METHODOLOGY
of National Risk Assessment on Money Laundering and Terrorist Financing in Ukraine

(Updated)

Organization for Security and Co-operation in Europe
Project Co-ordinator in Ukraine

METHODOLOGY
of National Risk Assessment on Money Laundering and Terrorist Financing in Ukraine

(Updated)

Kyiv – 2018

Organization for Security and
Co-operation in Europe
Project Co-ordinator in Ukraine

The publication is funded by the OSCE Project Co-ordinator in Ukraine. The publication reflects the authors' point of view and may not coincide with the official position of the OSCE Project Co-ordinator in Ukraine.

Content

ON THE METHODOLOGY

The Methodology of National Risk Assessment on Money Laundering and Financing of Terrorism in Ukraine has been developed in line with the International Standards and best practices of conducting national risk assessments in the leading countries of the world.

The Methodology is an updated version of the "Money Laundering and Financing of Terrorism in Ukraine Risk Assessment Methodology", which was developed in 2014. The previous Methodology was used for the first NRA in Ukraine, completed in 2016.

During 2017 - 2018, Ukraine was evaluated within the 5th round of mutual evaluations by the MONEYVAL Council of Europe Committee for technical compliance with the FATF Recommendations and efficiency of the national financial monitoring system. Further, in 2017, the findings of the first supranational ML/TF risk assessment at the EU level were made public.

The results of the 5th round of MONEYVAL evaluation of Ukraine and supranational risk assessment at the EU level, as well as the key FATF guidelines prompted the idea of updating the previous NRA Methodology in Ukraine and were the prime causes of the presented Methodology.

It is planned that in 2019 the Methodology will be used for a second national risk assessment in Ukraine and the basis for subsequent NRAs in Ukraine.

The draft Methodology was developed with involvement of local research experts and specialists of the State Financial Monitoring Service of Ukraine. Further, the draft Methodology was reviewed by a foreign specialist with unique expertise in the NRA area who provided useful recommendations.

The entire process of developing the Methodology (as well as its first edition) and the first NRA conducted in Ukraine were supported by the OSCE Project Co-ordinator in Ukraine.

The publication is funded by the OSCE Project Co-ordinator in Ukraine. The methodology reflects the point of view of its authors and may not coincide with the official position of the OSCE Project Co-ordinator in Ukraine.

INTRODUCTION

Financial monitoring has become the practice of many countries due to establishment of an AML/CFT system. Its fundamental methodological foundation is the RBA, with risk assessment as its basic element. Currently, the risk assessment methodology in the field of AML/CFT at the national level has been insufficiently investigated due to novelty of the problem and limited practical experience. Therefore, the relevance of studying and comprehending it as a set of certain principles, methods, sequence of actions, as well as institutional measures aimed at preventing and/or mitigating the effects of the risks identified, has been increasing.

In today's society, characterized by rapid development of information technologies and globalization of the economy/financial services, the AML/CFT situation has been getting ever more complex. Solving this problem requires global counter-measures based on cooperation between countries.

FATF strongly recommends cooperative countries to identify and analyze domestic AML/CFT risks, and assess them in line with the "40 Recommendations" that were reviewed for the fourth time in February 2012.

Given the above, the SFMSU, in conjunction with the OSCE Project Co-ordinator in Ukraine, implemented a technical assistance project "Capacity Building of the Financial Monitoring System of Ukraine", under which the first National ML/TF Risk Assessment Report (Report) was presented in December 2016[1].

Risk assessment is an important basis for risk management and building systemic guarantees of sustainability in the country. The NRA is an important step in defining a common vision of the risk base, as well as an understanding of which risks should be taken into account, mitigated, neutralized and/or transferred (transferred to a supranational level). The NRA contributes to development of recommendations and identification of priorities for strengthening sustainability of certain types of economic activity, sectors, enterprises, institutions, and organizations.

The NRA in the AML/CFT area should be comprehensive and requires a sound management structure with agreed timelines and evaluation rules to ensure consistent, effective and reliable outcomes. It should also be understandable to all the participants and consistent with the context of the country concerned, take into account a combination of quantitative and qualitative criteria for assessing latent phenomena and processes in the AML/CFT area. Efficient risk assessment should stimulate development of all the participants in the national AML/CFT system, focus their efforts on identifying the most common threats and vulnerabilities and on neutralizing the risks identified – first of all, those with a high occurrence likelihood and significant negative impact on the state of affairs in the AML/CFT area.

At the same time, it is necessary to distinguish between the possibility of unpredictable significant events that are risk generators in the AML/CFT area (technological innovations on the financial services markets may become prerequisites for such events) and a large number of less resonant threats and vulnerabilities, which, however, generate more regular

1 National Risk Assessment Report on Preventing and Countering Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism [Electronic resource]. – Kyiv, 2016. – 208 p. – P. 42. – Access mode: http://www.sdfm.gov.ua/content/file/Site_docs/2016/20161125/zvit_ukr.pdf

risk events. To this end, the NRA results should be actively discussed with the main stakeholders in policy and programmatic decision-making in the AML/CFT area – SFME, law enforcement and intelligence agencies, as well as with RE.

Ensuring transparency and legality of financial transactions is one of the most important tasks of the state. ML and TF worldwide are grave crimes that impede a country's social, economic, political and cultural development, impair national and international stability, and undermine the integrity of financial markets and institutions. The above threats are closely linked with a decrease in the state budget tax revenues, adversely affect the exchange rate dynamics and interest rates, and significantly damage a country's reputation.

SECTION I.
BACKGROUND

1.1. NRA Prerequisites, Coverage, Goal and Objectives

In accordance with FATF Recommendation 1, countries should identify and analyze the national ML/TF risks, as well as evaluate them using a a risk-based approach (RBA) to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified[2].

At the same time, FATF provides states with an opportunity to independently choose the NRA methodology, taking into account the specific features of a particular country, without imposing any general schemes.

Identification, assessment and understanding of the ML/T risks are important components for establishing and developing of an efficient national AML/CFT system. At the national level, this is achieved by developing policies in the relevant field and making well-grounded decisions aimed at achieving specific goals and objectives, while at the private sector level, similar goals are achieved through implementation of adequate client due diligence procedures and monitoring of the clients' financial transactions, as well as by carefully observing compliance of the operational activities pursued by REs and certain non-financial institutions and professions with the requirements of the effective AML/CFT legislation.

The regulatory and institutional frameworks are two main elements of the national AML/CFT system, therefore their compliance with the relevant international standards and best practices for implementation of these standards is an issue of prime concern for Ukraine. This is evidenced by the Fifth Round Mutual Evaluation Report on Ukraine, published on 30.01.2018 by the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)[3]. In general, the Report showed Ukraine's progress in developing the national financial monitoring system and confirmed the growing operation efficiency dynamics of all its participants. Nevertheless, the conclusions of the last and previous mutual assessments of over fifteen years of the national AML/CFT system operation have revealed a significant number of weaknesses and gaps, neutralizing of which should be the focus of all the system participants.

In order to provide a sustainable and progressive AML/CFT system, Ukraine has taken important steps towards implementation and enforcement of international standards for combating ML/TF, including identifying, analyzing and evaluating national AML/CFT risks. In this context, in September 2014, the SFMSU developed the first revision of the NRA methodology, and during 2014-2016, 11 international events were organized, resulting in the said presentation of the first NRA Report in December 2016.

Development of the first NRA Report was preceded by establishing in April 2015 of an interagency working group comprising representatives of the SFMSU, Ministry of Finance of Ukraine, NBU, National Securities and Stock Market Commission, and scholarly experts.

The results of the first NRA, *inter alia*, evidenced that the practice of further (law enforcement and judicial) testing of signals about financial transactions suspicious in terms of ML/TF, detected at the level of the RE, required serious improvement, as

2 The FATF Recommendations [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

3 Ukraine's measures to combat money laundering and the financing of terrorism and proliferation: fifth round mutual evaluation report. December 2017. [Electronic resource]. – Access mode: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-ukraine-2017.html

the corresponding relations between the indicators of primary detection and further incrimination of the detected were very weak.

This methodology has been developed in line with the FATF Guidance on National ML and TF Risk Assessment, according to which the ML/TF risks should be assessed as a function of the threat, vulnerability, and respective risk consequences.

The purpose of the NRA methodology development is to describe systemic approaches to assessment of the AML/CFT risks, which are based on a combination of objective quantitative statistics and subjective qualitative expert assessments, analysis of operational intelligence information of law enforcement authorities (interviews, questionnaires), the results of criminal proceedings consideration, actions that are taken by the private sector and SFME in the AML/CFT area, examples of international cooperation of the FIU and law enforcement authorities, as well as other open source information. The NRA methodology is intended to structure the analysis of the available information on the threats, vulnerabilities and possible consequences of the ML/TF-related risks to absorb the main results of international practical and methodological research and to take into account the domestic specific nature of the national AML/CFT risk assessment.

Collection, structuring and analysis of data is proposed to be performed in specially designed spreadsheets (typical matrix templates) intended to be a guide for collecting accurate data, which can then be used for the NRA, drafting of relevant reports, and solving other tasks. Population of typical indicator matrices with the actual data in dynamics will allow a clearer understanding of how the national AML/CFT regime works, enable monitoring of the regime operation, and help increase the operating efficiency of the AML monitoring system.

The NRA ultimate objective is to detect (update) the national risks (threats, vulnerabilities, consequences) in the AML/CFT system and to identify the risk management elements and assistance in the development of AML/CFT development strategy system in Ukraine.

