2. Introduction: About the National Risk Assessment

2.1. General description of the Risk Assessment as an exercise

The National Risk Assessment[1] (hereinafter NRA) is an exercise to identify, assess and acknowledge the risks, threats, and vulnerabilities of money laundering and terrorist financing (hereinafter ML/TF). The NRA highlights ML/TF risks in the country and the most widespread means used to launder illicit proceeds or to fund acts of terror, and the action plan for further steps to be taken prepared based on this risk assessment, helps to direct the state's activities towards the areas where risks and vulnerabilities are high in preventing ML/TF.

The main aim of the Risk Assessment is to measure and prioritise the risks to ensure that the dedicated resources are in compliance with the risk positions ensuring efficient and effective management of the general risk position of the country. The task of the National Risk Assessment is to determine the extent of both individual and collective risks in order to highlight significant threats and vulnerabilities and to establish principles for responding to ML/TF risks.

The Financial Action Task Force[2] (hereinafter FATF) recommends that countries should conduct an NRA. Based on the Risk Assessment, an action plan, i.e. risk mitigation measures is developed, meaning that an authority or a mechanism is appointed to coordinate the risk assessment activities, resources for effective mitigation of ML/TF risk mitigation are identified, and a deadline is set for the actions to be taken. Thus, the NRA forms the main basis that helps to implement the risk based approach to the ML/TF prevention. This risk assessment is used for analysing circumstances and situations that need improvement at the national level, more resources from the state and private sector entrepreneurs for preventing risks, but also situations where adding additional resources is neither reasoned nor practical.

The previous NRA which was conducted in 2015 covered the years between 2011 and 2013 and it was carried out according to the World Bank methodology. This NRA includes the years 2017-2019 and is carried out in accordance with the "National money laundering and terrorist financing prevention risk analysis methodology" prepared at the request of the Government Office by PriceWaterhouseCoopers. The methodology is adjusted to Estonian conditions. The project was financed under priority axis 12 "Administrative Capacity" measure 12.2 "development of Policy-Making Quality" of the 2014-2020 European Union Cohesion Funds programme financed by the European Union Social Fund. The project initiator and partner was the Ministry of Finance.

The Estonian national money laundering and terrorist financing risk assessment is prepared according to paragraph 11 of the Money Laundering and Terrorist Financing Prevention Act (hereinafter MLTFPA) and its aim is to:

1) provides for the needs of drafting and amending anti-money laundering and countering the financing of terrorism legislation, other regulations of the field and related fields as well as guidelines of supervisory authorities;
2) specifies, among other things, the sectors, fields, transaction amounts and types and, where necessary, countries or jurisdictions with regard to which obliged entities must apply enhanced due diligence measures and, where necessary, clarifies the measures;

[1] NRA – National Risk Assessment

[2] Financial Action Task Force (hereinafter FATF) – an anti-money laundering task force operating between democratic governments that develops standards and methods for the fight against money laundering and terrorist financing and promotes the respective policies. FATF has 35 members: 33 states and governments and 2 international organisations, FATF also has more than 20 supervisors – five regional bodies similar to FATF and more than 15 international organisations or bodies. Currently, Estonia is not a member of FATF. FATF has two main tasks: to develop international standards (recommendations) and to observe its members' progress in work methods and counter measures related to money laundering and terrorist financing.

3) specifies, among other things, the sectors, fields, transaction amounts and types whereby the risk of money laundering and terrorist financing is smaller and where it is possible to apply simplified due diligence measures;
4) gives instructions to the ministries and authorities in their area of government regarding allocation of resources and setting of priorities for anti-money laundering and countering the financing of terrorism purposes.

According to an FATF recommendation, a clearly dedicated and authorised institution, organisation, or specially formed task force should be responsible for the management and coordination of the national risk assessment process. **The governmental anti-money laundering and counter terrorist financing committee** (hereinafter the AML/CFT Committee)[3] is responsible for coordinating the NRA. The committee's activities include both forming the money laundering and terrorism financing prevention policy as well as coordinating the mapping of national risks and preparing the action plan for their mitigation.

The Committee chaired by the Minister of Finance includes the chancellors of the **ministries** responsible for the relevant fields, as well as representatives from the **Tax and Customs Board, Prosecutor's Office, Police and Border Guard Board, Financial Intelligence Unit** (hereinafter FIU), **Internal Security Service, Bank of Estonia (Eesti Pank),** and **Financial Supervision Authority**. Meetings of the Committee take place when needed but not less than once every four months. The exact roles and tasks of the Committee are provided in the MLTFPA. The Committee prepares measures and an action plan for mitigating the risks determined in the NRA, appoints the institutions responsible for mitigating the risks and follows the progress of implementing the action plan. **The Ministry of Finance** is responsible for organising the work of the governmental anti-money laundering and counter terrorist financing committee's[4] and publishes the general results of the risk assessment on their website.

The NRA Steering Committee, which is overseen by the governmental AML/CTF Committee, prepares the NRA and the plan for implementing the measures and activities to mitigate the risks identified therein, i.e. the action plan. This committee organises, plans and coordinates the process of performing the risk assessment in accordance with the NRA development methodology. The steering committee also forms working groups, gives them tasks and follows their performance, among else, helps to organise seminars and interviews, gathers the necessary data and information, and leads the preparation of the NRA report. The NRA Steering Committee communicates and consults with the working groups participating in the project at a determined interval during the entire risk assessment process and reports on the performed tasks and passed stages to the governmental AML/CTF Committee, highlighting both the achieved results as well as the shortcomings in methodology and cooperation identified in the process. The Steering Committee submits to the governmental AML/CTF Committee the NRA report and action plan for approval.

Sectoral risk assessment starting points are taken from various sources, incl. the results of the last NRA, national statistics (e.g. Financial Intelligence Unit's yearbooks) and international guidelines. The aim of sectoral risk assessment is to gain an overview of the money laundering and terrorist financing risks in each respective sector of the particular state. The sectoral risk assessment results serve as instructions for obligated entities on the risks in their sector and these will be followed in organisation level risk assessments.

[3] The governmental AML/CFT Committee was formed on 19 April 2018 with Regulation No. 34 of the Government of the Republic.
[4] Hereinafter the governmental AML/CFT Committee

2.2. Used definitions and abbreviations

2.2.1. Definitions

Money laundering

According to the Money Laundering and Terrorist Financing Prevention Act (MLTFPA):

§ 4. Money laundering:

1) Money laundering is one of the following activities in respect of the property derived from criminal activity or property obtained instead of such property:
   1) the conversion or transfer for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;
   2) the acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein;
   3) the concealment or disguise of the true nature, source, location, manner of disposal, relocation or right of ownership or other rights related to the property;

Money laundering is a process used by criminals to conceal or disguise the identity, original ownership, and source of funds acquired through criminal conduct. The final intention of money laundering is to make it seem like the process has started from the legitimate source.

