

AML/CFT NATIONAL RISK ASSESSMENT METHODOLOGY

Republic of Estonia



European Union
European Social Fund



Investing
in your future



REPUBLIC OF ESTONIA
MINISTRY OF FINANCE



REPUBLIC OF ESTONIA
GOVERNMENT OFFICE

Contents

1.	Introduction & Context.....	2
1.1	Methodology Differentiators	4
1.2	Context	4
1.3	Objective & Scope	5
1.4	Intergovernmental Organisations	6
1.5	Links with Global AML/CFT Standards & Supranational Risk Assessments	8
2.	NRA Governance & Coordination	10
2.1	Administrative Burden	11
2.1.1	Previous NRA exercise.....	11
2.2	Governance & Stakeholders	12
2.3	Project Plan	15
2.3.1	Timeline	15
2.3.2	Milestones	16
2.3.3	Roles and Responsibilities	16
2.4	Risk-based Approach	17
3.	Risk Management Process.....	18
3.1	Stage One: Identification	20
3.1.1	Preliminary Country Risks Profile	20
3.1.2	Workshops & Questionnaires	22
3.1.3	Understanding Threat.....	23
3.1.4	Understanding Vulnerability	26
3.2	Stage Two: Analysis	30
3.2.1	Country Exposure Risk Rating (CERR)	33
3.2.2	Threat Risk Rating (TRR).....	40
3.2.3	Vulnerability Rating (VR).....	43
3.3	Stage Three: Evaluation & Reassessment.....	46
3.3.1	Risk Management Strategies	46
3.3.2	Reassessment of ML/TF risks.....	48
4.	Appendices	49

1. Introduction & Context

The **national risk assessment** (hereinafter “NRA”) is an exercise to identify, assess and understand the risks, threats and vulnerabilities of money laundering (hereinafter “ML”) and terrorist financing (hereinafter “TF”). The NRA highlights both ML/TF risks in the country and the most widespread means used to launder illicit proceeds or to fund acts of terror.

The Financial Action Task Force’s (hereinafter “FATF”)¹ Recommendation 1² highlights that countries should conduct an NRA, as well as take action (including designating an authority or mechanism to coordinate actions assess risks and apply resources) aimed at ensuring the ML and TF risks are mitigated effectively. The NRA therefore serves as the foundation that will aid in the further implementation of a risk-based approach to combatting ML and TF.

Following the FATF’s recommendation, the Republic of Estonia (hereinafter “Estonia”) conducted and published its first **national risk assessment** of money laundering and terrorist financing risks in 2015 (hereinafter “2015 NRA”)³ using the World Bank’s (hereinafter “WB”) methodology.⁴

This document, *AML/CFT National Risk Assessment Methodology*, was created upon request of the Government Office. The project was financed under priority axis 12 "Administrative Capacity" measure 12.2 "Development of Policy-Making Quality" in the 2014-2020 European Union Cohesion Funds programme financed by European Union Social Fund. The Ministry of Finance was initiator and cooperation partner of the project.

This methodology document is structured as follows:

- The introduction chapter (Chapter 1) lays out the objective, scope and differentiating elements of this guidance, along with an outline of the connections with FATF obligations relevant to ML/TF risk assessments at any level and the supranational risk assessment (hereinafter “SNRA”);
- Chapter 2 discusses the NRA governance principles, including guidance on organising a country-wide ML/TF risk assessment and the specific stakeholders involved; and
- Chapter 3 presents a high-level view of the main stages involved in the ML/TF risk management process.

The appendices to this document contain additional information relating to the ML/TF risk assessment, the questionnaires and the Estonian country-level risk assessment tool (hereinafter “ECRAT”), which is required for the quantification of risks.

Various methodologies and risk assessment approaches (e.g. WB, SNRA⁵, FATF, IMF, MER, *inter alia*) were analysed in order to determine the most suitable approach for the country of Estonia. It was determined that a tailor-made approach leveraging the best practices from the aforementioned methodologies was most appropriate given the existing administrative constraints and Estonian specifics.

¹ The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against ML, TF and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering and counter-terrorist financing standard. More details about the FATF are provided in the Chapter 1.2.

² The FATF Recommendations: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.

³ 2015 NRA: <https://www.rahendusministeerium.ee/et/finants-ja-ettevotluspoliitika/rahapesu-ja-terrorismi-rahastamise-tokestamine>.

⁴ World Bank Group, National Risk Assessment Tool Guidance Manual, January 2015.

⁵ Supranational Risk Assessment Report: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en.

The following Estonian specifics were analysed and taken into consideration when drafting the methodology, *inter alia*:

- Estonian composition of the market: The methodology is tailored to the current sector composition of Estonia. The Estonian sectors are identified in Chapter 1.5. The methodology also describes vulnerabilities inherent for those sectors – such vulnerabilities to ML/TF are both specific for Estonia and observed in the broader international context;
- Recent anti-money laundering and counter-financing of terrorism (hereinafter “AML/CFT”) developments in Estonia: The methodology is based on the understanding of the risk landscape in Estonia. The risk landscape was identified as part of the preliminary country risk profile analysis, that is described in Chapter 3.1.1;
- Geopolitical circumstances: The methodology incorporates threats arising from the geographical position of the country by, *inter alia*, analysing information obtained from the Estonian Financial Intelligence Unit⁶; and
- Limited state resources: The methodology introduces a risk-based approach to the ML/TF risk management process, which is described in more details in Chapter 2.4. This approach helps the state to allocate a maximum number of resources to the sectors that require more attention, while following a less burdensome procedure for sectors that pose less risk. Aside from that, the methodology introduces methods to reduce administrative burden throughout the document (i.e. a less burdensome review process for the certain risk sectors is introduced in Chapter 3).

The methodology was created in cooperation with the Estonian public and private sectors in order to fully understand the Estonian risk landscape, ensure that methodology is country-specific and subsequently test the model. The following testing, *inter alia*, was performed:

- A series of workshops was held with representatives from both private and public sectors to gain an understanding of the Estonian risks;
 - Public sector – Ministry of Finance, Ministry of Justice, Financial Supervision Authority (hereinafter “FSA”), Financial Intelligence Unit (hereinafter “FIU”), Police and Border Guard Board, Asset Recovery Bureau, Prosecution Office, Ministry of Justice, Ministry of Interior, Chamber of Notaries.
 - Private sector – Estonian Banking Association, NGO Union, Estonian Auditors Association, Estonia Assembly of Accountants, Gambling Association and Real Estate Association
- Estonian AML/CFT legislation was analysed to understand the context and potential AML/CFT risks that should be more deeply analysed during the NRA execution phase (e.g. reverse burden of proof); and
- Estonian intelligence reports and country risk information were analysed to identify Estonian risk typologies (refer to Appendix 2).

⁶ Financial Intelligence Unit's advisory guidelines: <https://www2.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/fius-advisory-guidelines/>.

1.1 Methodology Differentiators

This methodology should be built on Estonia's country specifics. In this process, we have considered elements such as the country's industries, main risk factors, common predicate offences, and the recent report on the prevention of ML and TF.⁷

The following list represents differentiating elements of the current NRA methodology:

1. Consideration of the **country specifics**, as systemic ML risks typical for Estonia and the broader Baltic region have been incorporated;
2. Reinforcing the value of a strong **evidence base** to reach a conclusion, which will increase **objectivity**. Evidence is essential to decreasing the subjectivity in the assessment, thereby decreasing the extent to which the assessor is affected by personal views, experience, or background;
3. **Addition of the quantification** of the results, as guidance for the assessment of the individual deciding factors has been provided;
4. Focus on Estonian **ML risks** as well as **TF risks**. These risk typologies are gathered during research and identified in the workshops with Estonian supervisory authorities and market participants. Consider TF risks across multiple dimensions that are inherent, given the current market composition of Estonia;
5. **Decreasing the administrative burden** on the Estonian public and private sectors by supporting them in the effective coordination of efforts and introducing a less burdensome review process for sectors that face less ML/TF risk.

1.2 Context

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 process of laundering is completed with the intention of making it seem that the process has come from a legitimate source. ML typically involves three stages: **placement**, **layering** and **integration**.

- **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 suspicion of ML. Another method is trade-based ML, which involves criminals using legitimate trade to disguise the movement of illicit funds by, *inter alia*, over- or under-invoicing the value of goods.
- The main purpose of the **layering** stage is to separate the illegal money from its source. This is accomplished through sophisticated layering of financial transactions to make tracing transactions difficult. The money can electronically move from one account to another and in different countries. Criminals also use the money to buy and sell 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 integrate laundered money back into the economy (i.e. criminals use shell companies to buy property and the proceeds are then considered legitimate). An alternative method is for criminals to set up front companies in countries with strict corporate secrecy laws.

⁷ Analysis and Proposals of the Governmental Committee on the Prevention of Money Laundering and Terrorist Financing: https://www.rahendusministeerium.ee/sites/default/files/rahapesu_tokestamise_valitsuskomisjoni_analuuus_ja_ettepanekud.pdf.

Terrorist financing involves financial support, in any form, of terrorist activities. TF is closely linked with ML as they both disguise the origin of money. 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 with 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 strip the criminal of the economic benefits received from engaging in criminal behaviour. Both, ML and TF are criminal offences and are detrimental to the economy and society as a whole.

Proliferation Financing (hereinafter “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 contravention 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 aim is 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 profits made by facilitating these movements.

Financing of proliferation can contribute to the 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.

1.3 Objective & Scope

The purpose of the NRA Methodology is to provide Estonia with advisory guidelines for the application of an ML/TF risk assessment on the country-level. The NRA Methodology covers the requirement for the assessment and management of ML and TF risks, as established in the Money Laundering and Terrorist Financing Prevention Act⁸ (hereinafter “MLTF Prevention Act”). The scope of this methodology is aimed at all stakeholders and obliged entities as defined in the MLTF Prevention Act.

As described in more detail in Chapter 2.4, the NRA Methodology was designed using a risk-based approach and took into consideration international leading practices. The risk-based approach allows countries to adopt measures in order to focus efforts in an effective way (i.e. target resources more effectively and apply preventive measures that are commensurate to the nature of the risks).

A risk assessment is an essential step in the creation of a robust risk-based AML/CFT defence mechanism on the country-level. During the ML/TF risk assessment, Estonia will determine how the ML and TF risks identified will affect the country by analysing the probability and consequence of threats occurring in combination with the effectiveness of national controls (i.e. vulnerability).⁹

⁸ ML/TF Prevention Act: <https://www.riigiteataja.ee/en/eli/521122017004/consolide>.

⁹ FATF Guidance for a risk-based approach: effective supervision and enforcement by AML/CFT supervisors of the financial sector and law enforcement: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-effective-supervision-and-enforcement.html>.

The users of the NRA include policy makers, supervisory authorities, the private sector, etc. The results of the NRA will benefit the users in different ways depending on the type of user. Policy makers and government officials should use the results of the NRA to make decisions on the legal and regulatory framework, allocate resources and develop national AML/CFT policies. The private sector should use the results of the NRA as a strong starting point for their own ML/TF risk assessments. Using a risk-based approach in combination with the NRA results, the private sector will decrease their own administrative burden by focusing their attention and AML activities on already identified high risk areas.

Please note that this is a methodology document. While the document includes a number of examples, these examples are merely illustrative and are intended to provide a practical context for the implementation of selected parts of the methodology. For the avoidance of doubt, this document does not offer completeness, neither express nor implied, in terms of risk factors, controls, or any other inputs that the methodology itself is designed to capture.

1.4 Intergovernmental Organisations

There are a number of bodies that provide guidance on best practices for the NRA. This chapter provides a summary of the international leading practices and the inter-governmental bodies governing AML/CFT in the European Union (hereinafter “EU”) as well as in Estonia.

FATF

The FATF is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions, and its objective is to set standards and promote effective implementation measures for combating ML, TF and PF. In essence, the FATF is a “policy-making body” in these areas. The FATF’s primary two functions are developing international standards (“Recommendations”) and monitoring the progress of its members as they implement ML and TF techniques and counter-measures.¹⁰ Estonia is not a member of FATF itself. The country is assessed by an associated member of FATF – MONEYVAL.

MONEYVAL

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (hereinafter “MONEYVAL”) monitors the implementation of FATF Recommendations through a peer review process (hereinafter “Mutual Evaluation”).

MONEYVAL is a permanent monitoring body of the Council of Europe tasked with assessing compliance with international AML/CFT standards and the effectiveness of their implementation.

Estonia is a member of MONEYVAL and as such is subject to MONEYVAL’s Mutual Evaluation procedures. Estonia has taken steps to implement and provide a sustainable legal and institutional framework that conforms to international AML/CFT standards.¹¹

¹⁰ FATF: <http://www.fatf-gafi.org/about/>.

¹¹ Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism: <https://www.coe.int/en/web/moneyval>.

The European Union (EU)

The EU implements FATF Recommendations through EU Directives that member states are required to adopt into national law. The Fourth AML Directive¹² was adopted into Estonian law through the Money Laundering and Terrorist Financing Prevention Act¹³, which came into effect on 26 October 2017.

The objectives of the Estonian National Money Laundering and Terrorist Financing Risk Assessment are set out in § 11 of the Money Laundering and Terrorist Financing Prevention Act to:

§ 11. National risk assessment

1) provide for the needs of drafting and amending anti-money laundering and countering the financing of terrorism (hereinafter AML/CFT) legislation, other regulations of the field and related fields as well as guidelines of supervisory authorities.