NRA aims to:

- assist in development of a proactive strategy and tactics of deterring criminals by timely detection, arrest, and confiscation of criminal proceeds;
- prevent terrorist acts and terrorist activities by timely detection and efficient blocking of their funding sources;
- analyze the ML and TF consequences for the society, social relations, and financial and economic system to identify appropriate measures to prevent and counter the existing threats and vulnerabilities.

NRA should identify the ML and TF likelihood based on the existing threats (a person (group of people)), object or activity with the potential to cause harm to the state, society, economy, etc.) and AML/CFT system vulnerabilities (things that can be exploited by threats), namely through:

a) early identification of threats related to a possibility of ML/TF;

b) reliable evaluation of their occurrence possibility;

c) identification of the national AML/CFT system vulnerabilities to threats;

d) assessment of consequences and scale of threat occurrence based on the identified vulnerabilities of the national AML/CFT system;

e) timely elimination or correction of vulnerabilities;

f) prevention of negative consequences of the AML/CFT risks;

g) determining priorities of the national AML/CFT system;

h) making decisions on the most efficient use of resources.

In view of the above, **the description of threats and vulnerabilities, as well as the goals, addressing which requires efforts of the NRA participants** in the AML/CFT area in Ukraine in order to neutralize the adverse consequences of respective risks, **can be described in the following sequence**:

1. analysis of **external** and **internal threats and vulnerabilities** for the financial and economic and social and political area of Ukraine;
2. analysis of **intense** (large one-time and unpredictable) and **extensive** (less extensive but regular) AML/CFT **risks**;
3. identification and typology of the key **areas** (financial products, tools, and services) and **ways** to form illegal sources of capital and its further legalization in Ukraine (cash, fictitious entrepreneurship, using the benefits of certain organizational and legal business forms, tax evasion, beneficial ownership, nonprofit sector organizations, risks of different types of legal entities to be used for ML/TF purposes, risks of organized crime, etc.);
4. integration of information flows and systematization of statistical summaries (**comprehensive administrative reporting**) in the AML/CFT area for monitoring the contribution of the FIU, regulatory and supervisory, law-enforcement and intelligence agencies, and judicial system to the efficiency and effectiveness of the national AML/CFT system;
5. analysis of **sectoral** ML/TF **risks** and establishing efficient mechanisms of the risk-based monitoring of potential ML/TF sources based on SFME processing of the aggregated data in the context of their supervised sectors;
6. **harmonization of anti-money laundering and anti-corruption state policy** through development of an efficient risk-based system for detecting and timely blocking of funds received through corruption, monitoring of suspicious financial activities of clients, as well as those over-threshold financial transactions, whose final beneficiaries are national politically exposed persons and/or their associates or related persons.

Minimizing the above generic threats and vulnerabilities can become a solid basis for improving the effectiveness and efficiency of the AML/CFT system in Ukraine, as well as the key to development, implementation and further expansion of a holistic set of analytical and investigative measures that will facilitate transition from traditional countering and combating of the consequences (symptoms) of socially dangerous unlawful acts to a proactive prevention strategy and systemic neutralization of the factors (causes) of illegalization of the national economic system.

The need for NRA is provided for in the Law[4] and CMU and NBU Resolution "On Approving the Procedure for National Risk Assessment on Preventing and Countering Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism, and Publishing Its Results" of 16.09.2015, No. 717[5].

To verify compliance of countries with the above FATF Recommendations, a "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems"[6] was developed and adopted in February 2013.

The following provisions of the Methodology for Assessing the FATF Recommendations should be highlighted in the NRA context:

"Technical Compliance" Block

Risk assessment

1.1. Countries should identify and perform a country-specific NRA.

1.2. Countries should designate an authority or mechanism to co-ordinate NRA actions.

1.3. Countries should keep the NRA up-to-date.

1.4. Countries should have communication mechanisms on the NRA results with all the relevant competent authorities and self-regulatory bodies, financial institutions and designated nonfinancial businesses and professions.

Risk mitigation

1.5. Based on their understanding of their risks, countries should apply a risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF.

1.6. Countries which decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions should demonstrate that:

(a) there is a proven low risk of ML/TF; the exemption occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

(b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of ML/TF.

1.7. Where countries identify higher risks, they should ensure that their AML/CFT regime addresses such risks, including through: (a) requiring financial institutions and

4 On Preventing and Countering Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of Proliferation of Weapons of Mass Destruction: Law of Ukraine, 14 October 2014 No. 1702-VII: [Electronic resource]. – Access mode: http://zakon3.rada.gov.ua/laws/show/1702-18

5 On Approving the Procedure for National Risk Assessment on Preventing and Countering Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of Proliferation of Weapons of Mass Destruction: Cabinet of Ministers of Ukraine Resolution, 16 September 2015 No. 717: [Electronic resource]. – Access mode: http://www.kmu.gov.ua/control/uk/cardnpd?docid=248493531

6 Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems. [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

DNFBPs to take enhanced measures to manage and mitigate the risks; or (b) requiring financial institutions and DNFBPs to ensure that this information is incorporated into their own risk assessment system.

1.8. Countries may allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its ML/TF risks.

1.9. Supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations under Recommendation 1.

"Effectiveness" Block

Characteristics of an efficient system: A country properly identifies, assesses and understands its money laundering and terrorist financing risks, and co-ordinates domestically to put in place actions to mitigate these risks. This includes the involvement of competent authorities and other relevant authorities; using a wide range of reliable information sources; using the assessment(s) of risks as a basis for developing and prioritizing AML/CFT policies and activities; and communicating and implementing those policies and activities in a co-ordinated way across appropriate channels. The relevant competent authorities also cooperate and co-ordinate policies and activities to combat the financing of proliferation of weapons of mass destruction. Over time, this results in substantial mitigation of money laundering and terrorist financing risks.

Core Issues to be considered in determining if the outcome is achieved:

1.1. How well does the country understand its ML/TF risks?

1.2. How well are the identified ML/TF risks addressed by national AML/CFT policies and activities?

1.3. To what extent are the NRA results properly used to justify exemptions and support the application of enhanced measures for higher risk scenarios, or simplified measures for lower risk scenarios?

1.4. To what extent are the objectives and activities of the competent authorities (regulators) and SRBs consistent with the evolving national AML/CFT policies and with the ML/TF risks identified?

1.5. To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?

1.6. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF risks?

a) Examples of Information that could support the conclusions on the Core Issues:

1. The country's assessment(s) of its ML/TF risks (e.g., types of assessment(s)

produced; types of assessment(s) published / communicated).

2. AML/CFT policies and strategies (e.g., AML/CFT policies, strategies and statements communicated/published; engagement and commitment at the senior officials and political level).

3. Outreach activities to private sector and relevant authorities (e.g., briefings and guidance on relevant conclusions from risk assessment(s); frequency and relevancy of consultation on policies and legislation, input to develop risk assessment(s) and other policy products).

b) Examples of Specific Factors that could support the conclusions on the Core Issues:

4. What are the methods, tools, and information used to develop, review and evaluate the conclusions of the assessment(s) of risks? How comprehensive are the information and data used?

5. How useful are strategic financial intelligence, analysis, typologies, and guidance?

6. Which competent authorities and relevant stakeholders (including financial institutions and DNFBPs) are involved in the assessment(s) of risks? How do they provide inputs to the NRA, and at what stage?

7. Is the NRA(s) kept up-to-date, reviewed regularly and responsive to significant events or developments (including new threats and trends)?

8. To what extent is the NRA(s) reasonable and consistent with the ML/TF threats, vulnerabilities and specificities faced by the country? Where appropriate, does it take into account risks identified by other credible sources?

9. Do the policies of competent authorities respond to changing ML/TF risks?

10. What mechanism(s) or body is used to ensure proper and regular cooperation and co-ordination within the national system, to develop and implement the AML/CFT policy, at both policymaking and operational levels, and where relevant, to counter the financing of proliferation of weapons of mass destruction? Does the mechanism or body include all relevant authorities?

11. Are there adequate resources and expertise involved in conducting the NRA(s), and for domestic co-operation and co-ordination?

The national RBA means providing adequate resources to particular components of the AML/CFT system. For example, if, based on NRA, ML is most likely to occur in the banking sector, more resources (money, staff, and specialized IT solutions) should be focused in this sector to decrease the level of risk identified and neutralize the threats and vulnerabilities. And opposite, if the risk is low in the legal services sector, the country can decide to apply simplified measures to some extent.

Actually, based on the NRA results, Ukraine should be ready to demonstrate that the authorities properly acknowledge the risks, have planned and take actions to mitigate the risks. Countries should also assess if the measures implemented actually decrease the level of the risks identified. That is another key point in conducting NRA.

1.2. NRA Methodological Sources, Terminology and Principles

In developing this Methodology, the following publications of international organizations were taken into account:

- FATF Recommendations and Methodology for Assessing the FATF Recommendations
- FATF Guidance on the National Money Laundering and Terrorist Financing Risk Assessment[7];
- FATF Guidance on Money Laundering and Terrorist Financing Risk Assessment Strategies[8];
- FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures[9];
- FATF Guidance on AML/CFT-Related Data and Statistics[10];
- OSCE Handbook on Data Collection in support of Money Laundering and Terrorism Financing National Risk Assessments[11];
- World Bank advisory package (methodology and instructions) on the national ML/TF risk assessment tool and a systematic and organized NRA process, with the broad participation of public and private sector stakeholders[12];
- IMF Staff Discussion Note: "Corruption: Cost and Mitigating Strategies"[13];
- guidance note on inclusion of AML/CFT in a country's surveillance and financial sector assessment indicators[14];
- International Monetary Fund Staffs' ML/FT NRA Methodology[15];
- World Bank National Risk Assessment Methodology[16];
- EU supra-national ML/TF risk assessment methodology[17].