In general, money laundering is done in three stages:

- **Placement** is the first stage of ML when an individual places proceeds gained from illegal activity into the financial system. A classic method of ML is known as structuring, whereby cash is broken up into smaller deposits (amounts below the AML reporting requirements) in order to avoid the suspicion of ML. Another method is trade-based ML, which involves criminals using legitimate companies to disguise the movement of illicit funds by, inter alia, over-invoicing or under-invoicing the value of goods.

- The main purpose of the **layering** stage is to lose connection between the illegal money and its source. This is accomplished through the use of sophisticated multilayer financial transactions to make tracing transactions difficult. The money can electronically move between different accounts and to different countries. Criminals also use the money to buy financial assets such as stocks.

- **Integration** is the final stage of ML where the money is returned to the criminal from what seems to be a reputable source, mainly through the banking systems. A common method is the sale of property to reintegrate laundered money back into the economy (i.e. criminals use shelf and/or shell companies to buy property and the proceeds from the sale of the property appears as legitimate). An alternative method for criminals is to set up shell companies in countries where corporate secrecy is strictly protected by the law.

2. Terrorist financing

According to the MLTFPA:

§ 5. Terrorist financing

Terrorist financing means the support of terrorist offenses and activities aimed at committing them as well as the financing and supporting of travel for the purpose of terrorism within the meaning of §§ 237^3 and 237^6 of the Penal Code.

Terrorist financing involves financial support, in any form, of terrorist activities. The purpose of TF is to transfer money that may be legal or illicit in origin to support terrorism. Financial terrorists usually do so in smaller amounts than in the case of ML using a variety of methods, which makes their detection and prevention more difficult. Some of the TF methods include moving money through unregistered money

services platforms and international ATM transactions, through new unestablished online payment systems or through charities and non-profit organisations. One of the distinctions between TF and ML is the purpose of the investigation. The investigation of TF is carried out to prevent individuals from accessing the funds that could finance future terrorist activities. On the other hand, a traditional ML investigation is carried out in order to link the funds to a criminal act that has already taken place and to leave the criminal without the economic benefits received from the criminal means. Both ML and TF are criminal offences and are detrimental to the economy and society as a whole.

3. Proliferation Financing

Components of weapons of mass destruction – several poisons, precursors for chemical weapons or explosives – are provided in the Common Military List of EU. For example ML7: "Chemical or biological toxic agents, riot control agents, radioactive materials, related equipment, components and materials" and ML8: "Energetic materials and related substances". The EU List of dual-use items includes, for example, nuclear materials, facilities, and equipment.

Proliferation Financing (PF) is an act of providing funds or financial services to manufacture, acquire, transfer, and export technology, services, or expertise used for nuclear and chemical weapons in breach of national and international laws. Proliferation financing can, therefore, be terrorism financing where financial support is provided to terrorist organisations. It can also be financing from a state where the financing aims to provide a state with a weapon of mass destruction. These transactions may appear as normal commercial activity and flow through financial channels although they are structured to hide the source of funds. Individuals can thus benefit from facilitating these movements. The financing of proliferation can contribute to global instability and potentially catastrophic loss of life if weapons of mass destruction are developed and deployed. Countries must, therefore, be able to identify and understand the risks of ML, TF, and PF, and apply preventive measures.

4. Threat

In the context of money laundering and terrorist financing, threat means the possibility that the illegally derived resources end up in the state economy or the financial means are used for supporting terrorism. Income from different types of organised crime may end up in economy via various channels. These channels may be different foreign states or economic sectors who are partners in cross-border activities. The threat is the derivative of the probability of the event and the consequence.

5. Consequence

Consequence is the impact of the event (positive/neutral/negative).

6. Probability

Probability is defined as the chance of an event occurring.

7. Vulnerability

Vulnerability means the weakness of a state's anti-money laundering and terrorist financing prevention system or national control measures, which enable using options for money laundering or terrorist financing. A vulnerability may be unsuitable policy or control measures that are not followed or the following of which is not supervised.

8. Risk

Risk is the realisation of a possible threat in case of vulnerability.

9. Risk management strategy and their types

Risk management strategies form an important part of the risk assessment process. A suitable risk management strategy is selected based on priorities so that the major risks would gain the most attention. In determining the suitable risk management strategy, it is important to consider the state's risk tolerance, i.e. the risk level of money laundering and terrorist financing the state is willing to accept. To ensure efficient management of money laundering and terrorist financing risks, it is important that the scope and timing of the risk management strategy complies with the specific money laundering or terrorist financing

risk level. For example, higher risk levels may require more immediate mitigation measures or point out systematic risks that require extensive measures over a longer period. In the case of a high risk level the suitable mitigation measures generally require developing policies and taking extended measures. A lower risk level requires less measures, for example monitoring, or if the risk remains within the state's risk tolerance, it could also be accepted.

Typical risk management strategies are avoiding, mitigating, and accepting:

- **Accepting** – accepting a risk does not alleviate the impact of the risk but it is nevertheless a recognised strategy. The risk and its consequences are accepted and specific measures are not considered necessary. This is a good strategy in the case of money laundering and terrorist financing risks that have an insignificant impact on the state. This strategy is usually opted for if other risk management strategies would be too expensive compared to the risk price. Solution plans should be prepared to tackle the consequences of money laundering and terrorist financing risks realising.
- **Avoiding** – avoiding a risk is the opposite of accepting a risk. This measure eliminates the possibility for the risk to realise by eliminating the risk source. For this, measures must be taken to stop and end the activity that causes the specific risk. This is a good strategy in the case of money laundering and terrorist financing risks that have potentially a great impact on the state.
- **Mitigating** – mitigating a risk is probably the most common risk management strategy. Certain measures are taken for mitigating the risk, which will reduce the state's vulnerability. The probability or impact of the risk is reduced by mitigating control measures.

In the context of the money laundering and terrorist financing risk, avoiding and mitigating are the most appropriate strategies.

10. Obliged entity in the meaning of the MLTFPA

An obliged entity is a person to whom the requirements and obligations provided in the MLTFPA apply, mainly in terms of performing due diligence measures when preventing money laundering and terrorist financing.