The NRA methodology addresses this, as it:

- describes the process of the Estonian legal system assessment. AML/CFT legal framework as well as its subsequent incorporation in sector-level policies, procedures and guidelines are evaluated as a part of the methodology;
- provides guidance and assessment tools that help to detect potential gaps in the legislation for the entire country (National Vulnerability module of the ECRAT) as well as for the separate sectors (Sector-specific Vulnerability modules of the ECRAT).

2) specify, 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.

The NRA methodology addresses this, as it:

- provides a detailed assessment framework for all sectors in scope (Sector-specific Vulnerability modules of the ECRAT). This assists the country to assign a risk rating to the particular sector;
- provides a detailed assessment framework for identification of threats associated with foreign countries and jurisdictions (Geographical Threat assessment element within the Threat Risk Rating Module); and
- provides a mechanism that permits identification of detailed risks, such as specific types of transactional patterns (i.e. transactions amount and types).

3) specify, 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.

As described above, the NRA methodology allows the country to categorise sectors and specific risks into risk classes. The methodology provides guidance on how to apply a risk-based approach to addressing the identified risks (i.e. simplified measures can be applied to sectors identified with a lower risk of ML/TF, while increased attention is placed on the areas that are identified as higher risk).

4) give instructions to the ministries and authorities in their area of government regarding allocation of resources and setting of priorities for AML/CFT purposes.

The NRA methodology provides a snapshot of the risks identified on the country level. Following the execution of the National Risk Assessment, the country should formulate a risk management strategy and action plan that is aligned with the country's risk appetite. The action plan will allow the country to manage and allocate resources efficiently by adding emphasis to areas with high risk and high priority.

¹² Directive (EU) 2015/849: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AJOL_2015_141_R_0003.

¹³ MLTF Prevention Act: <https://www.riigiteataja.ee/en/eli/521122017004/consolide>.

1.5 Links with Global AML/CFT Standards & Supranational Risk Assessments

Estonia, while executing its NRA, considers the risks identified both on the global and EU level and performs its risk assessment in such a way that it is easy for sectors and obliged entities within the country to incorporate the results in their own risk assessments. It is recommended that obliged entities use the NRA results to familiarise themselves with the risks of ML and TF in the country as well as the measures taken by the state to deal with these risks and incorporate this knowledge in their individual risk appetite statements and risk assessments.

Global AML/CFT Standards

As part of its ongoing review of compliance with the AML/CFT standards, the FATF identifies jurisdictions across the globe that have strategic AML/CFT deficiencies. The FATF conducts research into the trends and methods used to launder the proceeds of criminal activities and finance illicit activities and publishes reports based on their findings. Recent publications include:

- *FATF Monitoring of Terrorist Financing Risks and Actions Taken to Combat ISIL, Al-Qaeda and Affiliates Financing*¹⁴ published on 19 October 2018;
- *Financial Flows from Human Trafficking*¹⁵ published on 2 August 2018; and
- *Professional Money Laundering*¹⁶ published 26 July 2018.

In summary, these publications provide an overview of the ML and TF threats as identified by the FATF (i.e. on a “global” level) along with the ultimate potential consequences that they can bring about. The aim is to inform governments, the private sector and international policy-makers about ML and TF threats in order to better manage scarce resources and take more focused actions against ML and TF. The issues identified in these publications may be useful to Estonia when conducting its NRA.

The **SNRA**¹⁷ issued in June 2017 addresses the risks of ML and TF affecting the internal market and relating to cross-border activities in the EU. The European Commission (hereinafter “EC”) issued a report that analysed the risks of ML and TF and proposed a comprehensive approach to addressing these risks. The report showed that the EU internal market is still vulnerable to ML and TF risks. The EC will implement new measures as outlined in the SNRA report to mitigate the risks appropriately, and the Member States are expected to implement those recommendations issued in this report expediently. The EC will monitor the actions taken by the Member States based on the SNRA findings. The EC’s review will also assess how measures implemented at the EU and national level impact the risk levels. Selected risks discussed in the SNRA report are outlined in Appendix 3.

The purpose of the **National Risk Assessment** is to identify risks and assess risk magnitude, both individually and collectively, in order to focus attention on the most important threats and

¹⁴ FATF Monitoring of Terrorist Financing Risks and Actions Taken to Combat ISIL, Al-Qaeda and Affiliates Financing: <http://www.fatf-gafi.org/publications/methodsandtrends/documents/isil-alqaeda-affiliates-financing-update.html>.

¹⁵ FATF Financial Flows from Human Trafficking: <http://www.fatf-gafi.org/publications/methodsandtrends/documents/human-trafficking.html>.

¹⁶ FATF Professional Money Laundering: <http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>.

¹⁷ SNRA Report: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en.

vulnerabilities and lay the groundwork for a risk response related to ML and TF. The key aim of the NRA is to measure and prioritise risks so that risk exposure is aligned to resource commitment thereby effectively managing the country’s overall risk exposure.

The **Sectoral Risk Assessment** is informed by a variety of information sources including the NRA, national statistics (e.g. Financial Intelligence Unit Yearbooks) and international guidance. The aim of the sectoral risk assessment is to understand ML and TF risks within each of the country’s identified sectors. The results of a sectoral risk assessment provides guidance to the obliged entities on the risks relevant to their respective sector and informs the entity-level risk assessments.

Eight sectors were selected in such a way that all Estonian obliged entities highlighted in the MLTF Prevention Act¹⁸ are covered.

Sector breakdown in Estonia

Financial
Real estate
Financial technology
Trust and company service providers (hereinafter "Trust & Company SP")
Non-profit organisations (hereinafter "NPO")
Dealers in high-value and easily tradable "lifestyle" goods also cash and cash-like assets dealers (hereinafter "Dealers")
Gambling
Other designated non-financial businesses and professions ("DNFBPs")

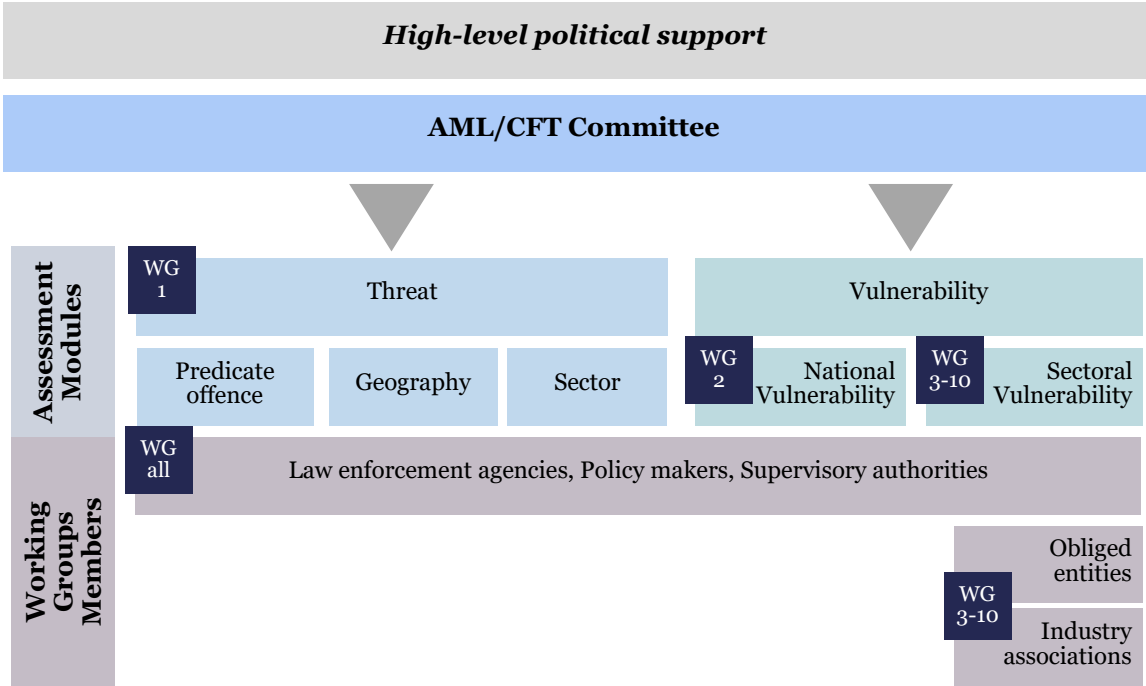
As addressed further in the document, the methodology helps the country to assess the risks of the activities of non-obligated persons by laying out the framework for analysis of the:

- **Country-wide threats**, including threats resulting from the country’s geographical position and threats arising from the individual predicate offences; and
- **Country-wide vulnerabilities**, including areas that the FATF identified as key goals achieved by an effective AML/CFT country-wide framework.¹⁹

2. NRA Governance & Coordination

The FATF recommends that there should be a clear determination and designation of the agency, organisation or “task force” in charge of leading and coordinating the NRA process.²⁰ As presented in Graphic 1 below, it is essential that there is adequate political support and attention given to the NRA. The AML/CFT Committee is responsible for NRA coordination. The Ministry of Finance (or Rahandusministereerium) is responsible for organising the AML/CFT Committee and publishing both the generalised results of the NRA on its website and the aggregate statistics in the field of ML and TF.

Graphic 1. NRA Coordination



¹⁹ An effective system to combat money laundering and terrorist financing: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html>.

²⁰ FATF NRA: http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

2.1 Administrative Burden

The concept of administrative burden is an important variable in understanding the citizens' perception of the government. Administrative burden is defined as the cost that natural persons and legal entities incur in order to comply with information obligations imposed by the state. For the purpose of this methodology, an information obligation means the disclosure of information to authorities.

In the context of AML/CFT, administrative burden is conceptualised as the function of learning costs and compliance costs that obliged entities experience in their interactions with the government. The **learning costs** arise from **collecting information** about legislation and regulations and **assessing the relevance** to the obliged entity. Knowledge of AML/CFT and sanctions varies from sector to sector (e.g. the obliged entities in the financial sector may be more aware of the AML/CFT legislation and regulations than the real estate sector). The **compliance costs** are incurred from **following legislative requirements** and **complying with regulations**.

It is important to have an understanding of the baseline from the previous NRA exercise and the level of engagement necessary for the NRA process, which is described in the subsequent chapters, when considering administrative burden.

2.1.1 Previous NRA exercise

The previous NRA exercise (2015 NRA) in Estonia took approximately **two years to complete and involved more than 60 people** from the public and private sectors.²¹ The 2015 NRA process along with lessons learnt, key takeaways and how the current methodology addresses those points are discussed below.

The 2015 NRA process began in October 2012 when the government of Estonia decided to prepare its first national risk assessment on ML and TF. The Ministry of Finance was tasked with coordinating the NRA exercise and a working group was established to prepare the risk assessment. The working group members included the Ministry of Finance, the Police and Border Guard Board, the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Security Police Board, the Financial Intelligence Unit, the Financial Supervision Authority, the Prosecution Office and the Tax and Customs Board.

The working group decided to use the WB methodology to prepare the 2015 NRA, and the WB methodology included seven modules: (1) Criminal income related to money laundering; (2) National vulnerability; (3) Banking; (4) Securities; (5) Insurance; (6) Other financial service providers; and (7) DNFBPs. The WB methodology did not initially include modules for virtual currencies, cash movement or financing of terrorism and proliferation. The working group members added these towards the end of the 2015 NRA exercise.

In late February 2013, a workshop was organised to introduce the WB methodology, to set up sub-groups and to map out risk assessment activities. Workshop participants included the working group members, the AML/CFT Committee, the Estonian Bar Association, the Chamber of Notaries and the Estonian Banking Association. A decentralised approach was taken by dividing the work amongst autonomous sub-groups according to their competence. Each sub-group owned their modules of the WB methodology (e.g. FSA owned the financial modules) and agreed on a common date to submit the final results. The decentralisation of authority can create problems with coordination and requires

²¹ Prevention Money Laundering and Terrorist Financing: <https://www.rahandusministeerium.ee/et/finants-ja-ettevotluspoliitika/rahapesu-ja-terrorismi-rahastamise-tokestamine>.

qualified and competent personnel. At the beginning of the 2015 NRA exercise, there was strong cooperation between the public and private sector; however, this worsened as the disadvantages of decentralisation manifested.

From March 2013 to December 2014, the sub-groups individually performed the risk assessment activities, such as collecting relevant statistics and interviewing the private sector. The results of the NRA were endorsed and published in January 2015.

The current methodology takes a more centralised management approach. The AML/CFT Committee, with its chairman as the Minister of Finance, will be the one, central body responsible for coordinating the NRA. The NRA Steering Committee, appointed by the AML/CFT Committee, performs the work involved in a NRA including outreach to the public sector. A centralised management style along with a risk-based approach will improve the effectiveness of resources allocation and decrease the administrative burden on private sector.

Current NRA methodology was designed in the way that it will put maximum emphasis on the more risk sectors, while administrative burden is decreased for sectors that pose less risk. This will support Estonia in its effort to decrease the time spent on the NRA project execution.

2.2 Governance & Stakeholders

The **AML/CFT Committee** includes representatives from the Ministry of Finance, the Financial Intelligence Unit (or Rahapesuandmebüro), the Central Bank of Estonia, the Estonian Financial Supervision Authority (or Finantsinspektsioon), other relevant governmental authorities and bodies and the secretaries general of the ministries responsible for the related fields. The Committee's specific roles and responsibilities are defined in the MLTF Prevention Act.²² The Committee prepares a plan of measures and activities to mitigate the risks identified in the NRA, designates the authorities to carry out the risk-mitigating activities, and examines the progress of the action plan implementation.