7 National money laundering and terrorist financing risk assessment [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

8 Money Laundering & Terrorist Financing Risk Assessment Strategies [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20Risk%20Assessment%20Strategies.pdf

9 FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures. [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf

10 Guidance on AML/CFT-related data and statistics. [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/reports/AML-CFT-related-data-and-statistics.pdf

11 OSCE Handbook on Data Collection in support of Money Laundering and Terrorism Financing National Risk Assessments [Electronic resource]. – Access mode: http://www.osce.org/secretariat/96398?download=true

12 Risk Assessment Support for Money Laundering/Terrorist Financing. [Electronic resource]. – Access mode: http://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support

13 IMF Staff Discussion Note: "Corruption: Cost and Mitigating Strategies". [Electronic resource]. – Access mode: www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf

14 IMF Guidance Note "Inclusion of AML/CFT in surveillance and Financial Sector Assessment Programs (FSAPs)". [Electronic resource]. – Access mode: http://www.imf.org/en/Publications/Policy-Papers/Issues/2016/12/31/Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-Inclusion-in-Surveillance-PP4726

15 The International Monetary Fund staffs' ML/FT NRA Methodology. [Electronic resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_IMF.pdf

16 The World Bank Risk Assessment Methodology [Electronic Resource]. – Access mode: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_World_Bank.pdf

17 European Commission Report on the Supra-National Risk Assessment (SNRA) of the risks of ML and TF.

Development of this Methodology also used elements of a research and practical summary of an approach based on risk assessment underlying Dionysios Demetis' work "Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach".[18] In the paper, based on the systems theory, the theoretical foundations of the study into the AML/CFT phenomenon are formulated, emphasizing that RBA is the most important modern tool of the AML/CFT system.

However, in the vast majority of modern research on RBA implementation in the legislative (regulatory) regulation practice, the essence and significance of this approach, as well as the practice of its application at the level of financial and credit institutions, are explored. At the same time, the methodological problems of AML/CFT risk assessment at the national level are virtually not highlighted.

As stated above, this Methodology is designed to structure the various AML/CFT NRA aspects at the national level in the context of approaches, principles, methods and technology of their implementation, taking into account the existing international standards, best practices, guidances and reports.

At present, it is common to treat risk as a loss hazard, a possibility of an adverse event and negative consequences of its occurrence. In other words, it is emphasized that the uncertainty factor is inherent in the risk.[19]

The most consequential trend of our time is that the information society has become an economic reality. Innovation in the communication and computing technology accelerates the rate of any changes due to bringing the speed of information transmission down to zero. New information technologies generate new types of economic activity, new financial products and services. When it comes to the information society, it is necessary to take into account the economy, in which the main resource (information) becomes inexhaustible, however access to it remains limited. At the same time it should be remembered that such type of economy has a flip side which can be called economy of misinformation – a variety of modern shadowing (illegalization) of the business processes, which breeds a novel type of opportunistic behavior that uses disinformation for masking and concealing the illegal content of its activities.

Limited access to information, information asymmetry, and high cost of the information product or service (cost of information) are the reason for a significant increase in the transaction costs in the economy, which consist of the cost of evaluating the object of exchange (legal transaction) and the cost of monitoring and ensuring fulfillment of the specified legal transaction terms. In turn, according to R. Coase's[20] theorem, significant transaction costs cause emergence of institutes (laws, regulations) and institutions (state authorities and institutions) whose task is to overcome asymmetry in the information awareness to the maximum possible degree, which leads to improvement of managerial decision-making models (Fig. 1.1):

[Electronic resource]. – Access mode: http://ec.europa.eu/newsroom/document.cfm?doc_id=45319

18 Dionysios S. Demetis. Technology and Anti-Money Laundering: A Systems Theory and Risk-Based. / D. D.Demetis. – Cheltenham,UK: Edward Elgar Publishing, 2010. – 188 p.

19 Hlushchenko O.O. Anti-Money Laundering Financial Monitoring: Risk-Based Approach: monograph / O.O. Hlushchenko, I.B. Semehen; under the general editorship of Dr. Econ. Sciences, Prof. R.A.Slaviuk. – K.: : UBS NBU, 2014. – 386 p.

20 Hodgson G. Economics and Institutions: A Manifesto for a Modern Institutional Economics / G. Hodgson; transl. from English – M.: Delo, 2003. – 464 p.

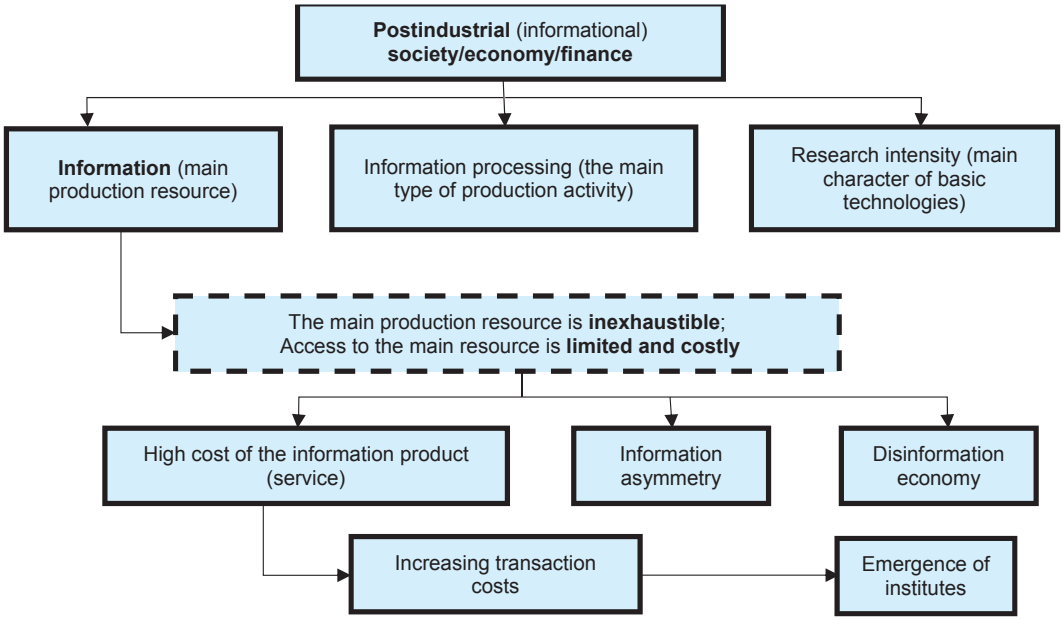


Fig. 1.1. The essence of information economy and finance

In Ukraine, as in many other countries, the main institute for curbing the disinformation economy is the financial monitoring institute. It accumulates the maximum amount of available information on suspicious financial and economic transactions at micro and macro levels.

The central "filter" of the national AML/CFT system responsible for collecting, processing, and summarizing information on suspicious (risky) financial transactions is the national FIU – the SFMSU (Figure 1.2):

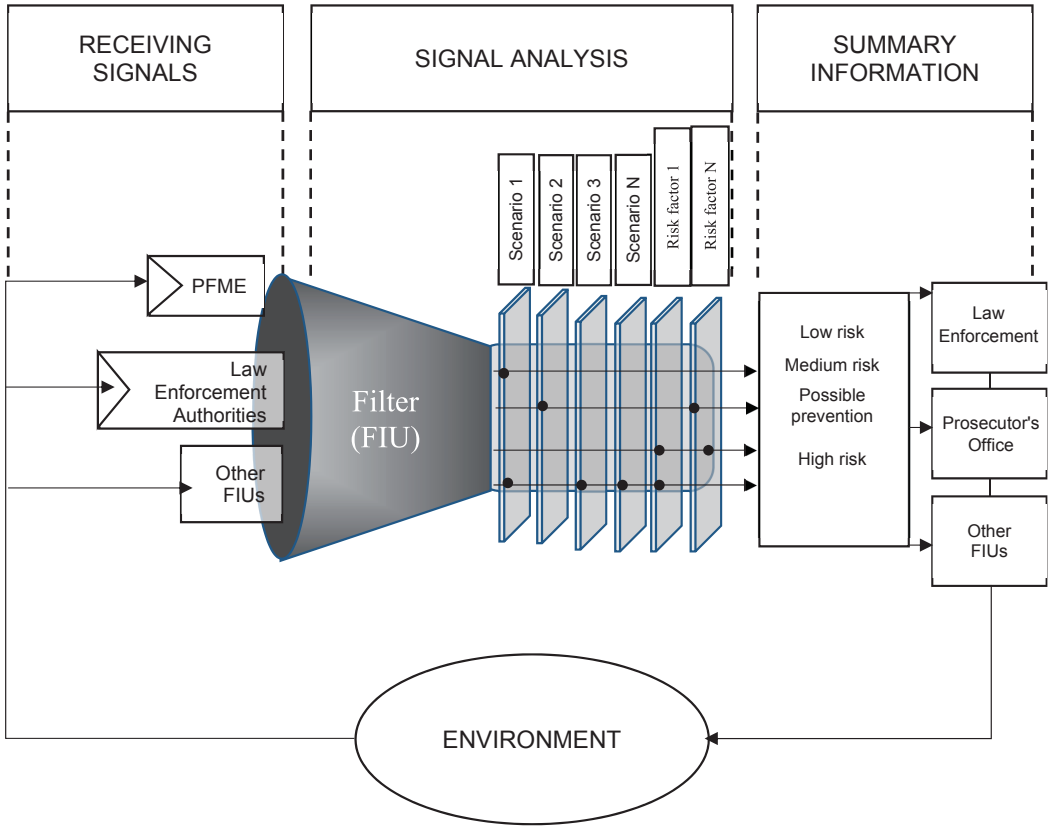


Fig. 1.2. Macro-level model of the risk-based financial monitoring institute

The main sources of primary information include the State's REs, law enforcement, intelligence authorities and foreign FIUs. The national AML/CFT system elements, which perceive the information processed and provided by the national FIU in the form of summary materials as an incentive to perform a specific action, are a total of law enforcement agencies, SFME, and foreign FIUs.