2.2.2. Used abbreviations

Authorities:

ISS – Internal Security Service

TCB – Tax and Customs Board

FIU – Financial Intelligence Unit

CRIS – Centre of Registers and Information Systems

Laws:

PC – Penal Code

MLTFPA – Money Laundering and Terrorist Financing Prevention Act

ISA – International Sanctions Act

Other:

KYC – Know Your Customer principle

AR – annual report

REA – register of economic activities

CEA code – classification of economic activities

PF – proliferation financing

NRA – National Risk Assessment

ML – money laundering

AML/CTF – anti-money laundering and counter terrorist financing

TF – terrorist financing

FIU notification types:

STR – suspicious transaction report (ML)

UAR – unusual activity report (ML)

UTR – unusual transaction report (ML)

TR_UTR – unusual transaction report (TF)

TFR – terrorist financing report

ISR – international sanctions report

CTR – cash transaction report

2.3. List of institutions participating in the preparation of the Risk Assessment and working groups

In the process of the National Risk Assessment the national risks related to money laundering and terrorist financing prevention both at the national level and those related to activities in sectors were assessed. For this, **two national level working groups were established:**

- **Country-wide threats working group** that identified the threats from the state's geographical position and from specific predicate offences, but also sectoral threats from the aspect of money laundering and terrorist financing.
- **Country-wide vulnerabilities working group** that identified the state's vulnerabilities, primarily by areas which the FATF identified as key goals in the effective AML/CFT country-wide framework.

For executing this NRA, the preparer of this methodology has proposed **eight sectors** that cover all the obliged entities according to the Estonian MLTFPA:

1. **Financial sector** and its subsectors: **credit institutions, financing institutions, (life) insurance companies, investment associations, payment service providers, currency exchange offices.**
2. **Real estate agents' sector**
3. **Financial technology sector** (hereinafter FinTech sector) and its subsectors: virtual currency service providers, crowd funding service providers
4. **Company service providers sector**
5. **Non-profit organisations sector** (hereinafter NPO sector)

6. **Dealers sector**[5]
7. **Gambling sector**
8. **Other designated non-financial businesses and professions** (hereinafter professionals' sector) and its subsectors: attorneys, auditors, bailiffs, notaries, trustees in bankruptcy, accountants, providers of other legal services, pawnbrokers.

Eight sector working groups were formed to assess the threats and vulnerabilities of each above-mentioned sector and subsector, the groups included experts in the field, specialists and market participants from the public and private sector. The Ministry of Finance served as the common leading institution for all the working groups that also coordinated the preparation of the NRA and the subsequent action plan.

Participating in the NRA was mandatory for the **public sector**. Among others, the participants of the NRA include from the public sector:

- Eesti Pank (Bank of Estonia),
- Financial Supervision Authority,
- Ministry of Justice,
- Internal Security Service,
- Tax and Customs Board,
- Police and Border Guard Board,
- Prosecutor's Office,
- Ministry of Finance,
- Financial Intelligence Unit,
- Ministry of the Interior,
- Ministry of Foreign Affairs.

Participation of the **private sector** in the NRA is important and strongly recommended. The private sector may be represented by the associations of the respective fields and by obliged entities, primarily the most significant participants of the Estonian market. Their participation is important to raise awareness, because the obliged entities are one of the most important beneficiaries of the NRA. In many countries, participation of the private sector has helped to advance the dialogue with the public sector and the anti-money laundering and terrorist financing prevention related cooperation. This NRA involves the private sector to a larger extent than the exercise of 2015, because the methodology of this exercise requires this. Participating in the NRA gives the companies significant input for preparing their own risk assessment. Among others, the following market participants from the private sector took part in preparing the NRA:

- Law office TRINITI,
- Betsson Group,
- Bondora AS,
- Creditinfo AS,
- Estateguru OÜ,
- Fundwise,
- ITL,
- Njord Law,
- Olympic Entertainment Group,
- Placet Group OÜ,
- PwC Legal,
- Sorainen,
- Tavexwise,
- Uus Maa real estate agency,
- xChange.

[5] Dealers of high-value and easily tradable "lifestyle" goods, also dealers of cash and cash-like assets

Additionally, **umbrella organisations** and **professional associations** of various fields of activity participated in the NRA process:

- Estonian Auditors' Association,
- Estonian Bar Association,
- Estonian Gaming Operator Association,
- Estonian Lawyers Union,
- Estonian Chamber of Commerce and Industry,
- Association of Real Estate Companies of Estonia,
- Estonian Banking Association,
- Network of Estonian Nonprofit Organizations,
- Finance Estonia,
- Chamber of Estate Agents,
- Estonian Chamber of Bailiffs and Trustees in Bankruptcy,
- Chamber of Notaries.

Representatives from all the aforementioned professions, companies, and organisations participated in the working groups formed for the NRA, by sharing their professional knowledge, experience, and expert opinions, and by contributing to the preparation of the report. Nearly 80 people participated in the current NRA process.

The Ministry of Finance would like to thank everyone who contributed to the process of this NRA.

2.4. Method of the conducted risk assessment

2.4.1. Risk assessment stages

The following stages were passed when preparing this risk assessment:

1. **Collecting statistics** via data enquiries to competent institutions (Bank of Estonia, Ministry of Justice, FIU, TCB, Financial Supervision Authority, commercial register, etc.).
2. **Processing the literature** concerning money laundering and terrorist financing prevention, incl. **SNRA 2017 and 2019 mandatory analysis.**
3. **Conducting a sector-specific survey** among the market participants of the segments covered in the exercise.
4. **Analysing the information gathered** in the three previous stages and **holding discussions in working groups**.
5. **Assessing the threats and vulnerabilities** in corresponding methodical tables.
6. Preparing the **report** and making proposals for a further **action plan**.

2.4.2. Collecting statistics

The NRA process started with collecting data and information. The aim was to identify money laundering and terrorist financing risks to analyse. Gathering data from national statistics and elsewhere is of paramount importance for establishing a strong evidence-based basis for assessment and to ensure more objective assessment. Evidence-based practice is a mandatory element of risk assessment based on the risk-based approach. Collecting the statistical data needed in the exercise was done centrally through the Ministry of Finance. The need for data inquiries was obtained from the NRA steering committee and all working groups. During the process, inquiries were made from the following institutions:

- Estonian Bar Association, Estonian Auditors' Association, Estonian Chamber of Bailiffs and Trustees in Bankruptcy, Chamber of Notaries – information was requested on the umbrella organisation work in the field of money laundering and terrorist financing, organisation membership, supervision (if any) and control measures and training provided.
- Bank of Estonia – data was requested on incoming and outgoing cash flows per countries, client base of investment associations (share of legal persons who are residents and non-residents in the

investment structure).

- Financial Supervision Authority – data was requested on issued precepts, supervisory activities, identified breaches, and sentenced punishments.
- Ministry of Justice – various criminal statistics on convictions, asset seizures and confiscation in ML and TF offences was requested.
- TCB – data was requested on cash declarations per countries, tax frauds, received and paid donations declared by NPOs.
- FIU – data was requested on statistics on reporting per sectors, forwarding of gathered materials, supervisory activities, made and received outside inquiries and asset restrictions, etc.
- Commercial register (CRIS) – lists of market participants per Classification of Economic Activities (CEA) codes were requested for the sector-specific survey conducted within the exercise, sales revenue information of market participants, information on the member of the board and/or owner of a legal person who is not a resident per sector.