Public Sector

The public sector's involvement in the NRA is compulsory. The public sector organisations that will participate in the NRA include, *inter alia*, the **Ministry of Finance**, the **Police and Border Guard Board**, the **Ministry of Justice**, the **Ministry of Internal Affairs**, the **Ministry of Foreign Affairs**, the **Security Police Board**, the **Financial Intelligence Unit**, the **Financial Supervision Authority**, the **Prosecutor's Office** and the **Tax and Customs Board**.

Private Sector

The private sector's involvement in the NRA is essential and **strongly encouraged**. These private sector representatives can be from the associations of relevant professions and from the obliged entities, especially the key players in the Estonian market. Their involvement is important for raising awareness, as the obliged entities are among the primary beneficiaries of the NRA. Further, in many countries this involvement has contributed to enhancing the public and private sector dialogue and cooperation in AML/CFT.

The level of engagement from the private sector, as required by this methodology, has increased from 2015 NRA. However, the results of the NRA exercise will be a very strong input to their own risk assessment. Utilising a risk-based approach will decrease their own administrative burden when

²² MLTF Prevention Act, §12: <https://www.riigiteataja.ee/en/eli/521122017004/consolide#para12>.

performing their own ML/TF risk assessment by focusing their attention and AML activities the already identified higher risk areas.

Working groups (hereinafter “WG”) are comprised of the relevant stakeholders – law enforcement agencies, supervisory authorities, representatives of obliged entities across all sectors and other experts – necessary to discuss the ML and TF risk landscape in Estonia. The Ministry of Finance is the common, overseeing body for all WGs, as it is the overseeing body of the NRA.²³ The proposed composition of all WGs is described in Table 2 below. To reduce administrative burden, the WGs may be merged or realigned by the AML/CFT Committee. Each WG is responsible for its respective module (e.g. Threat Assessment, National Vulnerability and Sectoral Vulnerability Modules).

The nature, extent and timing of the private sector involvement is at the discretion of the AML Committee. The following options should be considered when deciding the level of the private sector’s involvement.

- Private sector representatives as permanent members of the WG;
Options that would help Estonia to decrease the administrative burden:
- Private sector representatives only in initial workshop, then follow up with focus group meetings;
or
- Obtaining the private sector’s views and input through focus group meetings, without direct involvement in the NRA workshops.

The AML/CFT Committee is responsible for the implementation and coordination of NRA WGs (responsibility may be delegated to NRA Steering Committee). A proposed composition of WGs can be found in Table 2 below; however, the NRA Steering Committee may choose to merge or divide the WGs as needed. The AML/CFT Committee/NRA Steering Committee organises and coordinates a series of workshops for the WGs to attend. During the workshops, the WG members discuss the risk landscape and propose an estimated level of threat and vulnerability. Workshops are discussed in more detail in Chapter 3.1.2.

The WG members and the management of their agencies/institutions should be notified about the permanent nature of the WG (until the end of NRA project) and the importance of the NRA project. WG members are senior specialists within their field, given the analytical work involved in the NRA exercise.

²³ MLTF Prevention Act: <https://www.riigiteataja.ee/en/eli/517112017003/consolide>.

Table 2. Proposed NRA Working Groups Composition

WG 1 Threat Assessment	WG 2a National Vulnerability Assessment	WG 2b National Vulnerability sub-group – Legal Framework Assessment
<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Central Bank of Estonia • FSA • FIU • Police and Border Guard Board • Secret Services • Internal Security Services • Prosecution Office • Ministry of Justice • Tax and Customs Board • Ministry of Interior • Judges • Asset Recovery Bureau • Chamber of Notaries • Estonian Bar Association 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Central Bank of Estonia • FSA • FIU • Police and Border Guard Board • Secret Services • Internal Security Services • Prosecution Office • Ministry of Justice • Tax and Customs Board • Ministry of Interior • Judges • Asset Recovery Bureau • Chamber of Notaries • Estonian Bar Association 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • FSA • FIU • Chamber of Notaries • Ministry of Justice • Tax and Customs Board • Ministry of Interior
WG 3 Financial Sector Vulnerability Assessment	WG 4 Real Estate Sector Vulnerability Assessment	WG 5 Financial Technology Sector Vulnerability Assessment
<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Central Bank of Estonia • Supervisory authority (i.e. FSA and FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations (i.e. Estonian Banking Association) 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Supervisory authority (i.e. FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations (Estonian Real Estate Entities Association and The Chamber of Notaries) 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Supervisory authority (i.e. FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations
WG 6 Trust & Company SP Sector Vulnerability Assessment	WG 7 NPO Sector Vulnerability Assessment	WG 8 Dealers Sector Vulnerability Assessment
<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Ministry of Justice • Supervisory authority (i.e. FSA; FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Ministry of Justice • Supervisory authority (i.e. FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations (i.e. NGO Union) 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Supervisory authority (i.e. FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations

Table 2. Proposed NRA Working Groups Composition (continued)

WG 9 Gambling Sector Vulnerability Assessment	WG 10 Other DNFBPs Sector Vulnerability Assessment
<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Tax and Customs Board • Supervisory authority (i.e. FIU) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations (i.e. Gambling Association) 	<p>Representatives from:</p> <ul style="list-style-type: none"> • Ministry of Finance (oversight) • Supervisory authority (i.e. FIU; Estonian Bar Association; Ministry of Justice or Chamber of Notaries) • Representatives of the Obligated Entities for the Sector as Appointed By the Market Participants Advisory Committee • Industry Associations (i.e. Estonian Auditors Association; Estonia Assembly of Accountants; The Chamber of Bailiffs and Trustees in Bankruptcy)

2.3 Project Plan

A project plan is essential to keep the NRA on track by guiding both project execution and control. Following the FATF guidance, a project plan has been developed for the NRA process. The NRA project plan includes an approximate timeline, key milestones and the relevant responsibilities of the persons involved in the process. A detailed proposed project plan is available in Appendix 4.

2.3.1 Timeline

It is estimated that an NRA project will take approximately one year to complete; however, this depends on, *inter alia*, participant availability and response rates. By agreeing to participate in the NRA process, all parties (the NRA Steering Committee and the participants) endeavour to meet deadlines and to provide comprehensive, accurate and timely responses, reports or other materials. The intention of the timeline is to provide guidance on what is required if the NRA results are to be published within a reasonable timeframe. It is therefore imperative that all parties respect the timeline. Any deficiencies, such as a failure to comply with a deadline, may lead to a delay in the publication and discussion of the NRA results. Remedial action should be planned for cases when the timeline is not met.

2.3.2 Milestones

The key milestones are succinctly catalogued below.

- Pre-planning activities:
 - Establish the NRA Steering Committee (i.e. the people responsible for performing the work) and appoint members; and
 - Set-up central data repository (e.g. virtual database).
- Planning:
 - Kick-off meeting;
 - NRA methodology training;
 - Distribute questionnaires; and
 - Organise working group workshops.
- Risk Assessment Stage 1: Identification:
 - Determine a preliminary country risk profile;
 - Threat Workshops;
 - National Vulnerability Workshops; and
 - Sectoral Vulnerability Workshops.
- Risk Assessment Stage 2: Analysis:
 - Threat Risk Rating;
 - National Vulnerability Rating;
 - Sectoral Vulnerability Rating;
 - Sectoral Risk Rating; and
 - Country Exposure Risk Rating.
- Risk Assessment Stage 3: Evaluation:
 - Risk management action plan.
- Reporting & Closing:
 - NRA results report publication; and
 - Closing meeting.

2.3.3 Roles and Responsibilities

The key roles and responsibilities are described below. Refer to the MLTF Prevention Act²⁴ for more information in regards to the AML/CFT programme.

Ministry of Finance

The Ministry of Finance oversees the AML/CFT Committee. The NRA process begins and ends with a meeting hosted by the Ministry of Finance. The Ministry of Finance will also participate in workshops. The Ministry of Finance will publish the generalised results of the risk assessment and aggregate ML/TF statistics on their website.

²⁴ MLTF Prevention Act, §12: <https://www.riigiteataja.ee/en/eli/521122017004/consolide#para12>.

AML/CFT Committee

According to the MLTF Prevention Act, the function of the AML/CFT Committee is to coordinate and update the NRA. Therefore, the AML/CFT Committee establishes ad hoc and standing WGs, the Market Participants Advisory Committee and the NRA Steering Committee. Also, the AML/CFT Committee will determine the appropriate timing for reassessment of ML and TF risks identified.

Refer to Section 12. *AML/CFT Committee* of the MLTF Prevention Act²⁵ for more information on the AML/CFT Committee's roles and responsibilities in regards to AML/CFT.

NRA Steering Committee

The NRA Steering Committee, supervised by the AML/CFT Committee, will complete the necessary steps in the NRA process, including facilitating the workshops and interviews, gathering data and information, completing the ECRAT and drafting the NRA report. The NRA Steering Committee will engage with and consult the supervisory authorities and the private sectors on an on-going basis throughout the NRA process and at regular prescribed intervals, provide a progress report highlighting both progress and deficiencies to the AML/CFT Committee.

Supervisory Authorities

It is crucial for the supervisory authorities to work closely with the AML/CFT Committee. The most effective way of getting responses to NRA-related inquiries from the public sector is to assign supervisory authorities responsible for communicating with the obliged entities. However, to decrease the administrative burden, another option may be considered – supervisory authorities could provide an official cover letter to accompany the questionnaires that are sent to the obliged entities. Further, the supervisory authorities should serve as a point for escalation for obliged entities that do not respond. It is recommended that the supervisory authorities cooperate fully when engaged by the NRA Steering Committee.

Private Sector

The private sector's involvement in the NRA is strongly encouraged (refer to Chapter 2.2 for more details). The private sector (obliged entities) should cooperate fully and provide comprehensive, accurate and timely responses when engaged by the NRA Steering Committee.

2.4 Risk-based Approach

The FATF Recommendations consider the risk-based approach (hereinafter "RBA") to combat ML and TF as an essential foundation of a country's AML/CFT regime. The RBA allows countries to target their resources more effectively and apply preventive measures that are commensurate to the nature of the risks. An effective RBA involves identifying and analysing ML and TF risks and determining an appropriate risk management strategy to mitigate the risks identified. This risk management process for combating ML and TF is discussed in more detail in the next chapter, Chapter 3.

The RBA decreases administrative burden by allocating resources in the most effective way. The

²⁵ Ibid.

alternative approach involves deploying resources evenly to all sectors and risks, which may lead to a perfunctory exercise rather than focusing on combating ML and TF.

The RBA is not a “zero failure” approach. Regardless of the strength of the AML/CFT regime, criminals will continue to attempt to move illicit funds through the national economy. A reasonably designed and effectively implemented RBA will provide a control structure to manage identifiable ML and TF risks. However, it must be recognised that controls will not identify and detect all instances of ML or TF.

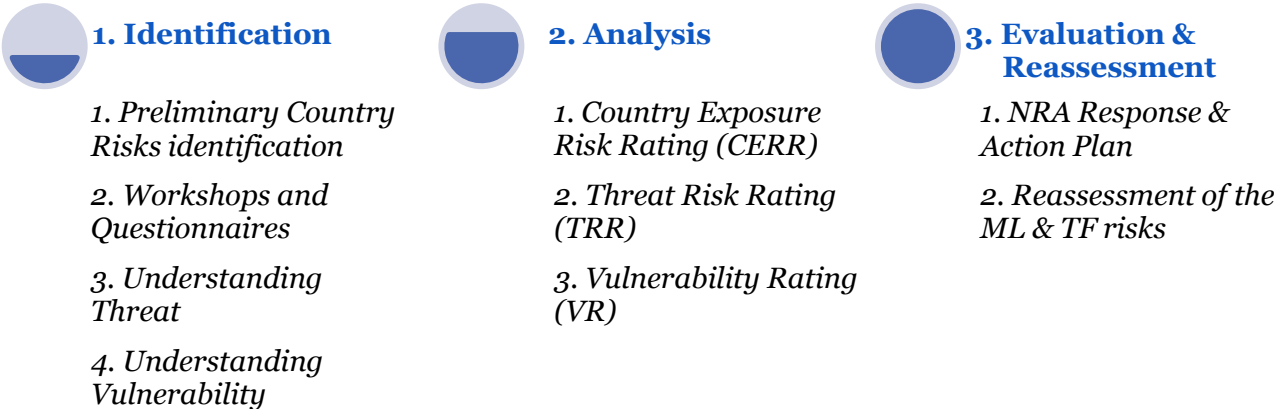
3. Risk Management Process

The risk management process encompasses recognising the existence of ML and TF risks, undertaking an assessment of the ML and TF risks and developing strategies to manage and mitigate the identified risks.

The NRA is a complex, iterative exercise that involves an evaluation of the threats and vulnerabilities from ML and TF while relying on continued feedback from the supervisory authorities and market participants.