The micro-level model is fractal to the macro-level one, given that the function of the central filter in it is played by the RE (banking and non-bank financial institutions, as well as DNFBP), while RE clients and financial the clients' financial transactions are the sources of primary information (including generators of probable threats) (Fig. 1.3):

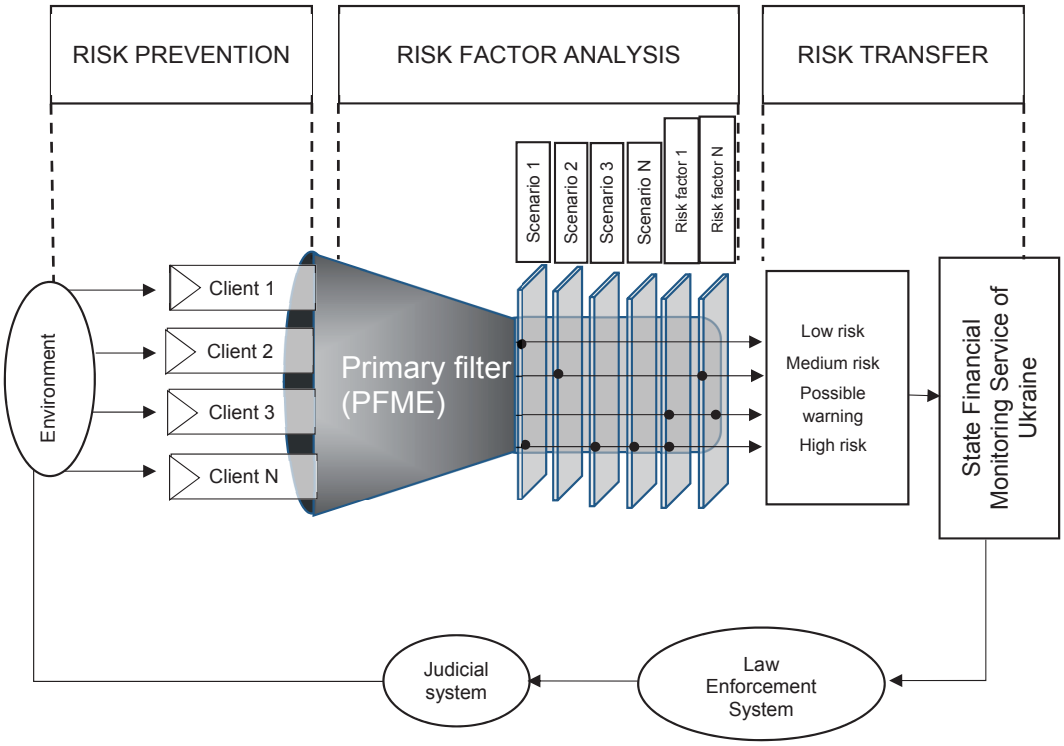


Fig. 1.3. Micro-level model of the risk-based financial monitoring institute

Thus, the purpose of the AML/CFT system in Ukraine is to overcome the situation of asymmetric awareness and other vulnerabilities which are threat and risk generators, as well as facilitators in using REs for ML/TF transactions.

Based on the above and taking into account the results of processing of the above methodological sources, the **NRA goals** can be specified through the following set of objectives:

- reduce the risk of ML/TF occurrence;
- assess the threat of ML/TF risk occurrence;
- assess the degree of vulnerability in relation to the existing ML/TF threats;
- correlate the threat of risk occurrence and its potential consequences with the amount of resources aimed at reducing the corresponding risk;
- minimize the consequences, where the ML/TF risk occurs.

The FATF Guidance on the application of the risk-based approach in the AML/CFT area and a number of other FATF documents view risk as a derivative of three factors: threat, vulnerability and consequence.

A **threat** is a person or group of people whose activities have the potential to cause harm to the state, society, the economy. In other words, terrorist groups and their facilitators, their funds, as well as past, present and future ML/TF activities.

Vulnerabilities are areas in which a threat may occur or factors that may facilitate threat occurrence. These may be structural components of the financial system, mechanisms, services or products used to transfer and store cash. When considering vulnerabilities, factors that generate risks in AML/CFT control and surveillance activities are taken into account, as well as the characteristics and peculiarities of a specific sector, financial product or service type attractive for ML/TF purposes.

Consequence refers to the impact or harm from criminal activities inflicted on the financial system and/or institutions, the economy in general, population, business environment, national and international interests, reputation and attractiveness of a country's financial sector to investors.

Risk assessment – judgment on threats, vulnerabilities and consequences based on a combination of quantitative (statistical) and qualitative (expert) methods.

National Risk Assessment is an organized systematic activity carried out by the state and reporting entities, as well as other authorized state authorities, aimed at identifying and studying the threats, vulnerabilities, risks, and consequences of their occurrence in the AML/CFT area. The NRA result is a Report on the nature and scale of the ML/FT in Ukraine.

The report, which is based on the NRA results, is a prerequisite for the competent authorities of the state in the context of developing and implementing an efficient **AML/CFT Action Plan**. The relevant Action Plan is a **strategic document**, since it provides for identification of the AML/CFT policy priorities and risk-based resource allocation priorities.

The risk assessment system provides information for law enforcement agencies, the financial intelligence unit, financial and credit institutions, provides an understanding of whether the current legislation meets the objectives of preventing new threats and whether the monitoring, enforcement and judicial protection methods are sufficient.

The FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures contains **five RBA principles**:

1. understanding the threats and vulnerabilities, national risk assessment;
2. a legal/regulatory framework that supports the application of a risk-based approach;
3. design of a supervisory framework to support the application of the risk-based approach in the RE environment;
4. efficient distribution of responsibilities between the entities of monitoring and ensuring interaction between them;
5. information exchange between the public and private sector in terms of assessments of the country risk, typologies or assessments of how ML/TF-related persons abuse the financial system.

The analysis of the FATF documents (first of all, National ML/TF Risk Assessment and ML Risk Assessment Strategies) allows identifying and formulating a number of NRA principles in the AML/CFT area, which explain and supplement the five RBA principles listed above.

The **NRA principles** are ranked as follows:

1. harmonization of NRA goals and scale;
2. NRA comprehensiveness;
3. political will, commitment of the high-level government officials to NRA;
4. organizing the interaction of the agencies involved in NRA, primarily in relation to collecting, processing and summarizing comprehensive administrative reporting (statistics) in the AML/CFT area, the results of the analysis of which should become the basis for NRA and serve as objective criteria for adjusting the ML deterrence policy;
5. availability of an NRA coordinating agency;
6. flexibility (updating, development) of the NRA system;
7. a combination of quantitative and qualitative input information, its sufficiency and versatility;
8. documenting the NRA toolkit and results.

A detailed overview of the above principles is provided below.

1. Harmonization of NRA goals and scale

The goals of risk assessment may include:

- assessment of the nature and scale of ML/TF and related predicate crimes, i.e. the threats. The said assessment is to identify the potential scope of proceeds laundered in the country, as well as to establish the ML/TF methods taking into account the results of the national FIU operation, results of law enforcement investigations, and taking into account prosecution and conviction;
- identifying specific products, types of activity, areas, industries that are most vulnerable to the ML/TF risks;
- identifying weaknesses of the AML/CFT system, as well as other peculiarities of jurisdiction which make it attractive to offenders involved in ML, i.e. vulnerabilities;
- development of a National AML/CFT Strategy and Action Plan for its implementation;
- distribution of resources between individual links of the national AML/CFT system, for example between law enforcement authorities, SFME and FIU.

NRA goals and scale may vary and depend on many input managerial decisions. The scale of assessment, in particular, may be influenced by a decision whether NRA is conducted for ML and TF separately or in combination. On the other hand, the NRA goals and scale depend on the users' needs (politicians, regulatory, supervisory and operative authorities, financial institutions, designated non-financial businesses and professions, the public, academia and experts) and should therefore be coordinated with the NRA stakeholders, actors and result users.

It is noteworthy that FATF and MONEYVAL guidances and reports are developed in a differentiated way, taking into account the following features:

- areas of criminal activity;
- ML/TF methods;
- types of operation of the agencies that are part of the AML/CFT system;
- types of organizations and persons who carry out money transactions;
- money transaction methods;
- regional peculiarities.

NRA goals and scale depend on:

- its nature;
- a list of questions that need to be answered;
- answer criteria, methods;
- participants;
- information necessary for reliable assessment;
- decisions made, based on the NRA results.

2. NRA Comprehensiveness

Risk assessment at the national level is inextricably linked with their assessment at the supranational level, as well as at the level of specific national sectors, industries, complexes, types of economic activities, products and services, and regions of the country. The above stipulates implementation of the assessment comprehensiveness principle. Such comprehensiveness can be defined as an opportunity to summarize the results of all the individual assessments and to build a coherent picture of the national risks.

Comprehensiveness implies existence of a unified approach to NRA, use of a unified information base (a single database of statistical indicators), and a systemic approach to collection of quantitative data in the AML/CFT area. Estimates obtained by various types of economic activity, different sectors, industries, complexes, areas, products and services, should aggregately give an overall assessment of the risks in the country. Assessments by the FIU, various supervisory, law enforcement and judicial authorities in the AML/CFT area should be comparable. At the same time, when implementing NRA, the main efforts should focus on assessing the risks that affect the entire AML/CFT system.