It was not possible to gather all the requested data. For example, it was identified during the process that criminal statistics on different sectors and subsectors is not kept, that such data can be gathered only manually. A similar problem emerged with court decisions in money laundering crimes, which in the end were reviewed one by one and then the necessary information was obtained. The working groups made respective proposals to improve the situation in lacking statistics and data that is hard to obtain. Without statistical information, it is difficult to assess the actual situation and to draw objective conclusions. Proposals concerning data collecting and keeping statistics ended up in the action plan to ensure that for the next risk assessment period, the necessary data would be gathered and available in an automatic format without the need for manual work.

Also, each working group has gathered the sector-specific data for their own assessment, if necessary, via its working group members, the majority of whom were representatives of various government authorities.

2.4.3. Sector-specific survey

In the assessment it is also important to gather information by consulting the respective stakeholders to learn the economic, political, social, legal, and technological risk factors. Market participants of the respective sector were involved in each working group. But, for this NRA to be more objective, a sector-specific survey on the topics of money laundering and terrorist financing prevention was conducted among the market participants of sectors participating in the exercise. A representative sample of obliged entities was selected who represented their sector to a sufficient extent and provided a comprehensive overview. Before starting the survey, the Ministry of Finance contacted the following professional associations and umbrella organisations to inform via them the market participants of the ongoing risk assessment, explain its content and importance for the country and also asking to be proactive in conducting the survey, thus contributing to the preparation of an objective risk assessment. The letter of notification was sent to the following organisations:

- In financial sector: Estonian Banking Association, Estonian Leasing Association, Estonian Insurance Brokers Association.
- In real estate agents' sector: Association of Real Estate Companies of Estonia, Chamber of Estate Agents.
- In FinTech sector: Finance Estonia, Estonian Cryptocurrency Association.
- In professionals' sector: Estonian Bar Association, Estonian Auditors' Association, Association of Estonian Accountants, Estonian Chamber of Bailiffs and Trustees in Bankruptcy, Chamber of Notaries.
- In NPO sector: Network of Estonian Nonprofit Organizations
- In dealers' sector: Estonian Chamber of Commerce and Industry, Estonian E-Commerce Association, Estonian Traders Association, Estonian Association of Cars Sales and Service Companies, Estonian Cosmetologists Association, Estonian Hairdressers Association.
- In gambling sector: Estonian Gaming Operator Association

Since all the market participants are not members of the professional associations or umbrella organisations of their sector, the Ministry of Finance published a press release on their website in May 2020 titled "The Ministry of Finance is inviting respondents to participate in the money laundering prevention risks awareness survey".

The aim of the sector-specific survey is to give the market participants an opportunity to assess the money laundering and terrorist financing risks of each sector. The questionnaires tackle various topics, for example sector-specific risks, sufficiency of existing legislation and efficiency of supervision, market participants' experience in the field of money laundering and terrorist financing prevention. The questionnaire responses provide a market level view on the estimated levels of threats and vulnerabilities. The depth of the questionnaire depended on the sector's characteristics and responses given, because specifying questions were added in the case of certain answers.

Each sector's working group adjusted the standard questionnaire developed by the methodology creator according to sector's characteristics. Several sectors used different questionnaires also per subsectors, a detailed overview is given of this in the sectors' vulnerability chapters.

The most extensive questionnaire was in the FinTech sector and the shortest in the dealers sector.

This survey was conducted anonymously in the online[6] survey portal LimeSurvey, meaning an optimum convenient solution for the respondents to reduce the administrative burden of the obliged entities and the law-abiding costs related to the ongoing NRA process. The questionnaires were available in Estonian and English. The survey was conducted between May and August 2020. 22,027 survey invitations were sent to the market participants of 8 sectors who were chosen for the exercise at random. The sample size[7] of each sector and its subsectors depended on the number of market participants. The confidence level was 95% and the limit of error was 5%. The market participants lists were taken either from the commercial register information database according to the respective CEA code[8] or from the register of economic activities (REA), if it was a licensed area of activity[9]. In order to consider the survey feedback as objective, the minimum number of required responses was fulfilled using for this a sample size calculator, which was achieved thanks to repeated reminders sent to the market participants to participate in the exercise. The details of the survey conducted in each sector are highlighted at the beginning of each sector's chapter.

The results of the survey conducted helps to understand better the skills and experience of the market participants in the area of money laundering and terrorist financing prevention. Immediate feedback from the market participants reflects the actual situation, highlighting the existing shortcomings in cooperation with supervisory authorities and between market participants, shedding light on new fraud schemes and on weaknesses in the control systems.

2.4.4. Analysing the gathered information and conducting discussions in working groups

Different stakeholders were represented in the working groups – law enforcement authorities, supervisory authorities, obliged entities of all sectors, i.e. private sector market participants, representatives of professional associations, i.e. umbrella organisations and other experts needed to discuss the Estonian money laundering and terrorist financing risk environment. The working group members discussed the available information, legislation in force and feedback of the surveys, assessed the efficiency of supervision and criminal proceedings and made proposals for determining the estimated threat levels and vulnerabilities.

[7] Sample size calculator https://www.syg.edu.ee/oppematerjalid/uurimistood_referaadid/valimimaht.html
[8] Market participant's main area of activity met the CEA code of the sector or subsector involved in the exercise
[9] Certain areas of activity require owning a license issued by the FIU or the Financial Supervision Authority

2.4.5. Assessing threats and vulnerabilities

Risk assessment modules

3 different risk assessment modules were used for assessing the national threats, national vulnerability and sector vulnerability. The main aim was to determine the threats and vulnerability related to money laundering and terrorist financing – efficiency of money laundering and terrorist financing prevention control measures applied at the state and sector levels in fighting money laundering and terrorist financing.

According to the methodology the state had to use the NRA steering committee and its various working groups involved in the risk assessment process to discuss and determine the weights of various assessment elements, which was done several times.

National threats

State threats risk assessment module is made up from three different assessment levels:

- sectoral level
- predicate offence based level
- geographical cashflows based level

In all the aforementioned risk assessment modules, parallel assessments were made from to the money laundering and terrorist financing aspect.

To determine the national threat level, the following weights are given by default:

- sectoral threat level 40%
- predicate offence threat level 40%
- geographical threat level 20%

The methodology did not reason the exact logic of the provided weights and permitted to make changes in the weights, based on the actual situation in the country and the opinions of the experts involved. The NRA steering committee decided to apply the following weights to determine the **money laundering threat levels**:

- aggregate threat level of sectors 60%
- aggregate threat level of predicate offences 20%
- aggregate geographical threat level 20%

The above-mentioned change in weights was made as the state threats working group concluded in the working process that predicate offences committed in Estonia do not have as much relevance in general and instead the sectorial threat level assessments have a greater role.

