



Financial Intelligence Unit of
Latvia

**Guidelines for Assessment of Risks of Money
Laundering and Financing of Terrorism and
Proliferation**

RIGA

2019

CONTENT

1. Introduction.....	3
Necessity of ML/FT/FP risk assessment.....	3
Benefits of ML/FT/FP Risk Assessment.....	3
2. ML/FT/FP Risk Assessment Process	4
Methodology of ML/FT/FP Risk Assessment	5
Target Audience of ML/FT/FP Risk Assessment	6
Competent Institutions and Persons Involved in ML/FT/FP Risk Assessment	6
Stages of ML/FT/FP Risk Assessment	8
Levels of ML/FT/FP Risk Assessment	9
Outcome of ML/FT/FP Risk Assessment	10
3. Communication of ML/FT/FP Risk Assessment	11
Communication Objective	11
Risk Assessment Reports.....	11
Channels of communication	11
Target audience	12
Provision of Distribution, Communication and Feedback to Supervisory and Control Authorities and to Subjects of the AML/CFT Law	12
Provision of Policy Makers with Information Distribution, Communication and Feedback	13
Provision of Law Enforcement Authorities and the Prosecution Office of LV with Information Distribution, Communication and Feedback.....	13
Provision of Society with Information Distribution, Communication and Feedback	14
4 List of abbreviations	15

1. Introduction

Necessity of ML/FT/FP risk assessment

- 1.1. Establishment, introduction and maintenance of an effective AML/CFT/CFP system has always been a global challenge, while today when everything becomes more and more digital and dynamic, the task becomes even more sophisticated. Although there are continuous measures for elimination and prevention of ML/FT/FP risks, as well as their consequences are being eliminated, ML/FT/FP are still adversely affecting both the world's economic processes and overall economics.
- 1.2. One of the key processes that allows recognising and identifying risks on a timely manner, as well as assessing (if necessary) their consequences, is performance of national ML/FT/FP risk assessment. Considering the global nature of ML/FT/FP schemes, it is crucial that every country performs qualitatively national risk assessment on a regular basis. The leading Latvian authorities in the field of AML/CFT/CFP, being aware of significance of the above process, have undertaken to assess national ML/FT/FP risks of Latvia on a regular basis. Thus, it can be ensured that Latvia identifies its topical ML/FT/FP risks and performs measures to effectively eliminate and prevent the identified risks, including application of a risk-based approach, by providing a proactive ML/FT/FP risk monitoring and management model.¹
- 1.3. According to international principles, countries according to relevant laws and regulations must require that the subjects of the AML/CFT Law² know the ML/FT/FP risks of the relevant sector considering the risks in relation to their customers, countries or geographic zones, products, services, transactions or delivery channels. Such risk assessment must be documented, continuously updated and made available to relevant competent authorities.
- 1.4. Also, effectiveness indicators of the Financial Action Task Force (FATF), the leading international institution for formation of an AML/CFT/CFP policy³, show that countries must raise awareness of the ML/FT/FP risks and, if necessary, implement measures for prevention of ML/FT/FP. In identification and assessment of the ML/FT/FP risks, comprehensive and reliable data must be used, by involving therein all competent authorities and persons. The ML/FT/FP risk assessment is used as a basis for formation of the AML/CFT/CFP policy.
- 1.5. Directive of the European Parliament and of the Council⁴ stipulates that every Member State of the EU must perform relevant measures to identify, assess, understand and eliminate ML/FT/FP risks they may face. Each Member State should appoint an authority or establish a mechanism for organisation of a national action in relation to the risk assessment. The national risk assessment must be made on a regular basis by considering the conclusions included in the transnational risk assessment elaborated by the EC.
- 1.6. At the same time, the above Directive stipulates that every Member State of the EU uses the elaborated national risk assessment to improve its system for AML/CFT/CFP, including by identifying sectors or fields with a lower or higher level of ML/FT/FP risks, granting resources for prevention of ML/FT/FP as well as developing of corresponding provisions for the established ML/FT/FP risks. Among other issues the Directive also stipulates that the EU Member States should make results of their national risk assessment available to the subjects of the AML/CFT Law with an aim to help in performance of sectoral risk assessments as well as to make it available to the EC, European supervisory authorities and other Member States.

Benefits of ML/FT/FP Risk Assessment

- 1.7. The process of ML/FT/FP risk assessment provides benefits on both national and international level. The risk assessment process includes:

¹ Such approach also corresponds to methodology of Financial Action Task Force (FATF), the leading authority in formation of AML/CFT/CFP policy. Available at: Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems – p. 23–25. Available at: <http://www.fatf-qafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf>

² Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing. *Latvijas Vēstnesis*, 116 (3900), 30.07.2008; *Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs*, 16, 28.08.2008 – Section 3, Paragraph one. Available at: <https://likumi.lv/doc.php?id=178987>.

