the introduction of the euro and which dropped to 2-4% from 2011 onwards. The average ratio of the size of a currency exchange transaction to the average salary was about 0.5 average salary before joining the euro and about 0.3 average salary after joining. Considering the specific risks related to currency exchange, the risk weight of the product was assessed as low/medium (0.21 - 0.40).

Summary

During the preparation of the risk assessment of the banking sector, several risk criteria were assessed and banking products were analyzed in accordance with the parameters set out in the methodology. The assessment was based primarily on the data published on the respective parameter, including the data published on the activities of the Financial Supervision Authority and the Financial Intelligence Unit, as well as data and views published in reports submitted to Moneyval on compliance with Estonian legislation and applied supervisory measures. In addition, the professional knowledge and experience of the members of the working group was used.

The assessment takes into account the data and circumstances for the years 2010 - 2012. In doing so, the estimates have not taken into account the results of Moneyval's IV evaluation report and other relevant changes that have entered into force after 2012 and which, by their nature, may affect the conclusions reached.

In case of banking products, private customers were treated in two categories: private banking, whose liquid assets at the end of the year were at least EUR 100,000 or more, and retail deposits, i.e. individuals with the liquid assets balance of less than EUR 100 000 at the year end. In addition, the deposits of legal persons were assessed. Credit products, correspondence relations and international payments of different customer groups were examined separately. In addition to the above, the electronically initiated payments (non-cash payments) and cash payments, as well as currency exchange, were also addressed by the working group. For each type of service, the work assessed different risk criteria related to the volume of the product, the average size of the transaction, the risk arising from the residence of the person performing the transaction, as well as the control measures applied.

The risk assessment of the banking sector in the visualized form has been obtained by entering the assessments found as a result of the risk criteria and product impact analysis to the relevant table. This table shows that the sector vulnerability was relatively low, amounting to 0.22-0.25 units on a scale of 0.00-1.00. At the same time, the assessment on the quality of general AML controls turned out to be relatively high, amounting to about 0.82 on a scale of 0.00-1.00 in the observed period. The indicators characterizing the quality of operations and the policies and procedures were also high, amounting to 0.82 and 0.89 units on a scale of 0.00-1.00, respectively.

The risk criteria addressed in the risk assessment largely corresponded to medium/high or high indicators, so their impact can be considered high in the context of money laundering and terrorist financing risks.

With certain derogations, the ineffectiveness of the sanctions applied must be acknowledged. Although Estonia has sufficient measures in place to prosecute individuals, the state's penal policy in relation to the prevention of money laundering and terrorist financing is disproportionate to the crime committed, as money laundering offenses are not covered by "financial crime with serious damage". The money laundering crimes are not indicated as a priority area in the development trends of criminal policy of the Riigikogu until 2018. Compared to the penalties for other offenses, the working group considers that the penalties for money laundering are rather lenient (e.g. in case of § 394 (2) of the Penal Code the minimum punishment (committing money laundering by a group, at least twice, on a large scale basis or by a criminal organisation) is 2 years' imprisonment).

In particular, based on the relevant evaluation of Moneyval round III (questioning the adequacy of the resources allocated to the supervision of anti-money laundering and anti-terrorist financing measures and the ability of supervisors to impose financial penalties in case of identified deficiencies)¹⁸, the impact of quality of supervision was assessed – medium/high.

Despite the legal measures applied to establish the transparency of corporate governance and ownership structure applied in Estonia, the assessment of this criterion was also low/ medium. The identification of the beneficial owner depends to a large extent on the availability of data based on supervisory findings. In case of complex ownership structures, it is difficult to identify the beneficial owner through the direct or indirect holding or control of shares, stocks or voting rights, including in the form of bearer shares or units. In this case, it is also difficult to identify the beneficial owner who otherwise controls the management of the legal person. However, in case of complex ownership structures, verification in another way is one of the main ways to identify the beneficial owner.

The relatively high share of non-resident customers in deposits, especially for individual credit institutions, can be considered as the main money laundering risk factors in the banking sector. The concentration of non-resident deposits in the hands of individual customers with very large balances.

During the preparation of the risk assessment of the banking sector, several errors appeared in the implementation of the methodology. First, the members of the working group found that not all standard products presented in the methodology are relevant in the context of money laundering or product volume analysis, therefore it was decided (upon agreement with the authors of the methodology) to change the list of products.

To analyze the new products described, it was decided to collect data from credit institutions as well as to use existing data on published banking statistics. In order to reduce the administrative burden on credit institutions, only five credit institutions were asked to do so. According to the feedback received during the process, the attendance of market participants in the risk assessment process had a positive effect on them. In addition, it provided an overview of the indicators and measures applied that are not published in the banking statistics. When processing the data provided in the published banking statistics, the generalized content of the data was not taken into account, e.g. in case of payments it is not possible to distinguish customer payments from all payments. In order to analyze customer payments, separate queries should be prepared in the respective databases. However, based

¹⁸ These shortcomings have been remedied by the time the risk assessment is adopted, as confirmed by Moneyval's IVth round of evaluation.

on the banking statistics, it is not possible to distinguish the customer's country of origin from the data.

Another bottleneck was finding the risk weight of the obtained data in relation to a suitable benchmark. The ratios used in the risk assessment (e.g. ratio to average remuneration, etc.) may not be the most adequate in the context of money laundering risk assessment. The members of the working group consulted with Kadri Männasoo, researcher at the faculty of economics in Tallinn University of Technology (TUT), in order to specify the metrics and suitable ratios used in the analysis. In the future, in cooperation with TUT, it is recommended to specify the ratio and metrics used.