The risk management process involves three main stages. Each stage is presented below in Graphic 2 and discussed in the next chapters.²⁶

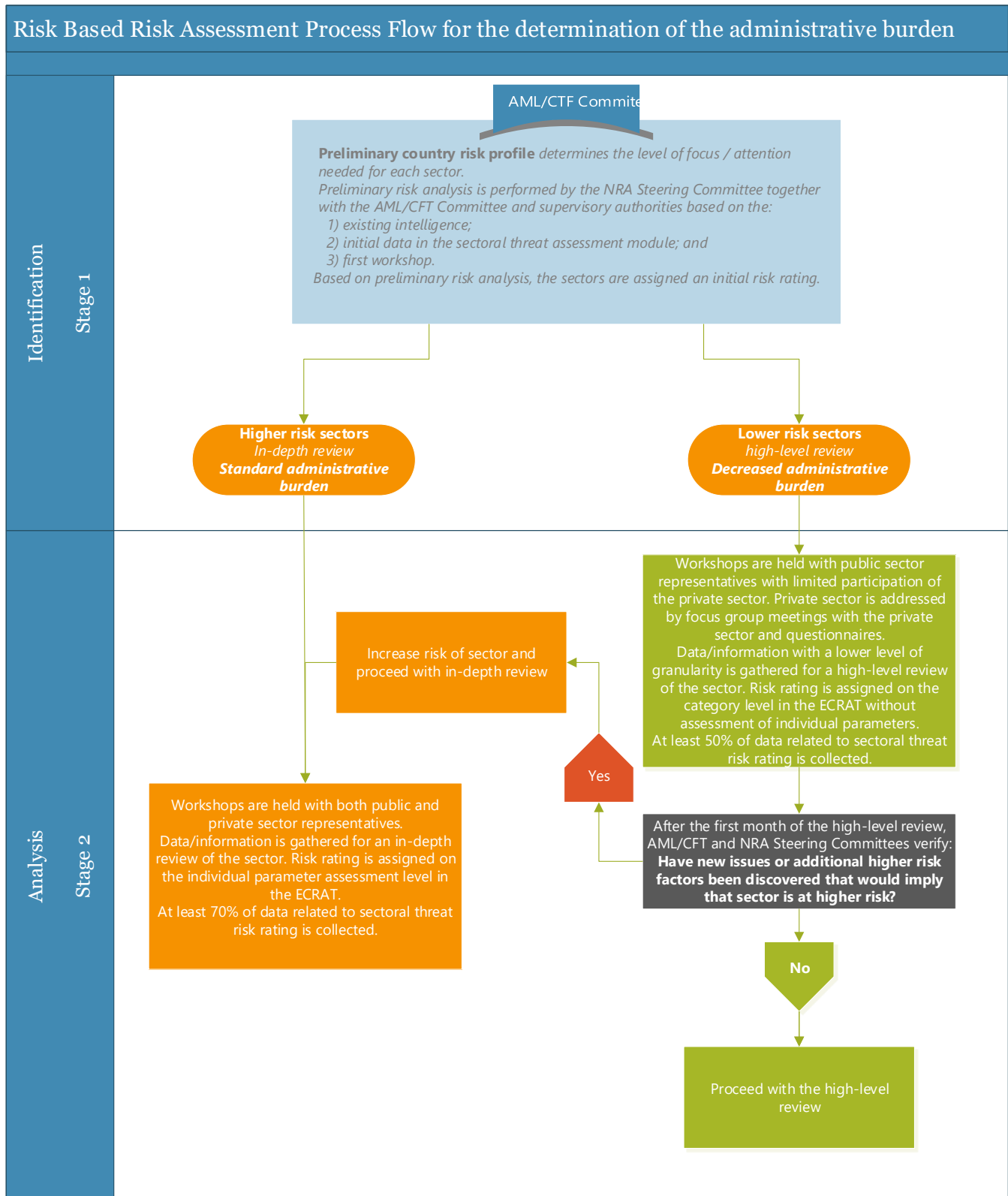
Graphic 2. Risk Management Process



The NRA opening meeting will include an overview of the country’s understanding of risk, which will complement the review of the country’s NRA. Based on the preliminary assessment of the country, the NRA Steering Committee may identify specific areas to apply increased attention. In doing so, the team will increase its efficiency and decrease administrative burden for certain sectors. If the NRA Steering Committee identifies new issues that need to be explored or if further clarification is needed on an issue already discussed, then a more in-depth review is required and time should be set aside for additional meetings and data gathering activities. Refer to Graphic 3 below for different focus levels of assessment.

²⁶ FATF National Money Laundering and Terrorist Financing Risk Assessment: http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

Graphic 3. Level of Assessment Options



3.1 Stage One: Identification

The NRA process begins with collecting data and gathering information. The objective is to identify the ML and TF risks to be analysed. Collecting data from sources such as national statistics is imperative to provide a strong evidence base for the assessment and thereby improve the objectivity of the assessment. Evidence is a mandatory element in a risk assessment, which becomes the foundation for the RBA. Gathering information through consultation with the relevant stakeholders is also important in order to gain an understanding of the economic, political, social, legal and technological risk factors.

3.1.1 Preliminary Country Risks Profile

Preliminary risk analysis includes the creation of the initial country risk profile that will further support subsequent discussions about threats and vulnerabilities. The risk profile includes: a list of the known or suspected threats and vulnerabilities that exist; the key sectors that have been exploited; and the primary reasons why those carrying out the ML/TF are not apprehended and or deprived of their assets.

Preliminary research performed as of 15/02/2019 can be found in Appendix 2, and sources of such research include, *inter alia*:

- Reports by international organisations (e.g., United Nations (hereinafter “UN”), WB Group, International Monetary Fund, World Customs Organisation, Basel Institute on Governance, World Trade Organisation, etc.);²⁷
- Reports by international bodies that set standards (e.g., Financial Action Task Force and FATF-Style Regional Bodies);²⁸
- Reports by governments/think-tanks/civil society organisations/private institutions;²⁹
- Books/articles/reports based on academic research;
- Media/Internet/other sources of public information;
- MLTF Prevention Act of Estonia³⁰ and other relevant legislation;³¹
- International Conventions, recommendations or guidelines (for example, UN Conventions, EU legislation, FATF Recommendations, guidelines issued by the Basel Committee on Banking Supervision, etc.);³²
- SNRA reports and recommendations;³³ and
- Reports of Estonian FIU and other regulatory and supervisory bodies.³⁴

²⁷ For example: <https://www.imf.org/en/News/Articles/2018/03/19/mcs031918-republic-of-estonia-staff-concluding-statement-of-the-2018-article-iv-mission>.

²⁸ For example: <https://www.coe.int/web/moneyval/jurisdictions/estonia>.

²⁹ For example: <https://www.knowyourcountry.com/estonia1111>.

https://www.transparency.org/whatwedo/publication/national_integrity_system_assessment_estonia.

³⁰ MLTF Prevention Act: <https://www.riigiteataja.ee/en/eli/517112017003/consolide>.

³¹ For example of other relevant legislation can be found in the Appendix 10 – Relevant legislation.

³² For example: https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2017.pdf.

³³ AML/CFT: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en.

³⁴ For example: <https://www2.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/annual-reports-of-fiu/>
<http://www.kriminaalpoliitika.ee/et/statistika-ja-uuringud/kuritegevus-eestis>.

Additional input from the intelligence services (such as information obtained from paid or restricted sources or threat intelligence obtained during the analysis of the deep web and dark web). The ‘deep web’ refers to anything that a search engine cannot find (e.g. government databases contain deep web content). The ‘dark web’ a small portion of the deep web that has been intentionally hidden and is inaccessible through standard web browsers. It is recommended that the dark web search be performed by law enforcement agencies.

Typical search strings that can be applied in order to find ML/TF-related information from public sources are listed below.

English	<i>Estonia (and either of the following terms) bribery; corruption; crime; deception; embezzlement; FCPA; fine; fraud; investigation; confiscation; litigation; money laundering; murder; penalty; scam; scandal; SEC; theft; violation; sentence; FATF; NRA; Mutual Evaluation; sanctions; non-resident; terrorist financing; FIU; criminal offence; trafficking; drugs; smuggling; terrorism; extortion</i>
Russian	<i>Эстония (and either of the following terms) взяточничество; коррупция; преступление; обман; растрата; FCPA; штраф; мошенничество; расследование; конфискация; судебный процесс; отмывание денег; убийство; штраф; мошенничество; скандал; кража; нарушение; предложение; санкции; нерезидент; финансирование терроризма; уголовное преступление; торговли людьми; наркотики; контрабанда; терроризм; вымогательство</i>
Estonian	<i>Eesti (and either of the following terms) altkäemaks; korruptsioon; kuritegevus; petmine; omastamine; FCPA; trahvi; pettus; uurimine; konfiskeerimine; kohtuvaidlused; rahapesu; mõrv; karistus; pettus; skandaal; SEC; vargus; rikkumine; lause; FATF; NRA; Riiklik riskihindamine; Vastastikune hindamine; sanktsioonid; mitteresident; terrorismi rahastamine; Rahapesu andmehüroo kuritegu; kaubandus; ravimid; salakaubavedu; terrorismi; väljapressimine</i>

Using the following Google search operators³⁵ will improve the quality of searches:

OR or | – Search for X or Y. This will return results related to X or Y, or both;

AND – Search for X and Y. This will return only results related to both X and Y;

AROUND(X) – Proximity search. Find pages containing two words or phrases within X words of each other;

“Query” – Exact match search; and

Site:example.com – Site-specific search.

³⁵ Google Search Operators: The Complete List (42 Advanced Operators): <https://ahrefs.com/blog/google-advanced-search-operators/>.

3.1.2 Workshops & Questionnaires

As described previously, NRA workshops are established for the purpose of discussing and assessing the risk landscape in Estonia.

It is crucial that the NRA Steering Committee works closely with the respective supervisory authorities such as FSA, FIU, Estonian Bar Association, Ministry of Justice and Chamber of Notaries to coordinate NRA workshops.

The WG members analyse available information and current legislation, evaluate the effectiveness of supervision and prosecution and propose an estimated level of threat and vulnerability. The detailed assessment framework is discussed in subsequent chapters of this methodology as well as in the Estonian country-level risk assessment tool in Appendix 5.

The NRA workshops are structured according to the risk assessment modules:

- Threat Assessment;
- National Vulnerability Assessment; and
- Sectoral Vulnerability Assessments;
 - Financial sector;
 - Real estate sector;
 - Financial technology sector;
 - Trust and Company SP sector;
 - NPO sector;
 - Dealers sector;
 - Gambling sector; and
 - DNFBP sector (independent legal professionals and advisors, notaries and lawyers, auditors, trustees in bankruptcy, bailiffs).

Prior to the workshops, the NRA Steering Committee will select a sample of obliged entities to participate in the NRA questionnaires.

3.1.2a Risk-based Sampling

In order to increase the objectivity of the NRA, a risk-based sample of obliged entities is selected to participate in the NRA process. A risk-based sample is a non-statistical selection of items based on various intentional elements, such as:

- Overall observed **sectoral risk** level (i.e. a high-risk sector would warrant a larger sample size);
- **Systemic issues** in the country (i.e. the existence of systemic or significant ML/TF issues in a particular sector would warrant an increase in the sample size for the sector);
- **Size** of the entity (i.e. a representative sample includes different-sized entities from the sector);
- **Geographical region** within the country (i.e. a representative sample includes entities from different regions);
- Foreign and nationally registered entities;
- Type of **business activities**;
- Industry **knowledge**; and
- **Professional judgment**.

The objective is to select a representative portion of the obliged entities so that they would sufficiently represent the sector, providing a comprehensive overview. Administrative burden on the private sector

is reduced through sampling, as not all obliged entities are selected to participate in the NRA process. A sampling template can be found in Appendix 6.

3.1.2b Questionnaires

The purpose of the sector questionnaires is to provide an opportunity for the market participants to assess the ML and TF risks that are relevant within each sector. The questionnaires address several topics, such as sector-specific risks, adequacy of current legislation and the effectiveness of supervision. The questionnaire responses will provide a market-level viewpoint of the estimated level of threat and vulnerability that otherwise would be lacking from the NRA. Refer to Appendix 7 for the NRA questionnaires prepared for this methodology.

Prior to the workshops, the NRA Steering Committee will send the NRA questionnaires to the sample selection of obliged entities. The supervisory authorities should provide an official cover letter to accompany the questionnaire. The cover letter should incentivise the participants to provide comprehensive, accurate and timely responses. It is advised that supervisory authorities serve as a point for escalation for participants that don't respond.

In order to increase efficiency, it is advised that the NRA questionnaires be sent to participants via a cloud-based platform³⁶. The online platform is one of the most widely utilised survey methods and allows for the systematic gathering of data from the participants. The benefits of a cloud-based platform include, *inter alia*:

- User- and environmentally-friendly medium;
- Rapid deployment of the questionnaires;
- Internet facilitates low-cost and fast data collection;
- Increase in response rates; and
- Automation of data input, handling, and aggregation.

Online surveys provide the highest level of convenience for the respondents and are the optimal recourse to decrease the administrative burden and compliance costs on the obliged entities.

3.1.3 Understanding Threat

A risk is defined as the ability of a threat to exploit a vulnerability of a given sector for the purpose of perpetrating ML and TF. The ECRAT in Appendix 5 guides the country through the process of threat and vulnerability identification. The logic behind the Threat Assessment Module is described below.

A threat in the ML/TF context can be understood as the potential for illicit proceeds to enter the national economy or the use of funds by perpetrators for TF purposes. Money generated from different types of crimes can enter the economy via different channels. These channels can represent various sectors of the economy or, alternatively, different foreign countries acting as partners in cross-border transfers.³⁷

The main objective of threat identification is to understand ML and TF threats in terms of predicate offence type, geography and sector.

³⁶ The evaluation of the cloud-based infrastructure used should be done in accordance to the national infrastructure security standards and should be addressed before sharing any information.

³⁷ The International Monetary Fund Staffs' ML/FT NRA Methodology: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_IMF.pdf.