³ FATF Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems – p. 93-95. Available at: <http://www.fatf-qafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf>

⁴ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU – Article 7-8. Available at: <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32018L0843>

- 1.7.1. Assessment of efficiency of the current system for AML/CFT/CFP, definition of shortcomings and necessary improvements;
- 1.7.2. Identification of previously undefined danger, vulnerability factors, risks and their consequences;
- 1.7.3. Performance of a strategic analysis as well as development of typologies;
- 1.7.4. Comparison with ML/FT/FP risk assessments of other countries, resulting in possible identification of causal relations and tendencies at international level;
- 1.7.5. Promotion of close mutual cooperation among public authorities and other competent institutions in elimination of ML/FT/FP risks;
- 1.7.6. Establishment of risk-eliminating measures and activities, including definition of priority activities as well as a long-term and short-term strategy for improvement of the AML/CFT/CFP system;
- 1.7.7. Improvement of awareness of both public institutions, private sector and population of the ML/FT/FP risks and their consequences.

2. ML/FT/FP Risk Assessment Process

Components of the ML/FT/FP Risk Assessment Process

- 2.1. According to the FATF guidelines for assessing ML/FT/FP risks⁵, the ML/FT/FP **risks** are established by analysing potential threats and vulnerability as well as consequences⁶ of ML/FT/FP.
- 2.2. **Threat** is a person or a group of persons, organisation or activities with potential to cause harm, for instance, to a country, nation, economy, etc. In context of ML/FT/FP, threats include criminal persons, terrorist groups and their coordinators, their financial assets as well as past, present and future activities in relation to ML/FT/FP.
- 2.3. Threats serve as a significant basis in gaining understanding about the ML/FT/FP risks. To determine nature and volume of offences and to identify origin of the illegal assets, it is important to understand the environment in which offences are committed. Assessment of threats should include the predicate offences that generate illegal assets, their frequency, regularity and dynamics, volume of laundered money in the country, a scale, methods and tendencies of money laundering. Also, assessment of threats should include an analysis of cross-border assets flow from other jurisdictions. Special attention must be paid to the financial assets that could be planned to be directed towards terrorism financing, i.e., both for terrorist groups and their support.
- 2.4. **Vulnerability** includes the aspects that allow implementing the threats, drive their distribution or do not restrict their implementation. In context of ML/FT/FP, vulnerability is related to shortcomings of protection mechanisms against possibility of ML/FT/FP. Therefore, when analysing vulnerability, special attention should be paid to the factors that point on shortcomings in AML/CFT/CFP systems and ML/FT/FP control mechanisms.
- 2.5. Vulnerability should be assessed both at the national scale and scale of each sector or field. Vulnerability assessment should include an analysis of an overall level of understanding and knowledge, defects and shortcomings in related laws and provisions and institutional system, economic, geographical and social factors, knowledge and understanding level of the subjects

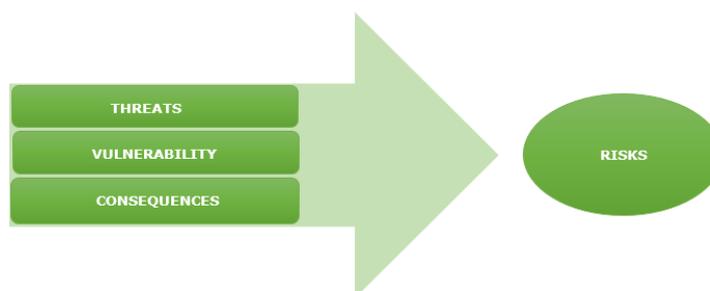
⁵ FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment. – p.7. Available at: https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

⁶ Assessment of consequences depends on applicable methodology. For instance, the methodology developed by the World Bank do not foresee assessment of the consequences. Available at: <https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support>

of the AML/CFT Law, efficiency of supervision and control mechanisms for AML/CFT/CFP and sufficiency of their resources.

- 2.6. **Consequences** reflect impact and harm caused by ML/FT/FP to the national financial system, economics and society in general. The consequences of ML/FT/FP may have long-term or short-term nature and apply to a certain population group, business field, national or international interests as well as on image of the financial sector. In context of assessment of consequences, also ratios of national economic growth, investment volume in the country, and Corruption Perceptions Index may be considered.
- 2.7. At the same time, according to the selected methodology, consequences may be excluded from risk determination, while the assessment is focused on single understanding of threats and vulnerability (see Image 1). For instance, the risk assessment model offered by the World Bank, defines the ML risk as a combination of threats and vulnerability.⁷