3. Political will, commitment of the high-level government officials to NRA

In the FATF guidances, political will is defined as a clear commitment from high-level government officials to the NRA exercise; also these officials need to understand existence of corresponding risks. NRA should not depend on a particular political course and legislative reforms, and also on lobbying by stakeholders.

4. Organizing interaction of the agencies involved in NRA in the AML/CFT area

Risk identification and assessment involves:

- ministries, agencies, state authorities
- law enforcement agencies and prosecutor's offices;
- special services and FIU;
- regulatory and oversight agencies;
- international partners;
- representatives of the private sector, financial institutions and DNFBP;
- industry associations and self-regulatory organizations, representatives of the academia and expert research environment.

An important role in risk assessment is played by financial and credit institutions, primarily banks that deal with a significant number of financial transactions and clients. Banks identify high-risk clients, as well as related client transactions related to corresponding risks. Regulatory and oversight agencies, as well as FIU and law enforcement agencies, develop a system of statistical indicators – criteria for risk assessment, provide coordination in the process of implementing the Strategic AML/CFT Action Plan.

In identifying and assessing risks, international cooperation is crucial for information exchange and utilizing the experience gained. For example, a valuable source of information

is data on cross-border financial flows and taking into account supranational approaches to AML/CFT risk assessment.

The SFMS pursues international cooperation based on both bilateral and multilateral interaction.

Bilateral cooperation is implemented through interagency, intergovernmental and interstate agreements.

Multilateral interaction is aimed at:

- developing and improving international AML/CFT standards (including in the area of RBA application);
- implementing these standards in the national legal systems.

Multilateral cooperation is implemented within FATF, MONEYVAL, Egmont Financial Intelligence Unit Group.

5. Availability of an NRA coordinating agency

A significant number of participants involved in the NRA requires a coordinating agency for managing collection and analysis of information, as well as for preparation of the final risk assessment document.

The FATF guidances note that risks in different countries are assessed using different models:

- by involving several supervising agencies or one specific organization;
- by implementing a one-time research project on the study of the AML/CFT situation.

The coordinating functions in different countries are performed by different structures: Criminology Research Council (Australia), Financial Information Processing Unit (Belgium), Intelligence Working Group (Canada), National Police Authority (Japan), Financial Intelligence Office (China), National Police Services Agency (The Netherlands), Center of Intelligence Against Organized Crime (Spain), Serious Organised Crime Agency (UK). A multi-agency model is also used (Poland, USA).

In Ukraine, the State Financial Monitoring Service of Ukraine is responsible for conducting NRA.

6. Flexibility (updating, development) of the NRA system

Flexibility of the system allows for its adjustment and development, taking into account new threats and arising vulnerabilities. Development is primarily related to continuous improvement of the risk assessment methodology, with inclusion of new statistical data sources in the input information base, a comprehensive analysis of NRA results in dynamic development, identification of emerging trends and multiple regression relationships between the aggregate of statistical data on which the NRA empirical findings are based.

At the same time, it is necessary to take into account the changes that take place in international standards, in the country's political and economic structure. FATF guidances recommend updating the risk assessment every 3 to 5 years.

7. A combination of quantitative and qualitative input information, its sufficiency and versatility

The FATF guidelines note that the NRA quality to a large extent depends on the type and quality of the available statistics. Data collection procedures within the national AML/CFT system are described in detail in the 2012 OSCE Handbook, which notes that various data are important in the risk assessment: retrospective and prospective, quantitative and qualitative, as well as combined.

Quantitative estimates based on statistics are more reliable. Time retrospective series of dynamics allow to predict trends and future problems. The significance of the quantitative data is emphasized in the above OSCE document, as well as in the FATF guidance on "Guidance on AML/CFT-related data and statistics".

Indicators calculated on the basis of quantitative data allow not only to confirm the expert-identified quality assessment of threats and vulnerabilities, but also to more deeply consider the components of the national AML/CFT system, measure them, compare and prioritize.

Among other data, quantitative assessments of the AML/CFT system include statistics on criminal justice and asset restrictions, as well as data on the resources involved in the AML/CFT system, on the number of suspicious financial transactions and the amount of funds transferred through the financial system using such transactions, etc.

Matrices (templates) can serve as tools for collecting quantitative data, examples of which, with breakdowns into thematic sections, are provided in the FATF and OSCE guidances, as well as additional criteria used in the process of assessing compliance with the FATF recommendations and assessing the efficiency of the national AML/CFT systems. The said criteria are contained in the 2013 FATF Methodology for Assessing Recommendations (as amended in 2017).

The importance of taking into account the above criteria from the FATF Methodology is that it is the main working document used by MONEYVAL Committee representatives when conducting mutual evaluations. In turn, the goal of mutual evaluations of countries by the FATF, Committee, IMF, and World Bank experts is to form efficient AML/CFT systems in countries.

The Committee performs mutual evaluations for all the relevant international standards in the legal, financial, and law enforcement areas. The MONEYVAL reports contain detailed recommendations on improving the efficiency of the national ML and TF combating regimes, as well as on the ability of states to engage in efficient international cooperation in these areas.

In its handbook, OSCE provides the following topical sections for formation of matrices (templates) for collection of quantitative characteristics (statistics):

- reports received by the national FIU;
- law enforcement agencies and the criminal justice system;
- asset blocking;
- AML/CFT resources and supervision;
- international cooperation;
- regulated sectors;
- proceeds of crime and terrorism financing assets.

Each matrix is a set of quantitative indicators in terms of categories of predicate crimes or reporting organizations.

At the same time, not all risks can be measured, and the statistical base requires a long period of data accumulation. In connection with this, there is a need for qualitative data, in particular:

- information from intelligence agencies;
- research, expert, and topical assessments;
- results of situational and typological research.

Expert assessments are obtained through surveys, questionnaires, seminars, interviews.

In order to save time and facilitate further processing of information, polling (questionnaires) should be sent in an electronic form.

The main questions, answers to which are advised to be collected by filling in the forms of electronic **questionnaires** are recommended to include the following:

- identify the main threats that arise in the context of attracting financial institutions to the AML/CFT related schemes;
- assess the existing risks of using financial products and services for the ML/TF purposes, to identify their dynamics compared to the previous time period (year, three years);
- rank (prioritize) financial products and services taking into account the level of their potential risk to be used in the ML/TF transactions;
- provide a description of the persons interested in establishing and using ML/TF schemes, based on the analysis of unusual (suspicious) financial transactions effected through a financial institution;
- receive recommendations of financial institutions regarding the desired areas of the AML/CFT system development.

An important issue that needs to be addressed in the planning of actions based on the NRA results is focusing attention and resources on those sectors and types of economic activities that are most vulnerable to the ML/TF risks: foreign economic activity, construction, land market and real estate transactions, housing and communal services, banking, macrofinancial activities, securities market, trade, military-industrial complex, consulting services, etc.

A separate block of issues to be covered by the NRA relates to external factors of risk arising in the national AML/CFT system. Among the said factors, the following merit special attention: economic, legislative, political, social, religious.

According to the Europol Financial Intelligence Unit[21], as well as taking into account the Ukraine Report on the first NRA, the highest-risk financial transactions in the ML/TF context include: depositing cash to be credited to the initiator's account; receiving and/or transferring cash; receipt of funds by high-risk persons (first of all, national politically exposed persons); cash transfer without opening an account and/or without using the initiator's account; transfer of funds abroad under foreign economic agreements (contracts), which do not provide for the actual supply of goods to the customs territory of Ukraine; carrying out transactions with funds, whose legal sources of origin cannot be substantiated, etc.

Since a special risk area includes cash flows circulating between countries, the

21 From suspicion to action – Converting financial intelligence into greater operational impact. [Electronic resource]. – Access mode: www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact

following are particularly valuable: information on cross-border financial flows; international information on the ML-related criminal activity; on transnational organized crime.

8. Documenting the NRA toolkit and results

Documenting the NRA methodology, methods, procedures, information which contains the results of the analysis and conclusions is necessary for awareness of all the assessment participants of their powers and obligations, for ensuring transparency of procedures, identifying dynamics and trends in risk assessment. The documentary information is the basis for decision-making by expert assessors in the AML/CFT area.

1.3. Overview of the most common NRA methodologies

1.3.1. International Monetary Fund Methodology

This section summarizes the main components of the structure that the IMF specialists are developing to be able to perform a national assessment of the ML and TF risks. Even though FATF emphasizes the need of applying RBA to AML/CFT, in practice many problems arise when clearly applying the risk management concept in the AML area. RBA implementation is complicated by the fact that the ML and TF processes are very multivariant, usually deliberately disguised and, given the above, these **processes are difficult to document and difficult to quantify**. Further, various stakeholders in the AML/CFT system consider the **ML and TF risks from different perspectives**: RE are concerned about legal, operational and reputational risks generated by their clients, products and services; SFME are concerned that the supervised REs should not be used (knowingly or unknowingly) to launder proceeds of crime; the law enforcement and security authorities are concerned about the risk that socially dangerous and unlawfully acting entities will be able to avoid detection and punishment when using proceeds from crime; senior public officials are concerned about the socio-political and socio-economic implications of any of the above risks.

From the IMF point of view, the application of the traditional risk-management concept to the ML/TF issues serves several purposes at once. Firstly, the RBA allows IMF staff to focus on limited resources in the countries that generate or are facing substantial ML/TF risks. Secondly, based on the country-specific assessment, RBA allows focusing on those aspects of the financial sector, as well as on those legal and institutional (organizational) structures that are the weakest (most vulnerable) links in the AML/CFT system. Thirdly, through technical assistance, IMF can help member states understand, assess and mitigate the ML and TF risks they are confronted with. Fourthly, the above IMF activity can help the international community more efficiently and clearly formulate and focus on the main objectives of the AML/CFT regimes, as well as assess the efficiency of AML/CFT measures in relation to achievement of the goals formulated at the previous stages.