The NRA steering committee decided to apply the following weights for finding the **terrorist financing threat level**:

- aggregate threat level of sectors 33%
- aggregate threat level of predicate offences 33%
- aggregate geographical threat level 33%

In the risk assessment process it was concluded that in the case of terrorist financing, none of the provided threat levels are determining because terrorist financing may take place in any sector for any sum of money and the region of financing may not have a crucial meaning either.

On all three threat levels, two different aspects are considered in the quantification of the threat risk – the probability for threat realisation and the consequence of threat realisation. The assessment of the probability and consequences while measuring threats, enables better to identify and rank main inherent threats.

Probability is defined as the chance of an event occurring. The probability of a threat occurring is measured on a scale from 1 to 5:

- 1 – low: Event likely to occur once in three or more years
- 2 – below average: Event likely to occur on an annual basis
- 3 – average: Event likely to occur more than once on an annual basis, but not on a monthly basis
- 4 – above average: Event likely to occur on a monthly basis
- 5 – high: Event with an ongoing effect or occurring on a daily basis

A consequence is defined as the negative impact of the event occurring. The consequence of a threat occurring is measured on a scale from 1 to 5, according to what impact is made on the national security systems, economy, state's reputation and society:

- 1 – very low, i.e. insignificant impact
- 2 – low
- 3 – average
- 4 – high
- 5 – very high

Detailed explanations of the points on the above-mentioned scale are available in annex 2.

The threat is calculated as the weighted average of the probability and consequence, so that the assessors can calibrate the weights of the probability of threat occurring and consequence according to their estimated importance in the total occurrence of the threat. The total of the weights of probability and consequence must be 100%. In the methodology, the default weights of money laundering and terrorist financing probability and consequence are 45 and 55, respectively.

The NRA steering committee decided to use the probability vs. consequence default weights of 45/55 provided in the methodology only when assessing the money laundering threats. When assessing terrorist financing, the decision was to use the consequence vs. probability weights as 10/90 for the following reasons:

- In the case of terrorism and its financing, the worst possible consequence can always be the same, i.e. unpredictable and extremely harsh, that is, with human casualties, which can be assessed only with maximum on the 1-5 scale, also the consequence of an act of terrorism cannot depend on other factors. Since the worst possible consequence is a constant in the case of every sector, it does not have a direct impact on the final score.
- The probability indicator is changing because it depends on many circumstances. Different factors impact committing terrorist financing: people, society, political situation, the specific sector and economy as a whole, state's comprehensive terrorism threat level, international cooperation and contact with other countries, settlement options (cash, cryptocurrency), share of risk groups in the specific sector, international cash flows passing the sector, and others, which is why its importance in assessing the threat is considerably higher.

Accordingly, the consequence of terrorist financing is marked with 5 points for all sectors and geographical regions participating in the exercise.

National vulnerability

National vulnerability risk assessment module is built based on the FATF effectivity indicators or Immediate Outcomes[10] (hereinafter IO). Based on the methodology used, state-level control measures of 11 effectivity indicators and four additional aspects, stakeholder-level control measures and general IT control measures in terms of their design efficiency as well as the functional efficiency were assessed per FATF IOs.

[10] IO – Immediate Outcome

The following default weights are provided for determining the national vulnerability level: sectoral vulnerability level 40% and national vulnerability level 60%. The national vulnerability level is higher than the sectoral vulnerability level because a strong money laundering and terrorist financing prevention system at the national level supports the resistance of respective sectors as well. The NRA steering committee decided to follow the methodology in this case.

Sectoral vulnerability

The following sources were used as bases for assessing the vulnerability of the sectors included in the exercise:

- sectoral literature concerning ML and TF prevention, incl. SNRA 2017 and 2019 country specific recommendations, processed by the working group;
- results of the conducted surveys, i.e. market participants' feedback;
- opinions and experiences of the working group members as experts and specialists in their fields.

The methodology provided for assessing the vulnerability of sectors, considering the characteristics of each sector and its subsectors and the following assessment modules for sectors were provided:

- dealers
- professionals
- FinTech
- gambling
- NPOs
- real estate agents
- financial services: credit and financing institutions, insurance companies, investments firms, payment service providers and currency exchange offices.

All sectoral vulnerability assessment modules were adjusted according to the sector's characteristics. The subsector of pawnbrokers is in the professionals sector, but it was assessed using the assessment module used for assessing the financial sector's subsectors, because a pawnbroker has more in common with a financing institution than with other professionals. The rest of the professionals sector subsectors were assessed using the same professionals sector module. The exact same module was also used for assessing the company service providers sector because it has a lot in common with the professionals. In the FinTech sector the virtual currency service providers and crowdfunding companies were assessed separately, but using the same module. Regardless of the fact that in the NPOs sector the survey results were differentiated in four subsectors, the assessments were given jointly.

The method for finding the money laundering and terrorist financing vulnerability level of the sector is the same for all the sectors. When analysing the vulnerability of sectors, the existing control measures and their implementation at three levels (national, stakeholders[11] and IT control) were assessed. The vulnerability of each sector was assessed in the following categories both from the aspect of ML and TF:

- legal framework, incl. comprehensiveness of the ML/TF prevention legal framework and its incorporation in sector-level policies
- quality of supervision, incl. the existence and implementation of sanctions, effectiveness of supervision and practices
- management commitment and leadership, incl. the availability and effectiveness of entry controls, integrity of staff
- effectiveness of compliance systems and reporting, incl. the effectiveness of compliance systems, the effectiveness of the monitoring and reporting of suspicious activity
- quality of the customer due diligence (CDD) framework, incl. the availability of reliable mechanisms for identifying persons and the availability of information concerning actual beneficiaries
- quality of identifying terrorist financing[12], incl. identifying terrorist financing and it's reporting

[11] Level of professional associations and umbrella organisations

[12] The NRA steering committee made a methodical decision in terms of this category – this category was assessed only from the

effectiveness
- quality of sanctions detection, incl. the efficiency of identifying sanctions and reporting of related incidents
- quality of identifying risks characteristic to the sector and its effectiveness
- quality of the responses to the risks identified during previous assessments and its effectiveness[13]

The specificity between sectors and subsectors was the quality of the identification of the sector-specific risks, that was the main reason why the modules were differentiated per sectors.

In the above mentioned assessment categories, various aspects were assessed and in the case of each aspect its planned and actual effectiveness was determined as well as its importance (weight) in the ML and TF assessment:

- The planned effectiveness scale was 0 to 4 where 0 – control does not exist, 1 – control exists but is insufficiently designed, 2 – control exists and is reasonably designed, 3 – control exists and is well designed, 4 – control exists and is perfectly designed.
- The actual effectiveness scale was 0% to 100% where 0% meant that control is not followed and/or enforced, 25% – control is followed inconsistently and not enforced, 50% – control is followed reasonably and enforced to a minimal extent, 100% – control is fully followed and enforced without any exceptions.
- The weight scale was 0 to 3, where 0 – no impact, 1 – low impact, 2 – average impact, 3 – high impact.