3.1.3a Predicate Offence Threat

This chapter focuses on assessing the predicate offences, which generate proceeds of crime and fund acts of terror. The following is a non-exhaustive list of predicate offences³⁸ to be considered for NRA purposes:³⁹

Economic offences:	Cybercrime
	Corruption and bribery
	Counterfeiting and piracy of products
	Extortion
	Fraud
	Fraud affecting the country financial interests
	Illegal Gambling
	Insider trading and market manipulation
	Money Counterfeiting
	Smuggling (including in relation to customs and excise duties and taxes)
	Tax crimes (related to direct taxes and indirect taxes)
Social offences:	Environmental crime
	Forgery
	Illicit arms trafficking
	Illicit trafficking in narcotic drugs and psychotropic substances
	Illicit trafficking in stolen and other goods
	Kidnapping, illegal restraint and hostage-taking
	Murder, grievous bodily injury
	Participation in an organised criminal group and racketeering
	Piracy
	Robbery or theft
	Sexual exploitation, including sexual exploitation of children
	Terrorism, including terrorist financing
	Trafficking in human beings and migrant smuggling

³⁸ SNRA Questionnaire on data regarding AML and CFT.

³⁹ The predicate offence categorisations can be determined by the WGs based on the values that they affect – patrimonial or personal / human, which is how we determined the classification. This classification does not follow the EE Criminal Act or any other criminal / penal legislation and was purely performed for the purpose of the NRA.

The predicate offences are quantified and assessed using the following non-exhaustive list of data.⁴⁰ This evidence provides for a strong foundation from which an objective conclusion can be reached.

- Number of cases detected;
- Number of cases investigated;
- Number of cases prosecuted;
- Number of convictions;
- Amount of proceeds seized;
- Amount of proceeds frozen;
- Amount of proceeds confiscated;
- Other Information (including FIU analysis and intelligence); and
- Estimate of the relative size of undetected criminal proceeds (grey economy) related to each offence (%).

It is important to note that data is collected separately for predicate offences, ML and TF offences. This data or evidence allows for objective decision making regarding the overall predicate offence threat.

3.1.3b Sectoral Threat

This chapter focuses on assessing the sectors in which the proceeds of crime are invested and laundered. The list of sectors that are subject to the risk assessment was provided in Chapter 1.3.

For sectoral threat identification, both qualitative and quantitative data is taken into consideration.

This data includes, *inter alia*:⁴¹

- Number of reports received from the obliged entities in each sector;
- Number of FIU cases;
- Number of requests for information made to obliged entities;
- Number of decisions to suspend or withhold consent to a transaction;
- Number of ML and TF prosecutions involving the sector;
- Number of ML and TF convictions involving the sector;
- Estimate of the relative size of undetected criminal proceeds (grey economy) related with each sector (%); and
- Other information on potential ML and TF activities related to sector (qualitative: public information, academic reports, intelligence, etc.)

This data helps to identify obliged entities and subsequent sectors where ML and TF threats are higher. This collection of this data is evidence upon which an objective conclusion on a sectoral threat can be reached.

⁴⁰ The full data set used to assess the predicate offence threat can be found in the Threat Assessment Module (Predicate Offence bookmark) in Appendix 5.

⁴¹ The full data set used to assess the predicate offence threat can be found in the Threat Assessment Module (Sectoral bookmark) in Appendix 5.

3.1.3c Geographical Threat

This chapter focuses on the identification of patterns regarding the jurisdictional origin of the proceeds of crime. This may be particularly relevant in cases where the predicate offence to ML or TF was committed in a foreign jurisdiction.

To assess a cross-border threat, the country identifies the top countries from the perspective of financial flows in the EU, outside of the EU and from/to offshore or high-risk jurisdictions.

It is recommended that not only those countries with which the cumulative sum of inflows/outflows is high be included in the sample but also countries with unexpected peaks in certain money-flow categories, such as inflows or outflows related to:⁴²

- Trade in goods;
- Services;
- Real estate;
- Foreign direct investment;
- Portfolio investments;
- Money service business inflows; and
- Remittances.

The countries identified as representing an important part of international financial flows for Estonia are further assessed from the perspective of cooperation, ML and TF threats.

3.1.4 Understanding Vulnerability

A risk is defined as the ability of a threat to exploit a vulnerability of a given sector for the purpose of perpetrating ML and TF. The ECRAT in Appendix 5 guides the country through the process of threat and vulnerability identification. The logic behind the National and Sectoral Vulnerability Assessment Modules is described below.

The vulnerability rating reflects the effectiveness of national AML/CFT controls in preventing and detecting ML and TF activities.

The NRA report outlines the legal and regulatory framework governing the AML/CFT regime. For this assessment, the WG takes into consideration the following:

- Relevant laws, regulations and enforceable directions;
- Findings from supervisory authorities;
- Reports from governments and/or international organisations; and
- Reports from academia and/or civil society organisations.

3.1.4a National Vulnerability

The legal framework assessment should be used as a basis for the national vulnerability assessment. The FATF has described eleven Immediate Outcomes (as presented in Table 3 below), which are the thematic goals of an AML/CFT system that is effectively protecting financial sector integrity and contributing to safety and security. The Estonian national vulnerability assessment is structured around

⁴² The full data set used to assess the predicate offence threat can be found in the Threat Assessment Module (Geography bookmark) in Appendix 5.

those Immediate Outcomes, with additional indicators taken into consideration. Moreover, additional vulnerabilities could be derived from analysing international rankings of Estonia, such as:

- Basel AML Index;
- Transparency International Corruption Index;
- World Governance Indicator – Control of Corruption;
- Fragile States Index (Fund for Peace);
- Compliance with FATF Recommendations (Last Mutual Evaluation);
- International Narcotics Control Strategy Report Summary (Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State); and
- Trafficking in Persons Report Summary (Office to Monitor and Combat Trafficking in Persons, U.S. Department of State).

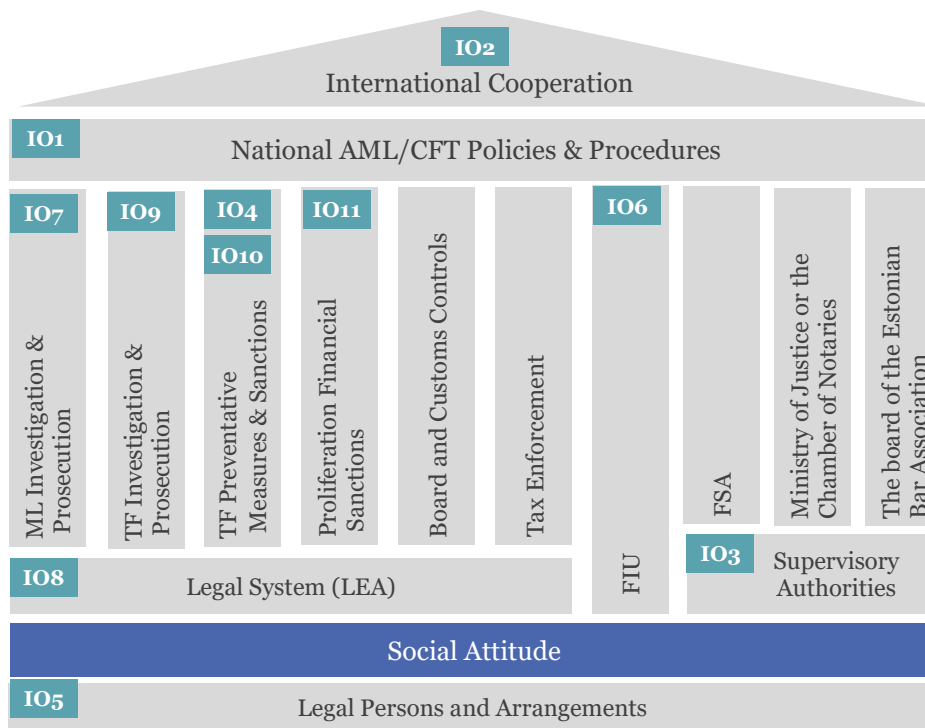
Table 3. FATF Immediate Outcomes⁴³

No.	Intermediate Outcomes	Immediate Outcome (IO)
IO 1	<i>Policy, coordination and cooperation mitigate the ML and TF risks.</i>	ML and TF risks are understood and, where appropriate, actions are coordinated domestically to combat ML, TF, and PF.
IO 2		International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
IO 3	<i>Proceeds of crime and funds in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.</i>	Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.
IO 4		Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.
IO 5		Legal persons and arrangements are prevented from misuse for ML or TF, and information on their beneficial ownership is available to competent authorities without impediments.
IO 6		Financial intelligence and all other relevant information is appropriately used by competent authorities for ML and TF investigations.
IO 7	<i>ML threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds. TF threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned, thereby contributing to the prevention of terrorist acts.</i>	ML offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.
IO 8		Proceeds and instrumentalities of crime are confiscated.
IO 9		TF offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.
IO 10		Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.
IO 11		Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

⁴³ FATF: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html>.

The FATF’s Immediate Outcomes are linked to the Estonian financial crime prevention system below.

Graphic 4. Hallmarks of the National Vulnerability Assessment



3.1.4a.1 Legal Framework Assessment

The legal framework assessment, as part of the NRA, includes various elements, such as the AML/CFT system, policies, operations, supervisory and licensing authorities and the risk landscape. ⁴⁴

The WG will prepare a brief overview of the **significant changes in the AML/CFT system**, which have taken place since the last evaluation and subsequent follow-up reports. Any measures that are not already in place must be clearly identified in the responses on technical compliance. Elements of the AML/CFT system to review are listed below.

- Estonian MLTF Prevention Act;
- All legislation relevant from the ML/TF perspective;
- Significant changes to the AML/CFT laws or regulations;
- New competent authorities; and
- Significant reallocation of duties between existing competent authorities.

A summary of the **AML/CFT roles and responsibilities** will also be prepared. Each competent authority briefly describes its roles and responsibilities in the detection, prevention and suppression of ML, TF and PF, at the national level. The designation of new authorities and any other relevant institutional change in the context of the fight against ML and TF are highlighted. Moreover, the specific legal provision (full references of relevant article(s) and act) setting out the AML/CFT responsibilities should be highlighted. This also includes monitoring bodies for non-financial businesses and professions, including self-regulating bodies (as defined in the FATF

⁴⁴ MONEYVAL’s 5th Round Mutual Evaluation Questionnaire.

Recommendations⁴⁵). For each FATF Recommendation, the responsible competent authority lists all the relevant legislation briefly describing in a high-level summary of their scope – highlighting when new legislation was adopted since the previous evaluation report.

Lastly, the **competent authorities** will also provide an overview concerning:

- The risk landscape of Estonia, in particular any ML/TF risk assessment(s), whether sectoral or focused on a particular type of obliged entities;
- Documents relating to sectoral risk analysis (e.g. Estonian National Security Strategy);
- Licensing/registration authorities and AML/CFT supervisory authorities; and
- Any other document helping to understand the context of the fight against ML and TF (political context, institutional framework, judicial system, etc.).

3.1.4b Sectoral Vulnerability

In order to determine its vulnerability to ML and TF, each sector is assessed against the following categories.⁴⁶ The WB methodology was used as a basis for this framework; however, the methodology was enhanced to build a more comprehensive and country-focused control assessment framework. Additional elements were added, *inter alia*: quality of the TF and sanctions detection, quality of the responses to risks identified during previous assessments, and quality of sector specific controls, as described below.

- *Legal Framework*. This is measured by assessing the comprehensiveness of the Estonian AML/CFT legal framework and its subsequent incorporation in sector-level policies, procedures and guidelines;
- *Quality of Supervision*. This is measured by the effectiveness of the supervision procedures and practices and the enforcement of sanctions;
- *Commitment and Leadership of Management*. There are a number of indicators that can directly or indirectly influence this category, such as:
 - Level of market pressure to meet AML/CFT standards (e.g. international pressure from correspondent banks for the financial sector);
 - Availability and effectiveness of entry controls (e.g. licencing requirements, shareholders transparency checks); and
 - Integrity of staff.
- *Effectiveness of Compliance Systems and Reporting*. This is measured by an overall assessment of the compliance systems, and by a targeted assessment of the effectiveness of the monitoring and reporting of suspicious activity.
- *Quality of CDD Framework*. In order to determine this, an understanding of the availability and access to reliable identification infrastructure and beneficial ownership information must be obtained. This is measured by the effectiveness of CDD measures in higher risk situations.
- *Quality of TF Detection and Prevention of PF*. This assessment includes the counter financing of terrorism and prevention of PF focused legal framework for the sector, screening against lists of persons, groups and entities involved in terrorist acts, CFT staff knowledge, etc.
- *Quality of Sectoral Sanctions Detection*. This assessment includes the sanctions screening capabilities, reporting identified sanctioned persons, groups and entities, and enforcement of asset freezing.

⁴⁵ FATF Recommendations: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

⁴⁶ The World Bank National Risk Assessment Methodology.

- *Quality of the Responses to Risks Identified during Previous Assessments.* A number of findings (risks that require mitigating action) were identified in the previous NRA and Mutual Evaluations. The WG determines the overall quality of response measures. The quality of response measures can be measured by the existence of clear action plans that were enforced in a timely manner and the overall improvement of the previously evaluated areas. Moreover, a non-exhaustive list of specific sector controls and sources can be found in Appendix 8 and 9, respectively. Sector controls are typically divided into the following groups:
 - Country-level control – mechanisms for the prevention of ML and TF on the country-level;
 - Stakeholder level control – controls on the level of the sector or individual obliged entities; and
 - Information technology general control – controls that either governmental bodies or obliged entities apply to reduce ML and TF risk by implementing technological solutions.

The above-described framework is the same for all sectors; however, sector-specific risks need to be taken into consideration. Therefore, sectors are assessed with regard to:

- *Additional Controls*
ML and TF techniques are rapidly evolving; therefore, the assessment sheet provides an option to add additional controls, such as:
 - Controls associated with newly emerged risks; and
 - Additional controls for previously identified risks.
- *Quality of Sector Specific Controls*
The sector-specific controls are subject to thorough discussions for each particular sector. The risks were derived from discussions with representatives from the Estonian private and public sector, as well as from the recent ML and TF typology reports.