The RE and the SFME are, by their nature, limited by the problems outlined above, and by the difficulties arising from applying both generic (verbal) risk criteria and quantitative criteria that may vary in very wide ranges of normality.

Despite the entire cascade of the existing criticism of the imperfection of the instruments offered today to assess the multivariant ML/TF risk, there is a clear belief in the need to continue the work, since the outlined principles of its organization are correct. The undeniable benefit of introducing a well-thought NRA in the AML/CFT area is focusing on a disciplined and well-regulated process of collecting, processing and summarizing the necessary data to generate informed judgments and to make efficient decisions in the AML/CFT system at both micro and macro levels.

ML is the process of transforming illegal “inputs” into the seemingly legitimate “outputs”, which is accompanied by abuse of financial institutions as intermediaries in the process. ML covers a wide range of acts aimed at disguising a criminal source of origin of funds.[22]

22 International Monetary Fund (IMF) (2001), ‘Financial system abuse, financial crime and money laundering’, Background Paper (SM/01/46), February 12, 2001. [Electronic resource]. – Access mode: www.imf.org/external/np/ml/2001/eng/021201.htm

Thus, criminal incomes reflect "inputs" in the ML process, while "outputs" are a set of assets with the aura of legality of the source of their origin. The ML process can cover a series of transactions that take place both in the formal and informal sectors. Every supplier of a product or service that can be used to save or transfer value, becomes a potential victim of abuse of its activities as an intermediary in the ML process. ML, in view of the above, is usually associated with institutions of the main financial sector (banks, non-bank deposit and credit institutions, securities traders and insurers), as well as with other financial institutions (for example, non-bank payment systems), types of economic activity and professions, which work in close connection with the financial sector (barristers, accountants, auditors, notaries, lawyers), and other institutional units of the real economy (casinos, realtors, antiques, jewelry, and hotel and restaurant business, etc.).

TF covers activities related to creation and transfer of financial resources to be provided to terrorists with the aim of their carrying out targeted terrorist attacks. This activity covers abuse of similar types of financial and non-financial intermediaries as in the case of ML, however, it is different in one main aspect. The essence of the difference is that in the case of ML the money laundered always has a criminal source of origin (the purpose of ML is to give them the appearance of legal origin), whereas in the case of TF, funds may come from both legal and illegal sources.

The IMF methodology outlines the main NRA components and describes the relevant processes and tools involved. As of the early 2018, various aspects of the methodology have been applied in over 50 countries. **The methodology proposes to consider three keys to ML and TF risk assessment:** threats, vulnerabilities and consequences.

International risk management standards define **risk as a function of occurrence likelihood of negative events**.[23] The occurrence likelihood of these events is a function of coexistence of a threat and vulnerability to this threat. In other words, risk events occur when threat exploits vulnerability. Formally, R – the national ML and TF risk level – can be expressed as:

$$\boldsymbol{R = f[(T), (V)] \times C}\ (1.1.), \text{ where}$$

"T" is threat; "V" is vulnerability; "C" is ML and TF risk occurrence consequences. Accordingly, the level of risk can be mitigated by reducing the threats, vulnerabilities (weaknesses), or the potential risk consequences. For example, the probability of spending drug dealer revenues (threat –T) by exploiting weaknesses of vehicle traders is obviously quite high in many jurisdictions, but the negative consequences of this particular transaction are relatively insignificant. In view of the above, this event would be assigned a lower ML and TF risk (R) in terms of of its occurrence consequences compared with the level of risk associated with organization of illicit drug trafficking on an industrial scale, with subsequent laundering of drug proceeds through acquisition of commercial real estate or a significant amount of government bonds (vulnerable place – V), which would have incomparably greater negative consequences in terms of increasing such a criminal organization's capability of influencing socio-political and socio-economic area in the relevant jurisdiction and therefore a higher ML and TF risk.

Let us consider the main components of Formula (1.1) in more detail.

23 Eide, E. (2000), 'Economics of criminal behaviour', in B. Bouckaertand G. De Geest (eds), Encyclopedia of Law and Economics, Cheltenham, UK and Northampton, MA, USA: Edward Elgar Publishing [Електронний ресурс]. – Access mode: http://encyclo.findlaw.com/8100book.pdf

R: The ML and TF risk level is characterized by net risk – it takes into account the influence of management (control) on minimizing the occurrence level of the generic (normal, inseparable) risk inherent in any field of activity. In other words, the control (supervisory) measures can reduce the level of generic risk, but the lack of appropriate measures does not increase the normal risk level. Supervision in the ML and TF area is divided into two categories: the first one is to carry out general supervision and develop risk reduction factors (general regulatory requirements); the second one is implementation of specialized supervision in the ML/TF area which takes into account the requirements of 40 FATF Recommendations. As one of the most important goals of risk management is efficient allocation of resources to mitigate the most important risks, the IMF recommends **focusing on the risks from ML and TF transactions substantial for a certain country**. A substantial ML/TF transaction is considered to be the one that generates the highest amount of ML relative to GDP or relative to the total scope of transactions effected in a certain segment of the financial sector over a period of time. In addition, substantial ML transactions should include the transactions, the negative consequences of which are particularly significant. A substantial ML transaction may relate to a single (one) transaction or a series of transactions that enable a substantial amount of money to be laundered over a 12-month period. A substantial ML transaction can include one that is part of a separate ML scheme or part of an entire series of unrelated ML schemes. *(Reference: pilot tests by the IMF experts suggest classifying as substantial ML transactions those ones, the total value of which throughout the year is from USD 100 million per year for an individual product, service or sector within a specific jurisdiction and from USD 1 billion in the global dimension).*

Unlike ML transactions, it is much more difficult to formalize the TF risk assessment, if at all possible, given the specifics of the TF transactions outlined above. *(Reference: the calculations carried out by the IMF experts claim that an adequate benchmark for referring typical transactions to those that may be related to terrorist financing is an amount from 10 million USD per year. The indicated amount is based on the assessment of average losses incurred as a result of a single terrorist act, and also takes into account the amounts of annual operating costs necessary to operate the current known terrorist organizations).* However, the overall RBA in the risk management context in the AML/CFT area should also be maintained for TF, at least on the basis of qualitative criteria for identifying and detecting individuals, organizations and transactions that may be related to TF.

T: From the ML risk assessment point of view, the **threat** is largely **due to the nature and scale of potential demand for ML transactions**. This demand is generated by the stakeholders with a pool of illegally-acquired assets that need to be laundered. From the TF risk assessment point of view, the threat is mainly due to the nature and scope of the funds intended for TF, as well as to the jurisdiction through which the funds are transited. **With respect to ML**, there are two components that determine the proceeds of crime (POC) that need to be laundered in any given jurisdiction: 1) the nature and types of domestic predicate crimes that exist and the scale of proceeds that they generate; and (2) the nature and scale of proceeds generated outside of the jurisdiction that are likely to enter the jurisdiction for laundering. **In relation to TF**, there are two similar components: 1) the nature and types of fundraising efforts at the national jurisdiction level; 2) the amount of funds raised outside of the jurisdiction that are likely to enter the jurisdiction for further transit or use to commit terrorist acts within the limits of a national jurisdiction. Therefore, in order to properly assess the ML/TF risks, it is necessary to collect data in the context of

the two above components in order to develop the ML/TF probability indicators, making them an integral part of the overall NRA in the AML/CFT area. Development of these indicators requires a clear understanding of the nature, occurrence forms, and amount of potential illegal proceeds generated by each type of predicate crime in the country, as well as a clear understanding of the TF environment in the country (its existing and potential sources and methods of transiting funds intended for TF). The said work will contribute to defying (quantifying) a clear ML/TF risk level, which will be considered substantial for taking all the necessary measures within the framework of the national AML/CFT system.

V: Vulnerability in the ML/TF risk assessment is related to the essential characteristics of products, services, product and service distribution channels, client bases, institutions, systems, organizational structures and jurisdictions (including weaknesses in the national AML/TF system, in the regulatory and supervision mechanisms) that enable ML/TF abuse. The primary task in vulnerability assessment is to assess the factors that contribute to successful ML/TF transactions in terms of relevant products, services, client categories, financial transaction methods, and more. The result of such an assessment should be development of appropriate vulnerability indicators. The vulnerability indicators are numerous, but they can be grouped into the following categories: geographical location; financial products and services; the level of informality (shadowing) of the relevant sector of economy (type of economic activity); gap in the AML/CFT systems and adequacy of the existing regulatory and supervisory mechanisms in the AML/CFT area; the level of corruption in the relevant sector of economy (type of economic activity); efficiency of the law enforcement and criminal justice system; other characteristics of a national jurisdiction that facilitate the ML/TF transactions (for example: level of organized crime). Vulnerability indicators should be aggregated and combined with threat indicators to produce an overall analysis of the likelihood of substantial ML or TF occurring successfully.

C: The **consequences** relate to the outcomes that result from the occurrence of risk events. Consequences can be manifested as incurred losses, loss of assets, undermining the reputation of a financial institution, loss of client confidence, loss of income in business units and the state as a whole. In general, it can be argued that the ML and TF processes generate **two types of consequences**: the first one is associated directly with the ML and TF related transactions (for example: committing predicate crimes; engaging financial institutions in laundering; committing terrorist acts); the second one is associated with the use of assets after they have been legalized (laundered).