Image 1. Interaction of threats, vulnerability and consequences⁸



Methodology of ML/FT/FP Risk Assessment

- 2.8. The process of ML/FT/FP risk assessment is based on the methodology agreed on by the involved persons and authorities. The risk assessment process can include use of the methodology elaborated by the International Monetary Fund, World Bank a.o. authorities or the methods developed independently at the national level. For assessment of risks of different levels, different approaches or methodologies can be used. There is no single universal methodology for the risk assessment.
- 2.9. All competent institutions and involved persons must initially agree on an objective and framework of the risk assessment as well as on the expected result. Risk assessment can be aimed at provision of support and justification for performance of particular activities or decisions. The methodology for risk assessment can be specified based on the objectives and framework of the risk assessment.
- 2.10. When selecting an approach for the risk assessment, it must be understood that in context of ML assessment, streaming of illegally acquired assets into the legal financial system is assessed, while for financing of terrorism and proliferation, financial assets from both illegal and legal activities with an aim to support illegal activities in future are assessed.
- 2.11. Although the key objective of ML/FT/FP risk assessment is to identify and understand the ML/FT/FP risk, assessment can be performed at various levels, i.e., at national or transnational level, with a different objective and certain fields of operation, for instance, on a certain field, sector, business path, region, service, product, etc.
- 2.12. The national ML/FT/FP assessment includes assessment of ML/FT/FP risk of various levels, defining the overall view of the country about the ML/FT/FP threats, vulnerability and risks.

⁷ Risk Assessment Support for Money Laundering/Terrorist Financing. Available at:

<https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support>

⁸ Assessment of the consequences depends on applicable methodology. For instance, the methodology developed by the World Bank do not foresee assessment of the consequences. Available at: <https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support>

- 2.13. Regardless the methodology used, it must be ensured that ML/FT/FP risk assessment is comprehensive and provides a reasoned overview of the ML/FT/FP risk at the country, and it also must be ensured that the threats, vulnerability, their consequences and respectively also the risks are evaluated in a quality manner which is extensive enough.
- 2.14. ML/FT/FP risk assessment has to be performed on a regular basis, i.e. at least every three years. If it is necessary, ML/FT/FP risk assessment can be performed more often, e.g. to assess on a regular basis ML/FT/FP risks in concrete sectors, risks of new products delivery's and services providing's channels, etc.
- 2.15. ML/FT/FP risk assessment should also include identification of the aspects that encumbered acquisition, collection and analysis of quantitative and qualitative information or encumbered establishment of conclusions so that necessary improvements could be implemented in the identified fields in near future.
- 2.16. If assertive qualitative or quantitative data for reasoning definition of a lower risk level are lacking, a higher risk level must always be set. By fixing inaccuracies caused by lacking information, the risk level in the next assessment period can be determined according to the identified situation.

Target Audience of ML/FT/FP Risk Assessment

- 2.17. Nature, content and form of ML/FT/FP risk assessment should correspond to needs of its target audience. The potential target audiences may be:
- 2.17.1. Policy makers and public institutions involving or participating in formation of the AML/CFT/CFP system;
- 2.17.2. Law enforcement authorities and the Prosecution Office of the Republic of Latvia;
- 2.17.3. Financial Intelligence Unit of Latvia;
- 2.17.4. Supervisory and control authorities⁹;
- 2.17.5. Subjects of the AML/CFT Law;
- 2.17.6. non-governmental organizations and persons carrying out donations, gifts, etc.;
- 2.17.6. Observers of the national AML/CFT/CFP system and other international organisations;
- 2.17.7. Society including the interested persons from academic environment.

Competent Institutions and Persons Involved in ML/FT/FP Risk Assessment

- 2.18. The FIU is the leading authority in the field of AML/CFT/CFP in Latvia aiming at elimination of possibilities of using the financial system of the Republic of Latvia for ML/FT/FP¹⁰. The FIU organises and coordinates performance of ML/FT/FP risk assessment¹¹ by involving institutions of shared responsibility, takes a final decision on the most appropriate methodology for risk assessment and establishes the risk assessment objectives, framework and results to be reached.
- 2.19. The FIU, in cooperation with other competent institutions and persons, develops a plan for ML/FT/FP risk assessment by determining the process, results to be reached and a detailed schedule as well as tasks and duties of the responsible institutions and persons and of those of shared responsibility.
- 2.20. Contribution of each involved institution and person in ML/FT/FP risk assessment is significant, and each institution can greatly affect correct identification and adequate assessment of the ML/FT/FP risks. The process of risk assessment should include the following participants:

⁹ Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing. – Section 45.

¹⁰ Ibid – Section 50, Paragraph two.