3.2 Stage Two: Analysis

To decrease the level of subjectivity, it is important to introduce quantification to the risk assessment process. Graphic 5 below describes different levels of granularity on which those risks are quantified.

Level 1 presents the final calculation of the Country Exposure Risk Rating (hereinafter “CERR”). CERR is a function of the country’s vulnerability rating (hereinafter “VR”) and threat risk rating (hereinafter “TRR”). In order to further promote a TF risk overview on different dimensions, there is a CERR for TF and PF that is separate from the CERR for ML.

The CERR calculation mechanism is described in Chapter 3.2.1.

The actual calculation takes place in a separate module of the ECRAT – NRA CERR Heat map.⁴⁷

⁴⁷ The ECRAT can be found in Appendix 5.

Level 2 presents the composing elements of the country VR and the country TRR. As mentioned above, there is a separate TF assessment element for both VR and TRR.

The TRR and VR calculations are described in Chapters 3.2.2 and 3.2.3, respectively.

The actual calculation takes place in separate modules of the ECRAT – NRA Threat Assessment Module, NRA National Vulnerability Assessment Module and NRA Sectors Vulnerability Assessment Module.⁴⁸

Level 3 provides guidance on the assessment of various elements needed to calculate the TRR and VR. The clear and transparent indicators provided for probability, consequence, control design and operating effectiveness promote objectivity.

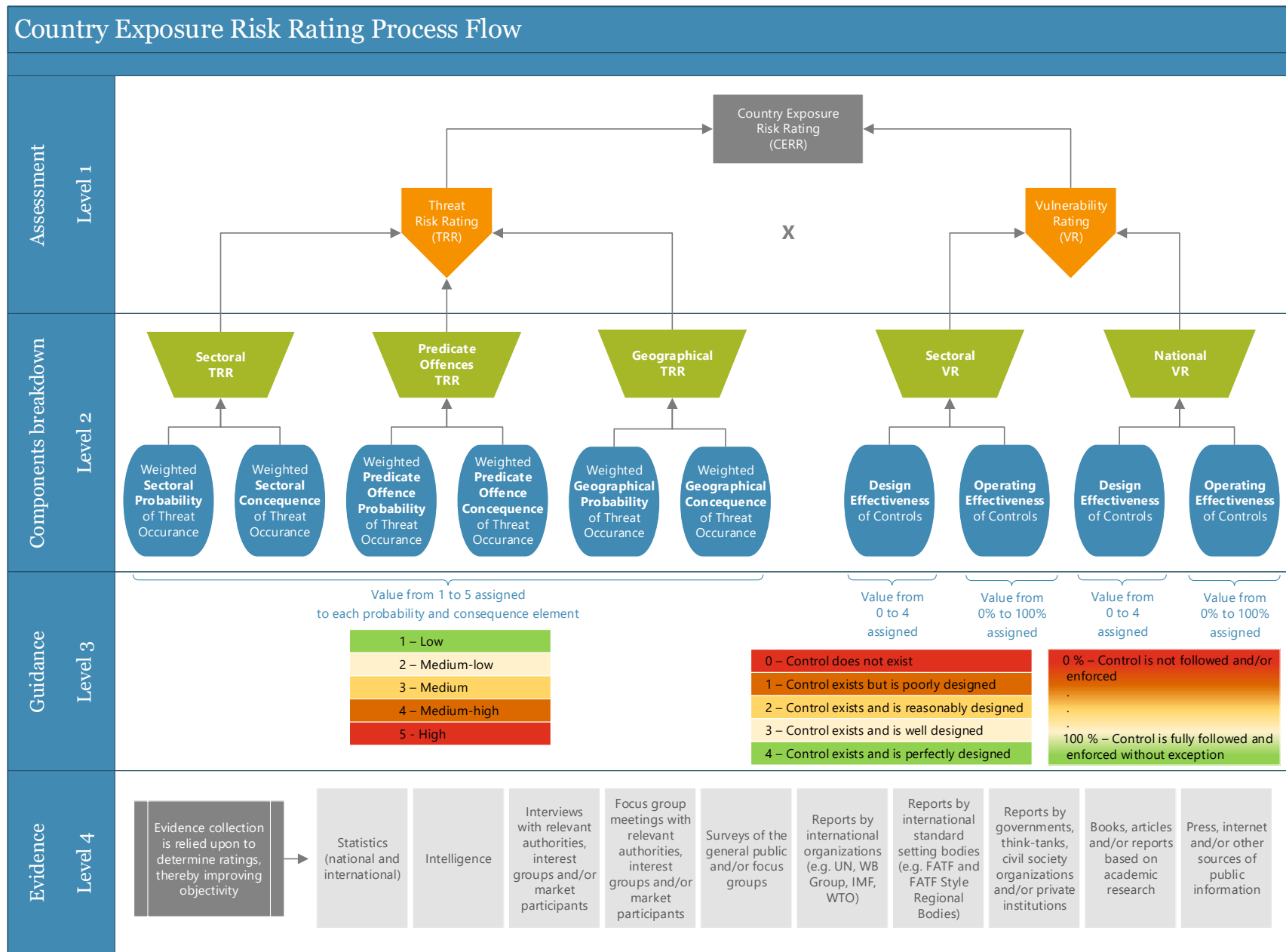
The guidance is provided in Chapters 3.2.1 and 3.2.3.

Level 4 requires evidence to provide a stronger foundation of objectivity. All Threat and Vulnerability Assessment Modules of the ECRAT⁴⁹ give an overview of which evidence should be collected in order to make an informed decision.

⁴⁸ Ibid.

⁴⁹ Ibid.

Graphic 5. Country Exposure Risk Rating Process Flow



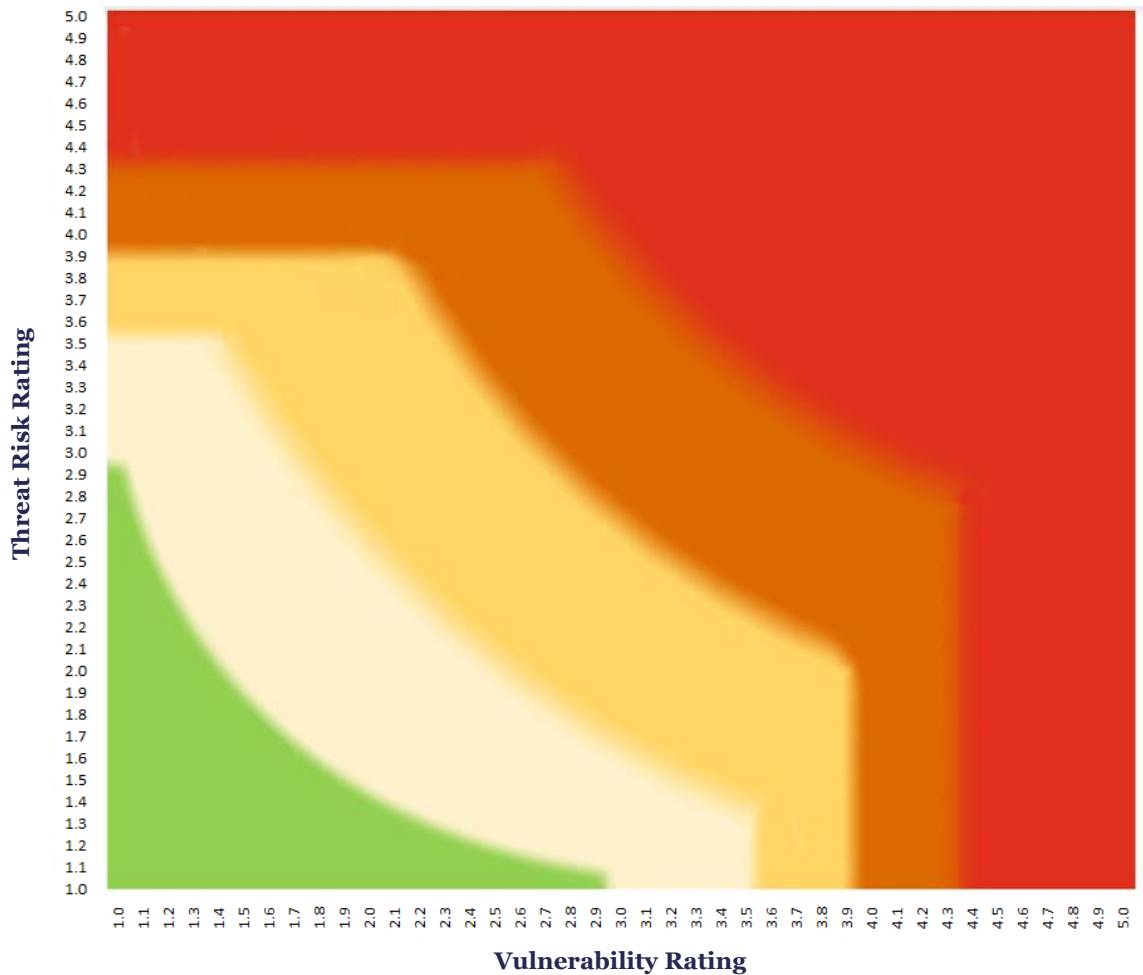
3.2.1 Country Exposure Risk Rating (CERR)

The country exposure risk relating to ML and TF is a function of threat and vulnerability, which can be graphically observed in the heat map in the ECRAT. An illustration of the heat map is shown below in Graphic 6, and the annotation of its colours is in Table 5 below. Following this methodology, CERR is a quantitative expression of country-specific and systemic risks relating to ML and TF. As described below, CERR has a strong evidence foundation providing an objective understanding of the Estonian risk landscape.

Threat in the ML/TF context can be understood as the potential of illicit proceeds to enter the national economy or the use of funds for TF. Money generated from different types of organised crime can enter the economy via different channels. These channels can represent various sectors of the economy, or, alternatively, different foreign countries acting as partners in cross-border transfers.

Vulnerability, on the other hand, reflects weaknesses in the national AML/CFT system or country-wide controls allowing the exploitation of ML or TF opportunities. Vulnerabilities can include poorly designed policies, but also controls which are not respected or enforced.

Graphic 6. Heat Map



Horizontal axis represents VR.

Scale: As described in Chapter 3.2.3, the VR is initially measured on a scale from 0.0 to 4.0. However, for the purpose of creating an accurate heat map, the scale was shifted by +1, i.e. from 1.0 to 5.0.

Vertical axis represents TRR.

Scale: from 1.0 to 5.0

The heat map is based on the multiplication of the TRR and VR, which results in values between 1.0 and 25.0. The annotation of the colours present in the heat map can be found in Table 4 below.

Table 4. Initial thresholds used for the heat map

	Result of calculation	Risk level
TRR * VR	≥ 12 (12 and above)	High
	$8 \leq TRR * VR < 12$ (8 and more AND below 12)	Medium-high
	$5 \leq TRR * VR < 8$ (5 and more AND below 8)	Medium
	$3 \leq TRR * VR < 5$ (3 and more AND below 5)	Medium-low
	$0 \leq TRR * VR < 3$ (0 and more AND below 3)	Low

In order to draw attention to high-threat or high-vulnerability situations, additional areas of higher risk (“legs”) were added in the upper left quadrant and lower right quadrant of the heat map. The concept is that the final risk assessment should not be medium or low when either TRR or VR is high. For example:

- **High Threat, Low Vulnerability** – even with a strong control mechanism on the sectoral or national level, it remains attractive to perpetrators. This situation might result in the development of more sophisticated ML or TF techniques, which are not addressed by current controls.
- **Low Threat, High Vulnerability** – although neither the sector nor the whole country were yet substantially abused for ML or TF purposes (or the abuse was not yet discovered), the lack of strong controls might increase the attractiveness of it to criminals or terrorists.

To capture this type of combination, additional areas were added in the upper left quadrant and lower right quadrant to highlight a higher category of risk.

This resulted in more advanced heat map thresholds represented in the table below:

Table 5. Final thresholds used for the heat map

Parameters	Risk level
$TRR * VR \geq 12$ OR $TRR \geq 4.4$ OR $VR \geq 4.4$	High
$8 \leq TRR * VR < 12$ (* and more AND below 12) OR $4.0 \leq TRR < 4.4$ (TRR 4 or more AND below 4.4) OR $4.0 \leq VR < 4.4$ (VR 4 or more AND below 4.4)	Medium-high
$5 \leq TRR * VR < 8$ (5 and more AND below 8) OR $3.6 \leq TRR < 4.0$ (TRR 3.6 or more AND below 4.0) OR $3.6 \leq VR < 4.0$ (VR 3.6 or more AND below 4.0)	Medium
$3 \leq TRR * VR < 5$ (3 and more AND below 5) OR $TRR < 3.6$ (TRR below 3.6) OR $VR < 3.6$ (VR below 3.6)	Medium-low
Otherwise	Low

Threat Risk Rating (TRR)

As suggested above, a TRR can be analysed from different perspectives. It is suggested that different approaches be combined in order to achieve a more accurate result.

As outlined below, the country’s TRR is calculated as a weighted average of the threat risk for economic sectors (“sectoral threat risk rating”), linked to different types of organised crime where the proceeds can represent a ML or TF threat (“predicate offence threat risk rating”) and linked to foreign countries subject to cross-border transfers (“geographical threat risk rating”).

$$TRR_{total} = w_{SEC} \times TRR_{SEC} + w_{PO} \times TRR_{PO} + w_{GEO} \times TRR_{GEO}$$

Where

w_{SEC} Weight of sectoral threat risk rating is 40%;⁵⁰

w_{PO} Weight of predicate offence threat risk rating is 40%;⁵¹ and

w_{GEO} Weight of geographical threat risk rating is 20%.⁵²

This is explained by the fact that a geographical threat is also factored in at the level of predicate offence and sectoral assessments.