The assessment module tables included formulas by the methodology creator to find each sector's ML and TF vulnerability level. Thus, after filling in all the fields of the assessment module, each working group obtained the assessed vulnerability level indicators. When filling in the assessment modules, notes were also taken in the respective table, which were followed in assessing each category (effectiveness, impact, etc.). The filled in assessment modules are each working group internal work documents, helping to prepare in a structured format the part of the report concerning their sector.

Weights of sectors

The exercise methodology is prepared so that the greatest emphasis is put on the riskier sectors, while relieving the administrative burden for less riskier sectors that were not included in the exercise. According to the methodology, the risky sectors included in the exercise, that cover all obliged entities in the meaning of MLTFPA, make up 100%. To find the national threat and vulnerability level, it was necessary to also consider the average indicators of the sectoral threat and vulnerability, whereas each sector's indicator had to be considered according to its share. However, since the sectors were of varying sizes and importance, the NRA steering committee had to decide on the weights of sectors. Here, the methodology suggested to rely on, for example, the number of market participants and/or obliged entities, economic impact, importance for the state, etc. Thus, based on the aforementioned, the NRA steering committee had the chance to adjust the weights to their own discretion considering various components and aspects.

The sector weights were identified based on the components indicated in the table below (see Table 1) and coefficients attributed to them using the method which was prepared in the risk assessment work process (the PwC methodology did not provide for such or another solution for finding the weights; however, it was suggested to consider each sector's turnover volume, market participants number, etc.):

perspective of terrorist financing, meaning this category was not assessed from the ML perspective and was not considered due to its controversial nature

[13] This category was assessed and considered only in the case of the following sectors that passed the NRA 2015: real estate agents, dealers (incl. sellers of precious metals), insurance subsector or finance sector

Table 1. Weights of sectors

Sector	Share	Sales revenue coefficient [14]	Market participants number coefficient [15]	Obliged entities share coefficient [16]	Cash flow coefficient[17]	Total
Financial sector	25.2%	1.00	0.50	1.00	6.00	8.50
Real estate agents	6.7%	0.50	0.25	1.00	0.50	2.25
FinTech VC[18]	11.1%	0.25	0.50	1.00	2.00	3.75
FinTech CF[19]	8.1%	0.25	0.25	0.25	2.00	2.75
Dealers	15.6%	2.00	1.00	0.25	2.00	5.25
Gambling	8.1%	0.50	0.25	1.00	1.00	2.75
NPOs	9.6%	1.00	1.00	0.25	1.00	3.25
Trust and company service providers	6.7%	0.25	0.50	1.00	0.50	2.25
Professionals	8.9%	0.50	0.75	0.75	1.00	3.00
Total	100%					33.75

Sector weights were determined based on the following indicators:

- sales revenue – sector market participants' sales revenue for 2019 which is presented in the annual reports submitted to the commercial register
- number of market participants – the number of legal persons in the sector (based on the CEA code or REA activity license)
- share of obligated entities – the share of obliged entities in the meaning of MLTFPA, i.e. is the entire sector covered or does the obligation applies only on certain conditions (e.g. in the case of dealers with large cash transactions)
- cash flow through the sector – the volume of cash flow that circles through the sector (e.g. in the case of real estate agents the volume of real estate transactions, in the case of financial sector the volume of money moved via bank accounts)

Since a comparison of numerical data would have created sizeable differences among various sectors (e.g. 20 market participants in the gambling sector vs. ca 7000 market participants in the professionals sector vs. ca 40,000 market participants in dealers sector), it was decided to replace the numerical data with relative coefficients which supported comparing the data.

The financial sector includes several subsectors: credit institutions, financing institutions, insurance companies, investment associations, payment service providers, and currency exchange, which in total make up 100%. The methodology described in the table below was used in determining the weights of subsectors, which was done during the risk assessment work process:

[14] 2.00 – income leader, 1.00 – 2nd place income leaders, 0.5 – 3rd place income leaders, 0.25 – lesser income earners
[15] 1.00 – much, 0.75 – less than much, 0.5 – on average, 0.25 – little
[16] 1.00 – all, 0.75 – majority, 0.25 – minority
[17] 6.00 – major, 2.00 – large, 1.00 – average, 0.5 – small
[18] Virtual currency service providers
[19] Crowdfunding service providers

Table 2. Weights of subsectors of the financial sector

Subsector	Share	Sales revenue coefficient [20]	Market participants number coefficient[21]	Obliged entities share coefficient [22]	Cash flow coefficient[23]	Total
Credit institutions	51.6%	5.00	0.50	1.00	10.00	16.50
Financing institutions	8.6%	0.25	1.00	1.00	0.50	2.75
Insurance companies	7.0%	0.50	0.25	0.50	1.00	2.25
Investment associations	14.1%	1.00	0.50	1.00	2.00	4.50
Payment service providers	11.7%	0.25	0.50	1.00	2.00	3.75
Currency exchange	7.0%	0.25	0.50	1.00	0.50	2.25
Total	100%					32.00

The subsector weights were determined based on the following indicators:

- sales revenue
- market participants number
- share of obliged entities
- cash flow through the sector

The professionals sector includes multiple subsectors: notaries, accountants (incl. tax advisors), attorneys, other legal service providers, auditors, trustees in bankruptcy and bailiffs, pawnbrokers, that in total makes up 100%. The methodology described in the table below was implemented in determining the weights of subsectors, which was done during the risk assessment work process.

Table 3. Weights of subsectors of the professionals' sector

Subsector	Share	Market participants number coefficient [24]	Obligation occurrence coefficient [25]	Transaction witnessing coefficient [26]	Transaction interference coefficient [27]	Daily role coefficient [28]	Total of all coefficient input
Notaries	19%	0.50	0.75	2.00	2.00	3.00	8.25
Accountants	17%	1.00	1.00	1.50	1.25	3.00	7.75
Attorneys	14%	1.00	0.75	1.50	1.00	2.00	6.25
Law offices	13%	0.75	0.75	1.50	1.00	2.00	6.00
Auditors	12%	0.50	1.00	1.00	1.00	2.00	5.50

[20] 2.00 – income leader, 1.00 – 2nd place income leader, 0.50 – 3rd place income leader, 0.25 – lesser income earners
[21] 1.00 – much, 0.75 – less than much, 0.50 – on average, 0.25 – little
[22] 1.00 – all, 0.5 – partially
[23] 10.00 – major, 2.00 – large, 1.00 – average, 0.5 – small
[24] 1.00 – much, 0.75 – less than much, 0.5 – on average, 0.25 – little
[25] 1.00 – always, 0.75 – conditional
[26] 2 – in real time, 1.5 – in the past and in real time, 1 – in the past
[27] 2 – direct, 2 – indirect
[28] 3 – high, 2 – average, 1 – low