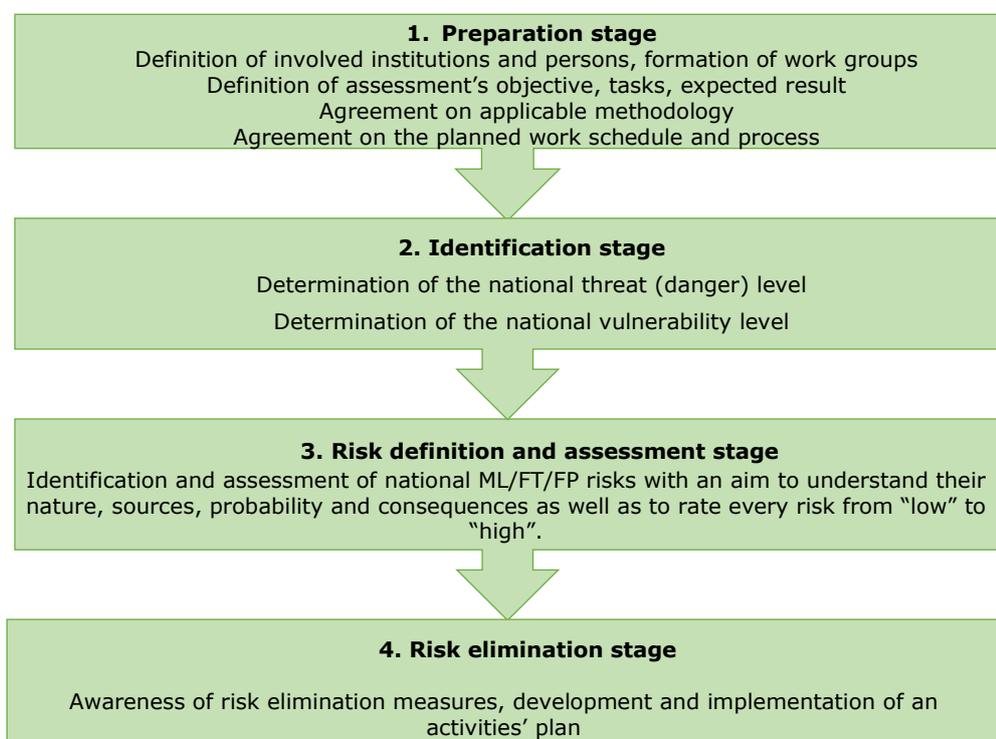
¹¹ Ibid – Section 51, Paragraph one, Clause 14.

- 2.20.1. **National policy makers** should be involved both as providers of quantitative and qualitative information and as expert opinion's providers and as users of risk assessment. The policy makers ensure that the identified risks are understood, appropriate activities are implemented and relevant decisions are taken for the risk elimination and prevention (MF, MJ, MI, MFA, ME, a.o., if necessary);
- 2.20.2. **Law enforcement authorities and the Prosecution Office of the Republic of Latvia** may provide information on particular offences and other data for elaboration of risk assessment. In addition, SSS may provide important information related to activities of foreign terrorist groups and their impact on national safety, established cases of FT and FP as well as information about ML/FT/FP threats (the Prosecution Office, KNAB, SAB, SSS, SRS, ST, SBG);
- 2.20.3. **FIU** may provide typologies, strategic studies based on reports about suspicious and unusual transactions as well as other significant information that is available at FIU's data bases, at the same time providing professional opinion as the leading authority in the field of AML/CFT/CFP in Latvia;
- 2.20.4. **Supervisory and control authorities** may provide significant opinion about the threats, vulnerability, typologies, tendencies and risks of ML/FT/FP in the sectors supervised and controlled by them, as well as they can specifically turn to subjects of the AML/CFT Law to clarify particular issues, knowledge or opinion (FCMC, SRS, Bank of Latvia, CRPC, LCSN, LCSA, LACA, LGSI, SIHP);
- 2.20.5. **Other authorities** may help in collection and analysis of qualitative and quantitative data, as well as with field expert consultations. These could be: Central Statistical Bureau, Companies Register, Ombudsman, Insolvency Control Service, The Council of Latvian Sworn Bailiffs, Central Finance and Contracting Agency, Rural Support Service, Latvian Environmental Investment Fund, a.o.;
- 2.20.6. **Private sector** may provide significant qualitative and quantitative information for risk assessment, and field experts may provide consultations for quality performance of ML/FT/FP risk assessment, as well as participate in the risk assessment process, thus ensuring that private sector representatives completely understand justification of risk identification and risk level definition and that they can distribute correct information to other actors of the private sector, including the subjects of the AML/CFT Law. The private sector representatives may include: Finance Latvia Association, Latvian Chamber of Commerce and Industry, Latvian Insurers Association, Employers' Confederation of Latvia, Association of the Certified Administrators of Insolvency Proceedings of Latvia, The Association of Accountants of the Republic of Latvia, Latvian Tax Consultant Association, Latvian Real Estate Association LANĪDA, Society of Real Estate Specialists NĪSA, Society of Latvian Real Estate Agents and Brokers NĪMA, Automotive Association, Association of Used Cars Traders, The State limited liability company "Assay Office of Latvia", a.o.
- 2.20.7. **International organisations** such as EC, FATF, Moneyval, OECD, the World Bank, International Monetary Fund or similar organisations on a regular basis perform assessment of Latvia and other countries and their conclusions and recommendations are particularly valuable to adequately determine the level of threats, vulnerability and risks comparing them with similar indicators used in other countries. Also, significant addition of information can be provided by foreign FIUs on situations in other regions in relation to the identified risks, risk tendencies, etc., as well as in relation to an operation of Latvian natural and legal persons outside Latvia.
- 2.20.8. **Representatives of academic field** may ensure significant contribution in formulation of quality information and expert opinion based on conducted researches, such as national research on shadow economics, volume of crime, etc.
- 2.21. To ensure the utmost correct and well-timed results, it is important also for the top government officials to demonstrate their political will and provide support for assessment of ML/FT/FP risks, as well as for the top management to understand the identified risks and act within their competence to facilitate the risk prevention and elimination.