⁵⁰ All proposed weights which should be discussed and confirmed by the working groups.

⁵¹ Ibid.

⁵² Ibid.

Introduction to Probability and Consequence

On all three threat levels, two different aspects are considered in the quantification of the threat risk – the *probability* (P) and the *consequence* (C). The assessment of the probability and consequences to measure threats can be used as a way to identify and rank top 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, refer to Table 6 below.

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, refer to Table 7 below.

Threat is calculated as a weighted average *probability* and *consequence*, which allows the assessors to increase the significance of the impact of ML/TF occurring in the overall formula. It is recommended that consequences of ML/TF have a slightly larger weight than probability due to the negative impact on the national economy or welfare of Estonian citizens if ML/TF occurs. The total sum of the *probability* and *consequence* weights must equal 100%.

For example, the individual TRR (TRR_{ind}) for a particular type of entity in a given sector (e.g. credit institutions in the financial sector) is calculated as the weighted average of *probability* of the threat occurring and the *consequence* of the threat occurring.

$$TRR_{ind} = w \times P + (1 - w) \times C$$

Table 6. Thresholds used for probability

Probability Score	Probability	Description
1	Low	Event likely to occur once in three or more years
2	Medium-low	Event likely to occur on an annual basis
3	Medium	Event likely to occur more than once on an annual basis, but not on a monthly basis
4	Medium-high	Event likely to occur on a monthly basis
5	High	Event with an ongoing effect or occurring on a daily basis

Consequence (abbreviated in Table 7 below as “C”)

Table 7. Thresholds used for consequence and descriptions of implications⁵³

Score	C	Description of implications			
		National security implications	Economic implications	Political implications (country reputation)	Social implications
1	Very low	<ul style="list-style-type: none"> ♦ Insignificant impact on national security systems 	<ul style="list-style-type: none"> ♦ Insignificant impact on economy 	<ul style="list-style-type: none"> ♦ Insignificant impact on country’s reputation 	<ul style="list-style-type: none"> ♦ Insignificant impact on society
2	Low	<ul style="list-style-type: none"> ♦ Minor cybercrime attacks on computer infrastructure and databases, not involving loss of data or any confidential information 	<ul style="list-style-type: none"> ♦ Slight increase in interest rates (up to X %) ♦ Slight increase in inflation (up to X %) 	<ul style="list-style-type: none"> ♦ Minor increase in disputes and proceedings with regulators ♦ Local and small public media attention 	<ul style="list-style-type: none"> ♦ Minor increase in underlying criminal activity (X %)
3	Medium	<ul style="list-style-type: none"> ♦ Average cybercrime attacks on computer infrastructure and databases, involving losses in privacy or financial data ♦ Additional budget allowance for securing computer infrastructure and databases ♦ Monetary loss due to disclosure of information (up to X %) 	<ul style="list-style-type: none"> ♦ Slight decline in financial inclusion ♦ Loss of financial data (due to cybercrime attacks) ♦ Increased interest rates (up to X %) ♦ Increased inflation (up to X %) ♦ Slight decrease in credibility / customer trust ♦ Encumbrance of international correspondent banking relationships ♦ Slight decline in stock value of financial institution (up to X %) ♦ Decrease in foreign investment (up to X %) ♦ Slight decrease in financial sector growth rate (up to X %) 	<ul style="list-style-type: none"> ♦ Increasing interest by international regulators, including investigations ♦ International disputes and proceedings with regulators ♦ International public media attention, including political scandals 	<ul style="list-style-type: none"> ♦ Increase in underlying criminal activity (X %) ♦ Perceived complicity of financial institutions ♦ Increasing disapproval from public, weakening ethical and democratic standards ♦ Slight depopulation of the county (up to X %) ♦ Slight decrease in availability of jobs (up to X %)
4	High	<ul style="list-style-type: none"> ♦ High cybercrime attacks on computer infrastructure and databases, involving losses in confidential information ♦ Impact on decreasing level or reliability of operations on information, computer and telecommunication systems ♦ Terrorist attacks with no human victims ♦ Monetary loss due to disclosure of confidential information (up to X %) 	<ul style="list-style-type: none"> ♦ Decline in financial inclusion, impacting local businesses ♦ Loss of financial data (due to cybercrime attacks), including confidential customer and account data ♦ Increased interest rates (up to X %) ♦ Increased inflation (up to X %) ♦ Decrease in credibility / customer trust (including international business relationships) ♦ Limitation of financial products / services concerning international correspondent banking relationships 	<ul style="list-style-type: none"> ♦ International media interest and political scandals, having long-term implications on the country’s image ♦ Classified among “non-cooperating countries and territories” by FATF ICRG ♦ Slight impact on political stability caused by encumbrance of international affairs 	<ul style="list-style-type: none"> ♦ Organised crime infiltrated in financial institutions/sectors of economy ♦ Increasing exposure to drug trafficking, smuggling and other criminal activity ♦ Undermining legitimate private sector businesses ♦ Increased costs concerning strengthening law enforcement and prosecutorial systems (up to X %) ♦ Undermining social credibility and legitimacy

⁵³ FATF National Risk Assessment: http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

			<ul style="list-style-type: none"> Decline in stock value of financial institution (up to X %) Decrease in foreign investment (up to X %) Increase in underground economy and associated reduction in tax revenue Loss of trust and goodwill of stakeholders in financial institutions Decrease in financial sector growth rate (up to X %) 		<ul style="list-style-type: none"> Deterioration in the quality of life Decrease in entrepreneurial drive
5	Very high	<ul style="list-style-type: none"> Significant cybercrime attacks on computer infrastructure and databases, involving disclosure of National Secrets (classified information), increased damage on national operation level on information, computer and telecommunication systems Terrorist attacks with human victims producing panic among population or financial crisis. 	<ul style="list-style-type: none"> Decline in financial inclusion, impacting national economy Loss of financial data (due to cybercrime attacks), including confidential customer data Significant increase in interest rates (up to X %) Significant increase in inflation (up to X %) Significant decrease in credibility / customer trust (including international business relationships) Termination of international correspondent banking relationships Significant decline in stock value of financial institution (up to X %) or bankruptcies, leading to financial crisis Significant increase in underground economy and associated reduction in tax revenue Loss of trust and goodwill of stakeholders in financial institutions Almost no growth rate (or drop by X%) in the financial sector Almost no foreign direct investment/ drop by X %) Destabilisation in financial markets Crowding out of private sector businesses unable to compete with organised crime using illicit money funding 	<ul style="list-style-type: none"> Significantly undermined reputation for integrity and compliance Termination of international business relationships Classified among "call for action" by FATF ICRG Political destabilisation 	<ul style="list-style-type: none"> Increased complicity of financial institutions Deteriorating social image of democracy and the rule of law Collective ethical and democratic standards seriously weakened Pronounced increase in underlying criminal activity (by X %) Significant exposure to drug trafficking, smuggling and other criminal activity Significant costs concerning strengthening the law enforcement and prosecutorial systems Social panic, leading to serious depopulation of the country Destruction of entrepreneurial drive

The country should determine the percentage change for indicators in both the economic and social implications categories (e.g. Low Risk - Slight increase in interest rates up to X %).

These determinations should be made based on the following:

- Macroeconomic analysis; and
- Risk appetite of the country (i.e. level of ML/TF risk the country is willing to accept).

For the calculation of the weighted average, the probability and consequence ratings are assigned weights⁵⁴ of 45% and 55%, respectively. The consequences of ML or TF on the country-level have a slightly larger importance than probability, as they have more impact on the national economy or welfare of Estonian citizens. This weighting allows the assessors to increase the significance of the impact of ML or TF occurring in the overall formula.

Concept of relative importance

Not all sectors or cross-border transfers bear the same importance to the overall ML and TF risks on the national level.

Importance in the risk assessment context refers to the weight in percent of a particular sector in the Estonian economy when calculating the threat risk rating. The estimation of importance is a subjective one, but general guidance is given to determine its value. The total sum of the importance ratings for one assessment element equals 100%.

For the **sectoral assessment**, the WG determines the importance of the:

- Individual entities within the sector (i.e. credit institutions represent X % of the whole financial sector, where the total for the sector is 100%); and
- Individual sectors within the population of all sectors selected for the purpose of the NRA (i.e. financial sector represents X % among all sectors, where the total for all sectors is 100%).

Further, when determining the importance ratings, also consider the following factors:

- Total assets;
- Contribution to GDP;
- Money flowing through the sector (not captured in GDP); and
- Strategic importance of the sector, etc.

⁵⁴ All proposed weights which should be discussed and confirmed by the working groups.

For the **geographical assessment**, the WG determines the importance of the individual countries selected for the in-depth review. This could be done based on the combination of the factors:

- Financial inflows;
- Financial outflows;
- Unexpected peaks in certain types of financial flows that generate more risk of ML or TF;
- Systemic risks connected with the country; and
- Level of international cooperation, etc.

The respective TRRs (geography, predicate offense, sectoral) are then calculated as individual TRRs weighted by their importance.

$$TRR = \sum TRR_{ind_t} \times importance_{ind_t}$$

3.2.2 Threat Risk Rating (TRR)

TOTAL THREAT RISK RATING (TRR_{total})

$$TRR_{total} = w_{SEC} \times TRR_{SEC} + w_{PO} \times TRR_{PO} + w_{GEO} \times TRR_{GEO}$$

TRR_{SEC} ... Sectoral threat risk rating

TRR_{PO} ... Predicate offences risk rating

TRR_{GEO} ... Geographical threat risk rating

w_{SEC} ... Weight of sectoral threat risk rating

w_{PO} ... Weight of predicate offence threat risk rating

w_{GEO} ... Weight of geographical threat risk rating

As described above, $w_{SEC} = 40\%$

$$w_{PO} = 40\%$$

$$w_{GEO} = 20\%$$

i.e. $TRR_{total} = 0.4 \times TRR_{SEC} + 0.4 \times TRR_{PO} + 0.2 \times TRR_{GEO}$

PREDICATE OFFENCES THREAT RISK RATING

For individual predicate offence (TRR_{PO_r})

$$TRR_{PO_r} = w_r \times P_r + (1 - w_r) \times C_r \quad \text{where } r = 1, 2, \dots, n$$

P_r ... Probability of threat occurrence for predicate offence r

C_r ... Consequence of threat occurrence for predicate offence r

w_r ... Weight used for the probability of threat occurrence for predicate offence r

$(1 - w_r)$... Weight used for the consequence of threat occurrence for predicate offence r

Naturally, different types of predicate offences have different impacts on the overall threat risk rating. It is recommended that these offences be split into at least the following two categories – economic and social offences.

Total predicate offence is then calculated as a weighted average of TRR for economic predicate offences and TRR for social predicate offences.

Total predicate offences (TRR_{PO})

$$TRR_{PO} = w_{EPO} \times TRR_{EPO} + (1 - w_{EPO}) \times TRR_{SPO}$$

TRR_{PO} ... Threat risk rating for total predicate offences

TRR_{EPO} ... Threat risk rating for economic predicate offences

TRR_{SPO} ... Threat risk rating for social predicate offences

w_{EPO} ... Weight used for the threat risk rating for economic predicate offences

$1 - w_{EPO}$... Weight used for the threat risk rating for social predicate offences

SECTORAL THREAT RISK RATING

For a particular group of entities⁵⁵ (TRR_{ENT_t})

$$TRR_{ENT_t} = w_t \times P_t + (1 - w_t) \times C_t \quad \text{where } t = 1, 2, \dots, n$$

P_t ... Probability of threat occurrence for the group of entities t

C_t ... Consequence of threat occurrence for the group of entities t

w_t ... Weight used for the probability of threat occurrence for the group of entities t

$(1 - w_t)$... Weight used for the consequence of threat occurrence for the group of entities t

For individual sectors (TRR_{SEC_s})

$$TRR_{SEC_s} = \sum TRR_{ENT_t} \times importance_{ENT_t} \quad \text{where } t = 1, 2, \dots, n$$

$$TRR_{SEC} = TRR_{ENT_1} \times importance_{ENT_1} + TRR_{ENT_2} \times importance_{ENT_2} + \dots + TRR_{ENT_n} \times importance_{ENT_n}$$

TRR_{SEC_s} ... Threat risk rating for sector s

TRR_{ENT_t} ... Threat risk rating for entity t in a given sector

⁵⁵ For example, as group of entities, consider credit institutions within the financial sector, casinos within the gambling sector, etc.

$importance_{ENT_t}$... Importance of entity t in the given sector

For sectors in total (TRR_{SEC})

$$TRR_{SEC} = \sum TRR_{SEC_s} \times importance_{SEC_s} \quad \text{where } s = 1, 2, \dots, n$$

$$TRR_{SEC} = TRR_{SEC_1} \times importance_{SEC_1} + TRR_{SEC_2} \times importance_{SEC_2} + \dots + TRR_{SEC_n} \times importance_{SEC_n}$$

TRR_{SEC} ... Threat risk rating for the entirety of sectors

TRR_{SEC_s} ... Threat risk rating for sector s in the economy

$importance_{SEC_s}$... Importance of sector s in the economy, to be determined based on the sector's relative contribution to GDP as compared to the total contribution to GDP of the selected sector.