One of the most common systems to date is an ML and TF risk assessment system characterized by **a combination of qualitative scoring indicators (points)**. The system focuses on the main risk events associated with the ML or TF process that, in turn, make a difference to the ML or TF risk profiles. This approach helps better understand, model and analyze the ML and TF processes by differentiating and identifying the key contributing events that increase the likelihood of successful ML or TF. By generating scores for a range of objective and subjective indicators that are used to suggest the level of threats, vulnerabilities, and consequences related to ML and TF, it is possible for risk managers to assess the overall risk of substantial ML or TF, their nature, magnitude, and consequences. Such a **qualitative scoring analysis** is used to create two proxy variables for each estimated ML and TF case: the first variable is the **likelihood of substantial ML and/or TF**; the second one is the **ML and/or TF consequences**. The indicated two variables are combined in the overall system of the national ML and TF risk assessment.

The next part of this section describes in more detail the ML and TF risk analysis system, which is based on the IMF Methodology, focusing on the analysis and evaluation of the ML processes.

The most important NRA components in the AML/CFT area include:

1. the approach to obtaining indirect indicators of the likelihood of successful ML and TF in substantial volumes based on the assessment of the main ML/TF-related events (transactions), as well as on the use of analytical factor modules and indicators associated with these modules for qualitative scoring analysis of the likelihood of occurrence of major risk events;
2. the approach to obtaining indirect indicators of the relevant consequences which are generated by successful ML/TF transactions in substantial volumes;
3. the approach to assessing the overall ML or TF risk level.

To operationalize risk (R), a risk event must be identified in relation to threats (T) and vulnerabilities (V). The main risk events stem from the circumstances that coexist to encourage ML and TF transactions. These circumstances, which arise at the intersection of threats and vulnerabilities, create the basis for assessing the ML and TF risk, and to analyze the likelihood of successful completion of the ML/TF transactions in substantial volumes. Risk events are always associated with the dynamics of the ML/TF process. Firstly, it is a matter of **obtaining and retaining a certain amount of illegal proceeds by a laundering perpetrator** (main beneficiary), or possession of legal or illegal proceeds by a perpetrator that finances terrorist acts (T – threat). Secondly, the **laundering perpetrator** or the terrorist financing perpetrator **finds the products, services, assets or other circumstances that can be used to effect ML/FT transactions** (vulnerability). Thirdly, **ML or TF entities estimate the likelihood of being detected, sanctioned and deprived of relevant assets** by the law enforcement system in the AML/CFT process (given the vulnerabilities in the ML/TF transaction). Thus, successful ML/TF transactions for substantial amounts are possible with occurrence of the following interrelated events:

1. **Effecting ML or TF transactions:**
   - 1.1. existence of a significant amount of criminal proceeds or existence of terrorist funds that need to be transferred to terrorist organizations;
   - 1.2. existence of products, asset services, and other circumstances that can be used to successfully effect ML/TF transactions.
2. **ML or TF enteties (including accomplice partners and advisers) do not appear:**
   - 2.1. the ML/TF crime is not detected by the law enforcement agencies. The direct and indirect ML/TF deterrence system provides inadequate response (through RE suspicious financial transaction reports). The criminal justice process is inefficient;
   - 2.2. the ML/TF crime is detected, but inadequately investigated by the law enforcement agencies;
   - 2.3. the ML/TF crime is detected, adequately investigated, but the perpetrator is not criminally or judicially prosecuted;
   - 2.4. the ML/TF crime is detected, adequately investigated, criminally and judicially prosecuted, but the perpetrator is not tried (not convicted).
3. **ML or TF entities are not sanctioned adequately**
   - 3.1. in the case of conviction, the ML/TF entities receive inadequate punishment;

3.2. in the case of punishment by deprivation of liberty, ML/TF entities are not deprived of their assets.

Likelihood of these events occurring is derived from related risk analysis modules (RAMs) containing factors, sub-factors and their indicators. Each RAM identifies unique risk factors linked to the relevant threats and vulnerabilities that affect the likelihood of the risk event(s) occurring. The structure and grouping of the ML risk related events, as well as the analysis modules used to obtain indirect (orienting) indicators of the ML likelihood are provided in Table 1.1.

Table 1.1. ML Risk Analysis Framework: Risk Events and Analysis Modules

Contributing risk events	Threats (T), vulnerabilities (V) that increase the likelihood of risk event (R) occurrence:		Areas to analyze (modules of risk factors)	Additional factors (sub-factors) and indicators
1	2		3	4
Risk event: 1) Effecting ML or TF transactions				
(1a) Domestic criminal proceeds: generated or available	(t) Availability of domestic criminal proceeds (v) Inadequate suppression of domestic predicate crime		(A) Amount of domestic proceeds: generated or available **(1)** (B1) Law enforcement agencies (crime suppressing) **(2)**	Types of crimes generating income: fake entrepreneurship; tax evasion; embezzlement; abuse of office, etc. Powers, resources, effectiveness **(3)**
(1b) Foreign proceeds entering the jurisdiction.	(t) Presence of foreign proceeds (v) Existence of cross-border products, services, assets, and circumstances that can be abused to meet ML's importing and exporting needs. (v) Cross-border scrutiny does not suppress cross-border ML activity.		(C) Amount of foreign proceeds entering the jurisdiction **(1)** (D) Cross-border products, services, assets, circumstances **(4)** (E) Border security measures and scrutiny	Jurisdiction of POC origin and factors contributing to receiving POC in the jurisdiction of their origin Unique cross-border aspects areas that require comprehensive analysis **(5)** Currency transfer, physical assets, people, and financial transactions
(1c) Abuse of jurisdiction's products, services, assets, or other circumstances for ML activity	(v) Jurisdiction and its institutions providing goods, services, assets, and other circumstances that can be abused to meet the ML's needs.		(F) General jurisdiction environment (G) Products, services, assets, and circumstances offered **(6)**	Characteristics of the economy, legal system (rule of law), business climate, quality of regulatory policy, political environment, culture and integrity, obligations in the AML/CFT area. Sectors, institution types, scale, client base, delivery channels, general mitigants
(1d) Corruption to facilitate ML occurring	(v) Corruption in the system of law enforcement agencies, cross-border corruption (customs), corruption in other institutions		(H1) Corruption **(7)**	

Contributing risk events	Threats (T), vulnerabilities (V) that increase the likelihood of risk event (R) occurrence:		Areas to analyze (modules of risk factors)	Additional factors (sub-factors) and indicators
1	2		3	4
Risk event: 2) ML entities (including accomplice partners and advisors) are not detected (not sanctioned)				
(2a) if attempted, ML activity not being detected by the authorities (RE, SMFE, and law enforcement agencies)	(v) LEAs do not detect ML activity directly (in the process of their own investigations) (v) LEAs and other agencies authorized to detect	(v) LEAs only investigate predicate crimes (v) LEAs do not submit requests to international FIUs or do not respond to international FIU requests on ML (v) National FIU does not receive quality reports from RE and SFME on ML activity due to: *(v) insufficiency, incompleteness, untimeliness, and inconsistency of reports;* *(v) Poor quality, including over-reporting.* *(v) Inadequate monitoring of transactions;* *(v) Inadequate information about clients;* *(v) Institution incapacity of RE and SFME;* *(v) Inadequate supervision of RE;* *(v) Ineffective submittal of reports to the FIU.*	(B2) LEA (specific efforts to identify ML) (I) STR reporting system (J) Transaction and account monitoring (K) Client identification, profiling, ongoing and enhanced due diligence (L) Capacity and competence of institutions (M) Supervision (N) FIU	Effectiveness of ML suppression and domestic cooperation Requirements, quantitative and qualitative indicators, sectors, institution types (RE, SFME) **(8)** Requirements, effectiveness **(9)** Requirements, effectiveness Systems and controls, resources, guidances Effectiveness, especially when deficiencies are identified. Effectiveness of analysis, dissemination (Summarized materials/ additional summary materials)
(2b) if detected, ML activity not being investigated adequately by LEA	(v) LEA ineffective at investigations of predicate crimes and related ML transactions (v) LEA POC/ML investigators cannot obtain leads or evidence during investigation of predicate crimes and ML.	(v) Poor access to information on suspicious financial transactions submitted by RE to FIU (v) Inability to obtain beneficial ownership information (v) Inability to obtain information and evidence from foreign jurisdictions	(B1) Law enforcement agencies (ML suppressing) **(10)** (O) Record-keeping, limited access to them and professional secrets (P) Transparency of ownership **(11)** (E2) Cross-border cooperation	Effectiveness of anti-legalization investigations Requirements, effectiveness, secrecy Entity and asset types, register requirements, powers to obtain ownership structure information Effectiveness of administrative cooperation, MLA, and extradition to obtain evidence and people
(2c) if investigated, entity of ML activity not being criminally and judicially prosecuted	(v) Offenders are outside jurisdiction (v) Prosecutor not pursuing ML charge (v) Prosecutor not pursuing any charge (v) Inefficient or ineffective criminal justice or court system	(v) Inability to extradite or prosecute an offender in his absence	(R1) Criminal justice system (prosecution and judiciary)	Prosecution and convictions of both predicate crime and ML, criminal justice system, priorities, constitution, law and jurisprudence
The ML/TF crime is detected, investigated, criminally and judicially prosecuted, but the perpetrator is not tried (not convicted)	(v) Ineffective criminal and judicial prosecution (v) Incompetent judiciary (v) Inadequate wording of criminal laws (articles of the criminal code)	(v) Inability to extradite or prosecute an offender in his absence	(R2) Criminal justice system (laws; articles of the criminal code)	Adequacy of laws (articles of the criminal code)
(2e) Corruption to facilitate ML occurring	(v) Corruption in LEAs, FIU, CJS, RE and SFME system.	(v) Inability to extradite or prosecute an offender in his absence	(H2) Corruption **(7)**	