Stages of ML/FT/FP Risk Assessment

2.22. ML/FT/FP risk assessment can be divided in four stages: preparation, identification of the current situations, risk definition and assessment, risk elimination (see Image 2).

Image 2. Scheme of ML/FT/FP Risk Assessment Process¹²



2.23. Before assessing the ML/FT/FP risks, a **preparation stage** should be implemented. Within this stage, objectives, tasks as well as the expected result of the risk assessment should be defined. It is important to determine authorities and persons involved in the risk assessment process as well as to form working groups, if necessary. It is also important to agree on the methodology to be used and the planned work process, including setting of a clear schedule, thus ensuring that the national risk assessment is completed within an acceptable term.

2.24. Within the **identification stage**, the national level of threats and vulnerabilities should be determined, and it should include detailed and well-defined, summarised and analysed quantitative, qualitative and expert-provided information. The assessment process includes making of conclusions about both the current and nearest possible threat and vulnerability aspects according to the pre-defined objective, work tasks and the expected result (depending on the selected methodology, also consequences can be assessed).

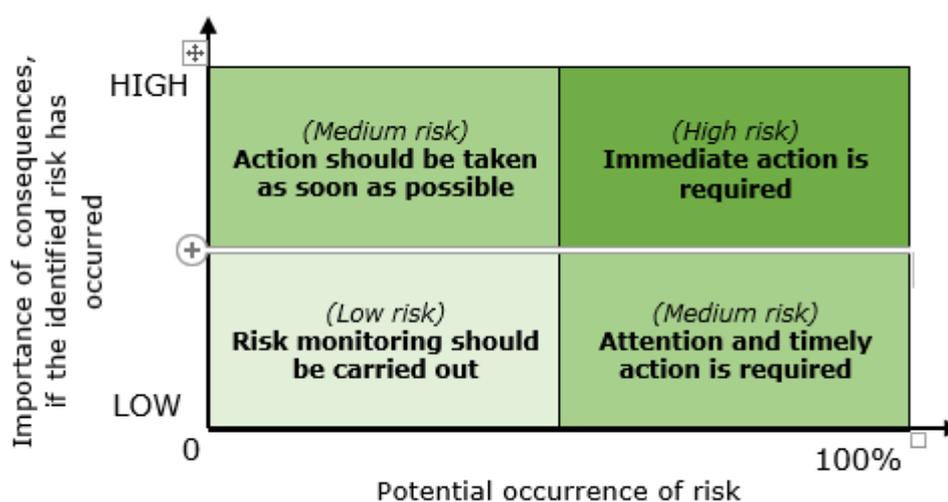
2.25. **Risk Definition and Assessment Stage** When defining the threat and vulnerability aspects, their mutual interaction should be examined, which results in defined ML/FT/FP risks (see also Image 1). The identified risks are causal relationship of threats, vulnerabilities and, depending on the applicable methodology, of consequences. By analysing the topical quantitative and qualitative data, it is possible to determine nature, origin, occurrence likeliness of the risks identified at the previous stage as well as to predict their consequences in future.

2.26. After identifying the risks at this stage, their specific level or assessment from "low" to "high" (or "very high", as it might be depending on the applicable methodology) is to be determined. The higher the assessment, the higher the probability to be subjected to ML, FT and FP. If assertive qualitative or quantitative data for reasoning definition of a lower risk level are lacking, a higher risk level must always be set.

¹²FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment – p. 22. Available at: https://www.fatf-gafi.org/media/fatf/content/images/National_ML_FT_Risk_Assessment.pdf

- 2.27. When assessing the risk level, one of the approaches uses the method of modelling different events, situations and cases that might be related to ML/FT/FP occurrence probability, e.g., an organised criminal group launders money by using legal companies; drug sellers are dealing with cash smuggling; foreign terrorist groups are using local NGOs for fund raising, etc.
- 2.28. It is difficult to set quantitative indicators of the ML/FT/FP risk level, thus, it should be noted that risks are a result of threat and vulnerability interaction and they reflect in risk consequences, and also risk occurrence probability should be considered.
- 2.29. The risk assessment stage concludes with a necessity to eliminate or even completely combat the identified risks. **At the risk elimination stage**, risk eliminating measures and activities are to be determined, priority activities and long-term and short-term strategy for their prevention are to be established. Risk assessment provides with an opportunity to sort the identified risks in a matrix, which points to the risks that must be prevented, as a priority. The higher the level of the identified risk, the more urgent measures must be set for their elimination (see Image 3).

Image 3. Simplified matrix for defining priority measures for ML/FT/FP risk prevention and elimination¹³



- 2.30. Higher level risks can indicate systematic activities and well-established schemes, thus, elimination or prevention of such risks will need more time and more complex measures than elimination or prevention of lower level risks.
- 2.31. Based on risk assessment result, a detailed action plan can be developed for implementation of a risk-based approach with an aim to prevent and eliminate the identified ML/FT/FP risks. The elaborated action plan includes also resource distribution among the institutions involved in its implementation.