Trustees in bankruptcy/ bailiffs	12%	0.50	0.75	2.00	1.00	1.00	5.25
Pawnbrokers	12%	0.50	1.00	2.00	1.00	1.00	5.50
Total	100%						44.50

The subsector weights were determined based on the following indicators:

- market participants number
- share of obliged entities
- witnessing transactions – to what extent the persons see the transactions happening in real time and/or in the past (e.g. notaries participate in transactions in real time; accountants see transactions after their completion)
- interfering in transactions – to what extent persons can be involved in the transaction and influence it (e.g. notaries participate in transactions while these are in progress and can be involved, because their task is to authorise the transactions; auditors see the transactions retrospectively, which is why they cannot influence the transactions and their task is only to assess the transactions)
- daily role – how big is a demand for the services provided by the subsector in daily life

Heat maps

To better understand and visualise the assessments given, additional national and sectoral so-called heat maps are prepared that visualise the risk as a threat to the vulnerability ratio. Threat and vulnerability assessments are made compatible to prepare the heat map, i.e. +1 is added to the vulnerability ratings given by the sectoral working groups to make the scale of both indicators between 1 to 5.

The higher the risk, the redder its colour:

Table 4. Heat map risk scale

RISK SCALE	
High	**5**
Average/high	**4**
Average	**3**
Average/low	**2**
Low	**1**

The positioning of the risk point in the respective colour zone of the heat map helps to determine the risk rate and decide the extent and strategy for mitigation measures. The heat maps were prepared for the national level aggregate threat assessment and aggregate vulnerability, and for ratios of sectoral threats and vulnerabilities where the sectors' threat assessments were taken from the national threats sectoral risk assessment module.

Since the financial sector and professionals sector include multiple subsectors, 2 additional aggregate heat maps were prepared for these two extensive sectors, that provide a detailed overview of the subsectors' risk levels.

The state's risk position in the case of ML and TF is the ratio of threat and vulnerability the graphic depiction of which can be presented on the so-called heat maps. National threats and vulnerabilities chapters highlight the national risk levels heat maps from the ML and TF aspect. Sectoral vulnerabilities chapters also include heat maps.

2.4.6. Preparing the report and making proposals for a further action plan

Each national and sectoral working group prepared their chapter in accordance with the prefilled assessment module and adhering to the general report structure provided by the NRA steering committee. The NRA steering committee reviewed every chapter, gave the working groups feedback for necessary corrections, and made proposals for additions.

Each working group made proposals to address the risks, threats, and vulnerabilities identified during assessment. Based on the proposals received, the NRA steering committee prepared an action plan proposal.

2.4.7. Bottlenecks discovered during initial implementation of the methodology and options for improvement

Bottlenecks discovered during initial implementation of the methodology and options for improvement

Following the risk assessment process, the NRA steering committee with the leaders of all working groups analysed the bottlenecks identified in the methodology used for the NRA, and it was done from four aspects:

1. Methodology malfunctioning from the point of determining threats, vulnerabilities, and risks
2. Methodology malfunctioning from the point of its various stages
3. Methodology malfunctioning from the point of common handling of ML, TF, and PF
4. Methodology malfunctioning from the point of organisational structure of the project

More details on the bottlenecks and possible options for supplementing the methodology are provided next.

1. Determining threats, vulnerabilities, and risks

The methodology prescribed the analysing and the assessing of the national threats, national vulnerabilities, and sectoral vulnerabilities in separate working groups. During the work process it was identified that the national threats assessment module is incomplete (described in detail below) and thus the vulnerability working groups had to analyse among else also the presence of possible threats, although according to the methodology the threats input was supposed to come for the other working groups from the national threats working group. The methodology prescribed for assessment of national threats and vulnerability via independent differently structured assessment modules, which is why it was impossible to assess specific threats and vulnerabilities against each other. The national threats assessment module required entering various statistical data and there were certain difficulties with gathering the data. This, however, did not hinder the national vulnerabilities working group from assessing the national vulnerabilities faster, as the methodology used assumed a high level of generalisation and independence from the assessments given to the threats. The sectoral working groups assessed the threats and vulnerabilities within the sectors in time, before the national threats working groups finished their assessments, because the national threats working group was not ready to give input to other working groups based on the data gathered. The participants of the risk assessment found that the main shortcoming of this methodology was the option to conduct the threats and vulnerability assessments separately. Analysing retrospectively the process of assessing threats and vulnerabilities, the NRA steering committee together with the heads of working groups has found that the structure of the working groups provided for in the methodology, where the main emphasis is on assessing various vulnerabilities, is not effective. They found that more attention should be given to threats, incl. in sectoral working groups. The methodology should include specific instructions for identifying threats and this both at the national and sectoral level. The entire NRA process should start with determining the national threats and other working groups (national and sectoral) should not start their work before the threats at the national levels are identified. Identifying threats, vulnerabilities, and risks in working groups, incl. residual risks and assessment, could take place in the following consecutive stages:

identifying national threats - > identifying sectoral threats -> identifying sectoral vulnerabilities -> identifying national vulnerabilities.

Assessment of threats should begin with determining the threats and for this purpose it would be useful to obtain various principles of risk assessment preparation from different investigative, supervisory, and law enforcement authorities (National Criminal Police, Security Police, Tax and Customs Board, Financial Intelligence Unit), incl. their threat assessments. It would be also recommended to inquire about possible threats from the market participants. This methodology provided for asking feedback from the market participants (in the format of a survey or an interview), primarily from the perspective of vulnerability, and the sectoral questionnaires were also built by the methodology creator based on this.

The national threats and vulnerabilities working group could determine the risk mitigation measures at the national level and sectoral working groups could focus primarily on the mitigation measures of sectoral risks. According to this methodology, all working groups made proposals for risk mitigation measures both at the sectoral and national levels, which is why the NRA report includes repeating proposals for improving the occurring situation, the working group proposals overlapped, but also mitigation measures for different angles or aspects of the same problem, which made the overall administration of proposals more difficult than it could have been.

The national threats and sectoral vulnerabilities assessment modules provided for in the methodology did not help to fully fill in the NRA report structure, which is why several working groups had to perform extra tasks so the reports would have all the necessary information and the data, materials, and evidence considered in the assessment.

The main shortcomings of the methodology were identified in the national threats assessment module. This made threats identification and assessment significantly more difficult:

- The assessment module requested statistical data primarily for predicate offences, other worksheets (i.e. sectors, cash flows) asked too little data, which is why it was difficult for the working group to prepare a threat assessment even after all the fields in the assessment module were filled in.

- The assessment module did not provide concrete guidance if certain data was missing, that is, the working group did not know how to assess this what was not known: the assessment module did not handle the aspect of shadow economy, emergence of possible criminal proceeds, tax gap, etc. which were all marked in the national vulnerability module, but were not assessed substantially as threats.