GEOGRAPHICAL THREAT RISK RATING

For individual country (TRR_{GEO_v})

$$TRR_{GEO_v} = w_v \times P_v + (1 - w_v) \times C_v \quad \text{where } v = 1, 2, \dots, n$$

P_v ... Probability of threat occurrence in transfers with country v

C_v ... Consequence of threat occurrence in transfers with country v

w_v ... Weight used for the probability of threat occurrence in transfers with country v

$(1 - w_v)$... Weight used for the consequence of threat occurrence in transfers with country v

For cross border transfers in total (TRR_{CB})

$$TRR_{GEO} = \sum TRR_{GEO_v} \times importance_{GEO_v} \quad \text{where } v = 1, 2, \dots, n$$

$$TRR_{GEO} = TRR_{GEO_1} \times importance_{GEO_1} + TRR_{GEO_2} \times importance_{GEO_2} + \dots + TRR_{GEO_n} \times importance_{GEO_n}$$

TRR_{GEO} ... Geographical threat risk rating

TRR_{GEO_v} ... Threat risk rating for a particular country v

$importance_{GEO_v}$... Importance of country v in the total cross border transfers

3.2.3 Vulnerability Rating (VR)

The vulnerability rating is determined by considering the effectiveness of appropriate controls to mitigate the probability or the consequence of ML and TF risk. Some of these controls relate to a specific sector, others are implemented on a country-level, hence “sectoral vulnerability rating” and “national vulnerability rating”. The final vulnerability rating is then calculated as a weighted average of these two values.

$$VR_{total} = w_{SEC} \times VR_{SEC} + w_{CAS} \times VR_{CAS}$$

where,

w_{SEC} Weight of sectoral vulnerability rating is 40%⁵⁶

w_{CAS} Weight of national vulnerability rating is 60%⁵⁷

National vulnerability has a higher weight than sectoral vulnerability, as a strong AML/CFT defence system on the country-level subsequently drives the resilience of the respective sectors.

The vulnerability rating reflects the effectiveness of national AML/CFT controls in preventing and detecting ML and TF activities in a given sector. The effectiveness of controls is composed of two factors – design effectiveness and operating effectiveness.

Design effectiveness assesses whether or not a control is in place and whether it is designed appropriately. The variable is measured on a scale from 0 to 4, as follows:

- 0- Control does not exist
- 1- Control exists but is poorly designed
- 2- Control exists and is reasonably designed
- 3- Control exists and is well designed
- 4- Control exists and is perfectly designed

However, even an ideally designed control brings no benefit when it is not actually used. This is where the operating effectiveness component comes into place.

Operating effectiveness measures whether the control is put in operation, whether it produces the desired result, and whether it is followed and enforced. The variable is measured as a percentage value ranging from 0% (control is not followed and/or enforced) to 100% (control is fully followed and enforced without exception).

- 0% – Control is not followed and/or enforced
- 25% – Control is inconsistently followed and not enforced
- 50% – Control is reasonably followed and minimally enforced
- 75% – Control is consistently followed and enforced with exceptions
- 100% – Control fully followed and enforced without exception

⁵⁶ All proposed weights which should be discussed and confirmed by the working groups.

⁵⁷ Ibid.

Overall control effectiveness is calculated as the product of *design effectiveness* and *operating effectiveness*. For instance, there is a well-designed policy (e.g. design effectiveness of 3); however, it is not fully implemented in practice (e.g. operating effectiveness of 40%). The overall control effectiveness is 1.2, which is calculated by multiplying 3 times 40%.

$$\text{Control effectiveness} = \text{design effectiveness} \times \text{operating effectiveness}$$

The product of the design and operating effectiveness variables is then subtracted from the maximum value of vulnerability (4). This ensures that *VR* correlates to weaknesses in the control system, hence giving a numerical indication the vulnerabilities in the AML/CFT system.

$$VR = \text{max value} - (\text{design effectiveness} \times \text{operating effectiveness})$$

The overall vulnerability rating is calculated in two parts – a sectoral and country-wide rating. *Sectoral* rating addresses controls specific to individual sectors. *Country-wide* controls, on the other hand, include areas, such as law enforcement, legislation, the judicial system, etc., which relate to the country as a whole.

SECTORAL VULNERABILITY RATING (VR_{SEC})

For individual sectors (VR_{SEC_s})

$VR_{SEC_s} = \text{max value} - (\text{design effectiveness}_s \times \text{operating effectiveness}_s)$ where $s = 1, 2, \dots, n$
design effectiveness_s ... Design quality of a control for sector s , ranked as follows:

- 0- Control does not exist
- 1- Control exists but is poorly designed
- 2- Control exists and is reasonably designed
- 3- Control exists and is well designed
- 4- Control exists and is perfectly designed

operating effectiveness_s ... Operating effectiveness of a control in place for sector s , measured as a percentage of control enforcement

max value ... Maximum value of the indicator ($4 \times 100\% = 4$). This ensures that a higher *VR* number correlates to high vulnerability.

For sectors in total (VR_{SEC})

$$VR_{SEC} = \sum VR_{SEC_s} \times \text{importance}_{SEC_s} \quad \text{where } s = 1, 2, \dots, n$$

$$VR_{SEC} = VR_{SEC_1} \times \text{importance}_{SEC_1} + VR_{SEC_2} \times \text{importance}_{SEC_2} + \dots + VR_{SEC_n} \times \text{importance}_{SEC_n}$$

VR_{SEC} ... Vulnerability rating for the entirety of sectors

VR_{SEC_s} ... Vulnerability rating for sector s in the economy

importance_{SEC_s} ... Importance of sector s in the economy (Determination of importance is described in the paragraph “Concept of relative importance” above).

NATIONAL VULNERABILITY RATING

For country-wide assessment criterion (VR_{CAS_m})

$$VR_{CAS_m} = \max \text{value} - (\text{design effectiveness}_m \times \text{operating effectiveness}_m) \quad \text{where } m = 1, 2, \dots, n$$

design effectiveness_m ... Design quality of a control as per assessment criterion *m*, ranked as follows:

- 0- Control does not exist
- 1- Control exists, but is poorly designed
- 2- Control exists and is reasonably designed
- 3- Control exists and is well designed
- 4- Control exists and is perfectly designed

operating effectiveness_s ... Operating effectiveness of a control as per assessment criterion *m*, measured as a percentage of control enforcement

For criteria in total (VR_{CAS})

$$VR_{CAS} = \sum VR_{CAS_m} \times \text{importance}_{CAS_m} \quad \text{where } m = 1, 2, \dots, n$$

$$VR_{CAS} = VR_{CAS_1} \times \text{importance}_{CAS_1} + VR_{CAS_2} \times \text{importance}_{CAS_2} + \dots + VR_{CAS_n} \times \text{importance}_{CAS_n}$$

VR_{CAS} ... Vulnerability rating for the entirety of assessment criteria

VR_{CAS_m} ... Vulnerability rating for assessment criterion *m*

importance_{CAS_m} ... Weight of assessment criterion *m*

Importance is assigned by the WG on a scale from 1.0 to 3.0. The WG determines the weight based on the significance of the assessment criteria for the overall AML/CFT risk management process. The following considerations support this decision:

- Whether the assessment criteria relates to all obliged entities or individual sectors;
- Whether systemic issues are identified in regards to the assessment criterion; and
- Whether serious inefficiencies are observed in the assessment area that led to country-wide AML/CFT related weaknesses.

3.3 Stage Three: Evaluation & Reassessment

The FATF Recommendations require that, when applying the RBA, countries and competent authorities decide on the most appropriate and effective way to mitigate the ML and TF risks identified. The evaluation stage encompasses this decision making process of finding the most appropriate risk management strategy.

3.3.1 Risk Management Strategies

Risk management strategies is an essential part of the risk assessment process. The appropriate risk management strategy is selected in accordance with priorities so that the greatest risks receive the most attention. An important consideration when determining the appropriate risk management strategy is the country's risk appetite – the level of ML/TF risk the country is willing to accept.

In order to manage ML/TF risks effectively, the nature, extent and timing of the risk management strategy must be commensurate to the level of the ML/TF risk. For example, higher levels of risk may require more immediate action to mitigate it or may indicate systemic risks which require an extensive response over time. With a high level of risk, appropriate mitigation responses generally require policy development and the implementation of enhanced measures. Lower levels of risk may require a lesser action, such as monitoring, or acceptance of the risk, if within the country's risk appetite.

It is the NRA Steering Committee's responsibility to propose a risk management strategy for each ML/TF risk and draft a risk response action plan. When determining the nature, extent and timing of the risk management strategies, the NRA Steering Committee may consult with key stakeholders, such as government ministers, supervisory authorities and sector representatives.

Typical risk management strategies include avoidance, mitigation and acceptance. In the context of ML/TF risk, the most relevant of these strategies are avoidance and mitigation.

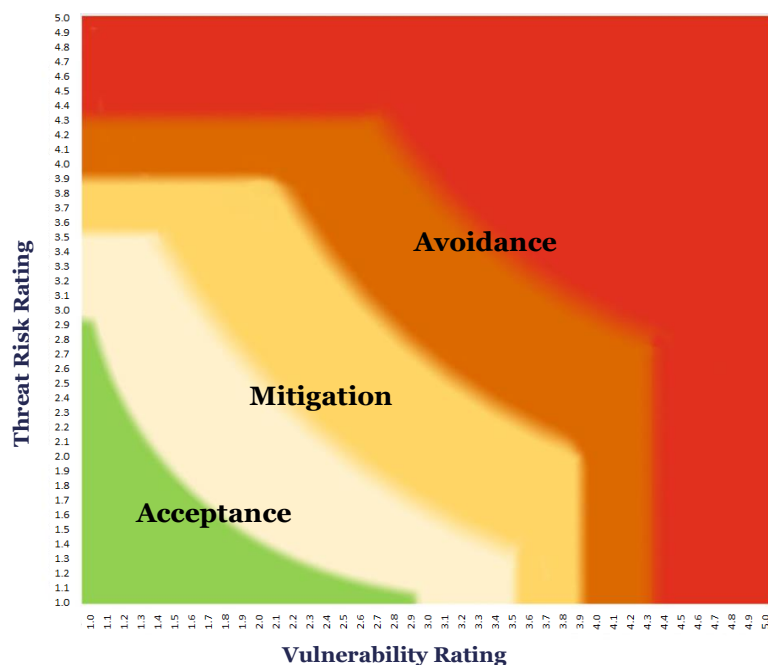
Acceptance – Risk acceptance does not reduce any effects; however, it is still considered a strategy. The risk and its consequences are accepted and no specific action is deemed necessary. This is a good strategy for ML/TF risks that will not have much of an impact to the country. Further, this strategy is a common option when the cost of other risk management strategies outweighs the cost of the risk itself. Contingency plans should be drafted to address consequences of the ML/TF risk occurring.

Avoidance – Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk by eliminating the cause of the risk. Actions should be undertaken to halt and exit activities that create such risk. This is a good strategy for when the ML/TF risk has a potentially large impact to the country.

Mitigation – Risk mitigation is probably the most commonly used risk management strategy. It is the action that limits the country's exposure by taking some action. The likelihood or impact of the risk is reduced by implementing mitigating controls.

Risk management strategies are graphically represented in a heat map in Graphic 7 below.

Graphic 7. Graphical representation of risk management strategies



In order to effectively manage the country’s risk response, the NRA Steering Committee catalogues the selected risk management strategies in a well-structured, properly labelled and categorised risk response action plan. The action plan includes a structured listing of, *inter alia*, all ML/TF risks identified, the respective risk rating and the selected risk management strategy. It is the AML/CFT Committee’s responsibility to approve the action plan as well as organise and check the implementation of the action plan.

The AML/CFT Committee is also tasked with developing AML/CFT policies, making legislative amendment proposals to the ministers responsible for the field. Managing the ML/TF risks at the country-level may be demanding, but approaching it with a structured action plan will support the AML/CFT Committee’s efforts, decrease the administrative burden and assist in the challenge of allocating scarce resources to fund AML/CFT programmes.

3.3.2 Reassessment of ML/TF risks

Further rounds of the risk assessment are performed to reassess the evolving threat situation and new emerging threats. The AML/CFT Committee is responsible for updating the risk assessment every two years, or more frequently if appropriate (similar to the SNRA).

It is recommended that the first update of the NRA takes place two years after the issuing of the initial NRA report. This first update will be a lighter procedure, which entails gathering information (e.g. questionnaires and updating the ECRAT), focusing on the implementation of the WG's recommendations, and re-evaluating of the previously mitigated risks.

The WG will then assess the experience gained and, if need be, adapt its methodological approach. The second update would likely be a more comprehensive assessment. It will consist of re-assessing the relevance of the initial risk assessment outcomes by including new emerging risks.

Appendices are located in the separate file: “NRA Methodology Appendices”.

4. Appendices

Appendices are located in the separate file: “NRA Methodology Appendices”.

Appendix 1 – Glossary

Appendix 2 – Estonian Intelligence

Appendix 3 – Selected risks to the internal market covered by the SNRA

Appendix 4 – NRA Project Plan

Appendix 5 – ECRAT

Appendix 6 – Risk-based Sampling

Appendix 7 – NRA Questionnaires

Appendix 8 – Sector-Specific Controls

Appendix 9 – Sources for Sectoral Controls

Appendix 10 – Relevant Legislation

Appendix 11 – Overview of obliged entities, licensing bodies & supervisory authorities

Appendix 12 - Supervisory Authorities

Appendix 13 – Data Repository

Appendix 14 – ECRAT Guide Manual

Appendix 15 – Indicative structure of the NRA report