Levels of ML/FT/FP Risk Assessment

- 2.32. Different risk assessment methodologies stipulate different methods for determining of a risk level. However, it is the most common approach to assess the level of ML/FT/FP threats, vulnerability and risks by using a five-point comparison system: "Low", "Medium low", "Medium", "Medium high" and "High". The higher the assessment, the higher the probability to be subjected to ML/FT/FP. Simplified assessment explanation might be as follows:
- 2.32.1. **"Low"** — danger with low occurrence probability. There are no data that criminals are going to use this sector, field, service, etc. for transactions directed to ML/FT/FP. To use this

¹³ Ibid. – p. 28.

ML/FT/FP type, complex planning, knowledge and/or the highest technical competence, compared to other options, are needed.

- 2.32.2. **“Medium low”** — danger with medium low occurrence probability. Criminals may have an opinion of using this sector, field, service, etc. for transactions referring to ML/FT/FP. To use this ML/FT/FP type, far-sighted planning and/or technical knowledge is needed when compared to other options.
- 2.32.3. **“Medium”** — danger with medium occurrence probability. This ML/FT/FP type can be available and/or its implementation is financially acceptable. The ML/FT/FP type is considered as being medium attractive and medium safe. Criminals have necessary capabilities to use this ML/FT/FP type, and average planning level and knowledge are needed. Threats in relation to use of this ML/FT/FP type must be taken into account.
- 2.32.4. **“Medium high”** — danger with medium high occurrence probability. This ML/FT/FP type is available and its implementation is financially acceptable. The ML/FT/FP type is considered as being rather attractive for criminals and safe. Criminals have capabilities to use this ML/FT/FP type, and average planning level and knowledge are needed. Threats in relation to use of this ML/FT/FP type are significant.
- 2.32.5. **“High”** — danger with high occurrence probability. The ML/FT/FP type is widely available and/or its utilisation costs are comparatively low. The ML/FT/FP type is considered as being attractive for criminals and/or safe. The ML/FT/FP type is rather easy to be implemented, does not require much planning, knowledge, when compared to other options. Threats in relation to use of this ML/FT/FP type are very significant.
- 2.33. If required, there may be an assessment between the two above assessments when significant differences of the assessed subjects’ activities are seen, e.g., “medium high/high” would mean that the overall risk level in the sector is high, while there are significant differences among the risk levels of subjects representing different sectors with certain representatives assessed as having medium or even low risk level.
- 2.34. In certain situations, there can be cases when risk assessment cannot be “Medium” or “Low”, if the threat or vulnerability level is permanently “High”. For instance,
 - 2.34.1. “High” threat level and “Low” vulnerability level — the state or a sector continuously is attractive to criminals for committing ML/FT/FP regardless of the implemented strict control mechanism. In such situations, criminals continue to establish more complicated technical methods of ML/FT/FP, while the state or the sector is not yet ready for that;
 - 2.34.2. “Low” threat level and “High” vulnerability level — even if the state or sector has not yet been misused for certain ML/FT/FP purposes (or such use has not been detected), lack of strict control would greatly increase interest of criminals or terrorists about using the state or sector for implementation of the certain ML/FT/FP objectives.

Outcome of ML/FT/FP Risk Assessment

- 2.35. The final report of ML/FT/PT risk assessment is a single document which includes comprehensive, detailed and reasoned information of a topical situation of the AML/CFT/CFP system, assessment of national threat and vulnerability level, assessment of ML, FT and FP threats and vulnerability of the subjects of the AML/CFT Law and the sectors represented by them as well as assessment of the identified risks of all above fields and their impact.
- 2.36. In case the report of ML/FT/FP risk assessment contains information of restricted availability or the report reveals possible ML/FT/FP schemes or scenarios, a public summary of the report of ML/FT/FP risk assessment is developed, and information of restricted availability is excluded.
- 2.37. The final report of ML/FT/FP risk assessment is supplemented with a detailed risk-based action plan by indicating strategic directions, objectives, required activities for the ML/FT/FP risk elimination, the expected outcome, responsible institutions, terms and volume of the required resources for implementation of the activities set in the action plan.
- 2.38. The final report of ML/FT/FP risk assessment is developed in cooperation with the competent institutions and persons. Final decision on the conclusions described in the report and decisions within the process as for the identified risks and their level are taken by the FIU as the leading

authority in the field of AML/CFT/CFP, and one of its aims is to eliminate possibilities of using the financial system of LV for ML/FT/FP.

- 2.39. The final report of ML/FT/FP risk assessment has to be agreed with all the competent institutions. After reconciliation, the final report of ML/FT/FP risk assessment is approved by the FIU Head and it is published on FIU website.
- 2.40. The final report of ML/FT/FP risk assessment can be presented at a FSDC meeting, meeting of Consultation Board of the FIU and meeting of the Cooperation and Coordination Platform of Supervisory and Control Authorities, meeting of the Council of Implementation of Cooperation Memorandum of the Cabinet of Ministers and Non-Governmental Organizations, meeting of Law Enforcement Management Working Group and Interinstitutional Expert Group, etc.