- Outstanding indicators of the statistical data referred to in the assessment modules (e.g. the largest cash declarations per country, etc.) do not have a direct connection to ML or TF, thus highlighting them in the table should not automatically result in a higher ML or TF threat assessment. There is substance behind every statistical indicator which should be separately assessed, numerical indicators alone are not enough, although the assessment module is built on quantitative indicators primarily.

- Assessing TF threats through predicate offences is incorrect because terrorist financing could also take place through completely legal means.

- The assessment criteria provided in the methodology for the possible consequence of threat realisation were contradictory.

In conclusion, the national threats assessment module needs to be developed because it does not work well in the format it is provided for in the methodology.

Among else, the working groups have found that general knowledge of TF and PF threats of the representatives of the competent authorities is weak, as it is solely based on theory and thus the risk assessment of both domains is more difficult. TF experts (mainly the Security Service) find that ML and TF risks are so different that handling these in the same chapter is not reasonable and can rather create a wrong image of the risks of the two fields of activity. FATF has not yet confirmed guidelines for PF for

assessing the risks of this domain, thus the situation will likely improve already partially thanks to the international guidelines coming soon and in the future, conducting the NRA for PF is more effective because there will be the possibility to control the compliance of the conducted assessment to the international standard.

2. Functioning of different stages

The methodology required the entire risk assessment process to be carried out under the guidance of the Ministry of Finance. The ministry was the central authority in conducting the NRA and thus had taken several work flows – project communication, conducting the survey, making inquiries to gather statistics, etc. The working groups found that the central management was the correct and effective choice and this should be implemented also during the next NRA. Gathering statistics could be the first stage also in the future. To ensure better feedback for the survey and increase the response rate, it would be useful to give the respondents the option to reply in three languages and also to reduce the number of questions, because in certain sectors the questionnaires were unreasonably long (more than 100 questions) and were too burdensome for the respondents.

To gain a more objective risk image it would also be necessary to prepare a more detailed guidance for filling in the sectoral assessment modules. The efficiency scales provided in the assessment modules should also be reviewed.

3. Mutual relations among the ML, TF, and PF risks

It was previously stated that the ML, TF, and PF risks are different which is why they cannot be assessed on the same scale. The current methodology provided for sectoral ML and TF risk assessment using a scale with a similar structure, which is essentially wrong, one example is linking the TF threat with predicate offences. Also, the methodology did not include assessment of PF risks and thus PF risk assessment was done using one's best knowledge considering the discussions at the FATF that are in progress and other countries' examples. The working groups admitted that their knowledge of the TF and PF domains is weaker, which is why it would make sense to give the task of TF and PF risk assessment to competent experts who could assess them in a separate working group to achieve a better result.

4. Organisational structure of the project

This has been an extremely ambitious project in the organisational sense from the outset, the number of people involved exceeded 70 and the entire process took nearly 2 years. The exercise scope included quite many sectors, multiple large working groups were formed. In total, the result of the work done was a bulky NRA report of nearly 300 pages. Throughout the entire project, the overburdening of the members (especially working group leaders) was visible. The leaders of several working groups were at the same time also the members of another working group or groups. Experience has shown that in reality, a working group leader cannot contribute to the work of another group while performing tasks in their main working group. Thus, situations occurred where the working group did not receive sufficient input from the representative of a specific institution who was busy with leading another working group. In the future, direct communication between the working group leader and the central project team should also be increased.

All NRA project members performed the project tasks as a sidework to their main work and their workload increased significantly. It is true that everyone did not have the time, energy, or willingness to sufficiently contribute to the project from their free time. The work and contributions of the working group members would probably be more efficient and effective if a financial compensation would be provided along with at least partial release from performing one's main work tasks during the project. Paying the members would also reduce the strain on the working group leaders because the working group members would not need additional motivating. The payment could be guaranteed if the working group member contributes actively during the entire NRA process. In the future, paying the NRA project members should be considered. Also, creating positions at all institutions, which are specifically targeted at performing tasks related to conducting the NRA, incl. part-time positions, should be considered.

The methodology also recommended active involvement of private sector representatives, but experience

has shown that motivating private sector representatives to contribute at each stage is complicated. There were also certain complications when information meant for intrainstitutional use only was discussed and shared in working groups that included private sector representatives also.

Several sectors in the exercise scope included in turn several subsectors. Unfortunately, for instance the finance sector working group did not include the representatives of all these subsectors, which in turn caused some problems with preparing and testing the questionnaires. This time, the working group solved this issue by conducting interviews with the market participants of the specific subsector, but in the future, including representatives from all subsectors in the NRA working groups should be ensured.

An emerging problem is also the members leaving or missing certain stages (incl. meetings). Replacing members should be mandatory for institutions. If the participation of a member from a certain institution is required and it turns out that they cannot contribute from a certain point in time, then the institution is obligated to ensure that a new member participates, giving the working group input and contributing. The project team should definitely involve a methodologist who consults the project team in methodology matters.

In the future, the number of sectors included in the exercise scope should be reconsidered. This time, the methodology provided for involving 8 sectors, which is why the entire NRA process became very vast. It should be considered whether the next NRA could tackle less sectors. For instance, the riskier sectors, i.e. virtual currency service providers and sectors listed in the FATF standard: financial sector, NPOs, issue of taking advantage of companies, could be in the picture at all times. Also, the leaders of the financial sector and FinTech sector working groups have cooperated throughout the entire project due to the similarities and overlaps between the two sectors, and they have realised that in the future it would make sense to approach the FinTech subsectors together with the financial sector subsectors. Less risky sectors could be analysed less frequently during the NRA.

In the NRA report writing and approval stage it was realized that it would be reasonable to look for ways to ensure more even quality and content of the report. A clearer division of roles and smaller circle of preparers in the final stage would save time and provide a report with a better quality.

In the future, it would be necessary to automate the NRA process or at least implement automation in certain stages, for example when gathering the statistics and market participants reporting into a common database, conducting interviews as a part of supervisory procedures or submitting the report.

To ensure better quality of the NRA report and meet the description provided in the MLTFPA, the methodology should be supplemented on how the working groups should choose the due diligence measures of the assessed sectors. Current methodology did not provide instructions for this nor did it describe the connection between choosing due diligence measures and the assessment results. Thus, for preparing the report, the methodology should provide clearer instructions on how to determine the due diligence regime for the assessed sectors – stricter or simplified. Also, the risk mitigation measures offered by the working groups should among else include if and why the offered activities should be a priority for the state (e.g. for supervision), because this would be beneficial in the latter stage, i.e. when preparing the further action plan, in directing the resources as necessary, incl. to ensure solving more urgent problems.

In conclusion, the methodology implemented in this NRA has room for development and the shortcomings identified in the methodology must be eliminated when preparing for the next NRA.