3. Communication of ML/FT/FP Risk Assessment

Communication Objective

- 3.1. To educate cooperation partners/target audience (according to the Point 2.17) with an aim of receiving support for prevention and combating of economic offences and significantly strengthen collaboration between various public institutions, raising awareness and understanding on the topical ML/FT/FP risks that are characteristic of the country or sector;
- 3.2. To improve efficiency of distribution and communication of information, risk level assessment and research;
- 3.3. To receive feedback about identified risks from the subjects of the AML/CFT Law;
- 3.4. To motivate subjects of the AML/CFT Law to review the ML/FT/FP risks to their activity and their clients as well as to improve internal control systems in accordance with the ML/FT/FP risks defined at national level;
- 3.5. To plan further actions necessary for the implementation of the policy;
- 3.6. To make the work of law enforcement institutions with the prevention of and fight against related offences more effective.

Risk Assessment Reports

- 3.7. ML/FT/FP risk assessment report at European level;
- 3.8. National ML/FT/FP risk assessment report of Latvia;
- 3.9. Sectoral ML/FT/FP risk assessments;
- 3.10. Current developments and tendencies in the field of ML/TF/PF obtained in result of an in-depth strategic analysis. Studies and reports related to prevention and identification of ML/FT/FP.

Channels of communication

- 3.11. The topical risk assessment reports are published on the FIU website, www.fid.gov.lv under "Useful — National risk assessment";
- 3.12. Direct communication: e-mails, meetings, participation in discussions;
- 3.13. Events: organisation of seminars and trainings, participation in conferences, etc;
- 3.14. Social media: LinkedIn account of the FIU.

Target audience

- 3.15. Supervisory and control authorities;
- 3.16. Subjects of the AML/CFT Law;
- 3.17. Non-governmental organizations and persons carrying out donations and gifts, etc.;
- 3.18. Policy makers, ministries responsible for the industries (MJ, MF, MI, MFA);
- 3.19. Law enforcement authorities and the Prosecution Office of the Republic of Latvia;
- 3.20. Society in general.

Provision of Distribution, Communication and Feedback to Supervisory and Control Authorities and to Subjects of the AML/CFT Law

- 3.21. Within the "Cooperation and Coordination Platform of Supervisory and Control Authorities", the drawn-up risk assessment is presented to supervisory and control authorities.
- 3.22. Supervisory and control authorities send publicly available risk assessments to the subjects of the AML/CFT Law, adding if necessary additional explanatory materials for each sector (if necessary) as well as further tasks to be carried out by the subjects of the AML/CFT Law.
- 3.23. Supervisory and control authorities evaluate the possibility to present and explain conclusions of risk assessments to subjects of the AML/CFT Law, their groups or associations in face-to-face meetings, seminars, trainings.
- 3.24. The subjects of the AML/CFT Law improve assessment of the ML/FT/FP risks referring to their type of activity and their clients and improve internal control systems as well as the respective procedures, IT systems and provide employee trainings. The aim of the subjects of the AML/CFT Law is to ensure that internal control systems work in accordance with a risk-based approach, providing for adequate resources and funds for such risk reduction measures where the highest risk has been defined.
- 3.25. Supervisory and control authority ensures that it receives feedback from subjects of the AML/CFT Law, subject groups, associations, other forms of subject representation, i.e. information about how subjects have taken into account the information laid down in risk assessment and what actions have been carried out in order to integrate it into every-day work and to accordingly improve internal control systems. Feedback may include opinions and suggestions of the subjects of the AML/CFT Law about necessary amendments in laws and regulations as well as other measures for elimination of the identified risks.
- 3.26. Based on received feedback, supervisory and control authorities may:
 - 3.26.1. Improve the mechanism for risk-based supervision and control measures;
 - 3.26.2. Create risk profiles for the subjects of the AML/CFT Law;
 - 3.26.3. Assess subjects' understanding of AML/CFT/CFP issues;
 - 3.26.4. Carry out training for subjects of the AML/CFT Law, targeting the improvement of understanding and the level of knowledge;
 - 3.26.5. Plan the methodology, regularity and scope of the targeted tests.
- 3.27. Supervisory and control authorities provide information about the feedback received from the subjects of the AML/CFT Law to the FIU — an overview of the action carried out by the subjects of the AML/CFT Law, identified factors that facilitate new risks, proposed measures for reduction of identified risks, etc.
- 3.28. The FIU may subsequently encourage responsible institutions to develop draft laws and regulations for remedy of the found deficiencies.

Provision of distribution, communication and feedback to non-governmental organizations and persons carrying out donations and gifts, etc.

- 3.29. Within the "Council of Implementation of Cooperation Memorandum of the Cabinet of Ministers and Non-Governmental Organizations", the drawn-up risk assessment is presented to representatives of non-governmental organizations.
- 3.30. Publicly available risk assessments are distributed to the major non-governmental organisations or associations thereof which raise funds for various charitable purposes by the FIU. Additional explanatory materials are added if required as well as the action expected from the non-governmental organization.
- 3.31. The FIU in cooperation with other competent authorities, shall evaluate the possibility of presenting and explaining the findings of risk assessments to non-governmental organizations, their groups or associations in face-to-face meetings, seminars or training sessions.
- 3.32. Non-governmental organizations supplement their websites with information that raises awareness of persons carrying out donations or gifts and any other good deeds of the potential threat to be exposed to ML/TF/PF.
- 3.33. Competent authorities, incl. FIU, SRS, SSS, organize informational and educational campaigns aimed at raising the awareness of non-governmental organizations and persons that carry out or are likely to carry out donations, gifts, etc., in order to focus their attention to the risk of being exposed to ML, as well as to inform non-governmental organizations about the measures to mitigate risks of being misused for TF purposes.
- 3.34. The FIU ensures that feedback is received from non-governmental organizations, their groups or associations or other forms of representation, that is, information on how the risk assessment has been taken into account by the non-governmental organizations and what steps have been taken to integrate the findings of the risk assessments into daily work of non-governmental organizations. Feedback may also include the viewpoints and suggestions of non-governmental organizations on necessary regulatory changes as well as other measures to reduce identified risks.
- 3.35. Sequentially, the FIU may propose the necessity to develop draft laws and regulations to remedy identified deficiencies to the competent authorities.

Provision of Policy Makers with Information Distribution, Communication and Feedback

- 3.36. The drawn-up risk assessment can be presented in an FSDC meeting. The FIU informs all institutions of FSDC about drawn up documents and conclusions in them.
- 3.37. Based on risk assessment, the responsible ministries:
 - 3.37.1. Decides on necessity to specify, improve and approve an action plan for elimination of ML/FT/FP risks;
 - 3.37.2. Ensures implementation of the action plan in case it is approved;
 - 3.37.3. Develops draft laws and regulations or their amendments to prevent the established deficiencies with an aim to reduce possibilities of performing ML/FT/FP in the Republic of Latvia.

Provision of Law Enforcement Authorities and the Prosecution Office of the Republic of Latvia with Information Distribution, Communication and Feedback

- 3.38. The drawn-up risk assessment can be presented in a meeting of the FIU's Consultation Board, meeting of Law Enforcement Management Working Groups as well as meeting of Interinstitutional Expert Group (CoM 24.01.2017. instruction No 1). The FIU informs all law

enforcement authorities and the Prosecution Office of LV in a written form about the drawn-up documents and conclusions made in them.

- 3.39. The law enforcement authorities and the Prosecution Office of LV assess the current and potential effect of offences, i.e. threat level, tendencies, dynamics and structure, on the national economic interests and public safety, based on risk assessment.
- 3.40. The law enforcement authorities and the Prosecution Office of LV take the conclusions into account when reviewing their priorities and decide on necessity to optimise their activities in the field of preventing and combating ML/FT/FP.
- 3.41. The law enforcement authorities and the Prosecution Office of LV form common understanding and knowledge of employees about the identified ML/FT/FP threats, vulnerability level, as well as about the risk danger and adverse effects. They plan an action for elimination and prevention thereof.

Provision of Society with Information Distribution, Communication and Feedback

- 3.42. The FIU publishes ML/FT/FP risk assessment reports on its website, www.fid.gov.lv, under "Useful — National Risk Assessment".
- 3.43. The FIU decides on necessity to prepare and provide an informative statement to media or a press release, as well as to continue collaboration with various media for purpose of information explanation with an aim to raise society's awareness of the level of threats, vulnerabilities and consequences regarding the probability of using the Latvian financial system for ML/FT/FP, as well as of the identified risks.

4. List of abbreviations

AML/CFT/CFP	Prevention of money laundering and terrorism and proliferation financing
MFA	Ministry of Foreign Affairs
EC	European Commission
ME	Ministry of Economics
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit of Latvia
FCMC	Financial and Capital Market Commission
MF	Ministry of Finance
FSDB	Financial Sector Development Board (Section 61 of the AML/CFT Law)
LGSI	Lotteries and Gambling Supervisory Inspection
MI	Ministry of Interior
KNAB	Corruption Prevention and Combating Bureau
LV	Republic of Latvia
LCSA	Latvian Council of Sworn Advocates
LCSN	Latvian Council of Sworn Notaries
LACA	Latvian Association of Certified Auditors
ML	Money laundering
ML/FT/FP	Money laundering, terrorism and proliferation financing
SIFP	The State Inspection for Heritage Protection
OECD	Organisation for Economic Co-operation and Development
FP	Financing of proliferation
CRPC	Consumer Rights Protection Centre
SAB	The Constitution Protection Bureau
FT	Financing of terrorism
MJ	Ministry of Justice
SSS	State Security Service
SRS	State Revenue Service
SP	The State Police
SBG	State Border Guard