Contributing risk events	Threats (T), vulnerabilities (V) that increase the likelihood of risk event (R) occurrence:		Areas to analyze (modules of risk factors)	Additional factors (sub-factors) and indicators
1	2		3	4
Risk event: 3) ML entities are not sanctioned adequately				
(3a) Convicted ML entities are not deprived of their assets	(v) Inadequate sanctions (v) Ineffective system for sanction implementation	(v) Inadequate imprisonment terms (v) Inadequate fines (financial and property) sanctions (v) Ineffective imprisonment system (v) Ineffective system for collecting fines (financial and property)	(R3) Criminal justice system (sentencing and imposition) (R3) Criminal justice system (sanctioning)	Powers, sanctions imposed **(12)** Minimum/maximum and average prison terms served Minimum/maximum amount and average of fines collected (financial and property)
(3b) Convicted ML entities are not deprived of their assets	(v) Inadequate confiscation orders being made (v) Inadequate recovery of assets	(v) Inadequate resources devoted to asset recovery (v) Inability to recover assets from foreign jurisdictions (v) Ineffective use of provisional measures (procedural rights) by law enforcement agencies within the framework of legal proceedings	(R3) Criminal justice system (asset confiscation) (E3) Cross-border asset recovery (B4) Law enforcement agencies (procedural rights)	Powers, policy, sanctions imposed, effectiveness focus on assets confiscated **(12)** Effectiveness of administrative cooperation and MLA to recover assets Assets seized or frozen
(3c) Corruption to facilitate ML occurring	(v) Corruption in LEAs, FIU, CJS, RE and SFME system.		(H3) Corruption **(7)**	

The modules listed in the third column of the table are called “Area(s) to analyze” (modules of risk factors). Each module in the third column of the table identifies unique risk factors that are associated with threats and vulnerabilities (weaknesses) and affect the likelihood of a risk occurrence within the next 12-month period, taking into account the efficiency of the existing control measures. The list of indicators corresponds to each risk factor. The risk factors and their indicators are structured within the framework of analysis modules based on the nested hierarchy principle. The highest level of hierarchy includes those factors that directly affect the likelihood of a corresponding ML or TF risk occurrence. The next (lower) hierarchical level of the corresponding group of factors includes the sub-factors that affect the higher hierarchical level factors, etc. The last column of Table 1.1. summarizes the main highest level indicators for each analysis module.

The analysis modules for the ML risk assessment use both quantitative and qualitative indicators, based on the data obtained from both open and private (commercial) sources of information (IMF, World Bank, UN, country mutual assessment databases, and published documents, non-public data (internal statistics of the public authorities)).

Within each analysis module, each risk factor should be analyzed taking into account the indicators that are relevant to it and only after this the factor is subject to **scoring (qualitative assessment in points)**, which in turn enables pre-determined establishing of criteria for decision-making associated with an evaluated likelihood of substantial ML occurrence. For each indicator that the ML risk factors listed in the table correspond to, its own decision-making criteria (score points groups) should be determined, depending on which the ML risk increases or decreases. The indicated criteria should be typical (approximated) to the maximum extent for similar types of indicators. The decision-making

criteria are descriptive. They correspond to a qualitative measurement scale formed on the basis of scoring assessment of factors and relevant indicators and consist of seven risk levels (Table 1.2):

Table 1.2. Risk level scores

Risk level score	Risk Level Descriptor	Risk Mitigation Priority
≤ 6-7	Extremely high risk	Extremely high priority
≤ 5-6	Much higher risk	Much higher priority
≤ 4-5	Higher risk	Higher priority
≤ 3-4	Medium risk	Medium priority
≤ 2-3	Lower risk	Lower priority
≤ 1-2	Much lower risk	Much lower priority
≤ 0-1	Extremely low risk	Extremely low priority

The scoring of each indicator is designed so that there is a significant difference between the scores awarded on the qualitative scale. Some rating points in the ML risk assessment scale are based on the efficiency calculation based on the available statistical data that is collected and summarized in the periodic mutual evaluation reports. Scoring is based on the concept of using the most available data to evaluate relevant indicators. The above data can serve for indirect assessment of linked factors relative to the main one. Scoring does not require that each indicator of the main or secondary risk factor be assessed. The indicators for which it is impossible to obtain data should be assigned a default score of "5" ("High Likelihood of Risk").

The analysis is used to determine the values of two variables: one is to assess the probability of occurrence of substantial ML or TF, and the second one is to assess the corresponding consequences. The indicated variables are combined to assess the national ML and TF risk level. The structure and grouping of the ML and TF risk events and analysis modules are used to obtain a tentative probability indicator. A similar matrix can be used to obtain tentative consequence indicators, but it will vary depending on the relevant consequences that will be selected for a particular study. The indicators used for the analysis will be both quantitative and qualitative.

A higher level (score) indicates a higher occurrence likelihood of an event associated with substantial ML and the likelihood of more severe consequences. Tables 1.4. – 1.7. demonstrate this approach with some examples of the pre-determined decision-making criteria and scoring scale used for analyzing likelihood, taking into account: properties of products, services, jurisdictions etc.; effectiveness of general controls and mitigants; specific AML/CFT controls. The indicators used are suggestive of that likelihood, not perfectly representative of the actual ML risk likelihood. The proposed scoring system results in a relative likelihood score (i.e., scores are only meaningful in relation to other similar scores, across the modules, sectors, factors, regions, products, etc.).

Scores across indicators of the relevant analysis modules are assigned by **deriving the geometric mean** for all the indicators within a nested hierarchy. The scoring is aggregated upwards to sub-factor (the lowest level indicators within each indicator hierarchy), factor, module, and finally the overall likelihood level of a risk event occurrence is assessed. This is done using the nth root equation $\sqrt[n]{A}$, **where "n" is the number of indicators, factors, or risk events, and A is their product**. For the analysis modules that analyze the indicators broken down by RE types, it is recommended to have intermediate aggregation of the score in proportion to the scale of activity being undertaken within each RE type in the total of the transactions effected (submitted to the national FIU) by all the RE types.

The above method of score aggregation has the following three advantages. First, the method maintains the appropriate relationships between the analysis modules of ML risk assessment (in terms of factors and indicators) set out in in Table 1.1. By combining factor scores using this method, any one factor's influence is limited to its primary area of impact. Second, the geometric mean produces a more appropriate result than a simple average because it smoothes the outlying indicator scores, which is desirable at this stage of NRA development because many of the indicators still need to be tested for their suitability for estimating the actual ML or TF activity. Third, this approach always results in a score on the seven-point scale, making results easy to interpret.

The scores for each analysis module are aggregated to produce a score for the overall likelihood of substantial ML of TF abuse occurring in each jurisdiction of the world. The aggregated likelihood score calculates the geometric mean from each analysis module listed in the third column of Table 1.1. The following equation follows the outline of the key risk events in the table and calculates the geometric means within the scores corresponding to the factors given in each round bracket, after that – in each square bracket, and finally – in the total square bracket:

Likelihood score = geometric mean from $[[(\boldsymbol{A}, \boldsymbol{B1}), (\boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}), (\boldsymbol{F}, \boldsymbol{G})], [\boldsymbol{H}],$

$\big[(\boldsymbol{B2}, ((\boldsymbol{I}, \boldsymbol{J}, \boldsymbol{K}, \boldsymbol{L}, \boldsymbol{M}), \boldsymbol{N})\big), \big(\boldsymbol{B3}, (\boldsymbol{O}, \boldsymbol{P}, \boldsymbol{E2})\big), \boldsymbol{R1}, \boldsymbol{R2}], [(\boldsymbol{R3}, \boldsymbol{R4}), (\boldsymbol{R5}, \boldsymbol{E3}, \boldsymbol{B3})]]$

In order to score the ML consequences, a similar approach should be used to what is used to score the risk factors (see Table 1.9). Scoring of consequences should be made in the context of the structure of risk factors and sub-factors and their indicators. Decision-making criteria, measurement scale and scores for factors and their indicators are based on the seven-level semi-quality measurement scale (Table 1.4.). The higher the score – the greater the likelihood of substantial ML transactions being successful, the more negative the consequences of the relevant transactions are.

Finally, the geometric mean method (similar to that used for the ML likelihood indicators) aggregates the indicator for the ML consequences of all successful transactions.

The choice of managerial priorities based on the NRA results must take into account the different levels of the ML and TF consequences. First of all, in order to minimize the number of successful ML or TF cases, it is necessary to focus on the overall goal, which is most important for most AML/CFT regimes. The hierarchy of priorities should be correlated with the results obtained in the context of the analytical modules considered above.

The proxy indicators for consequence are derived largely from the perceptions of informed officials, using a structured approach to make informed judgments. The process consists of informing the officials of the results of the likelihood analysis, presenting them with general information about the potential impact of successful ML or TF abuse,

and asking them to choose what they think is the most adequate level of ML or TF consequences on each objective.

The overall level of the national ML or TF risk is derived by combining the jurisdiction's ML/TF likelihood and consequences proxy scores, and assessing whether the result falls within acceptable bounds. The combination can be done in two ways to aid understanding:

1. First, the two proxy scores can be combined using their geometric mean. This results in a one dimensional score which can be compared against the pre-determined scale in Table 1.4 to assess whether the overall ML/TF risk fits within the acceptable bounds, or whether it indicates that efficient steps need to be taken to mitigate its level;
2. Second, the two proxy scores can be combined and presented via a pre-determined matrix (Table 1.3). The matrix allows for an assessment of whether the level of risk is acceptable, but with the added dimension of identifying the relative contribution of likelihood and consequences.

Tabl. 1.3. Level of ML or TF Risk Matrix

Extremely high							Extremely high
Much higher						Much higher	
Higher					Higher risk		
Medium				Medium			
Lower			Lower				
Much lower		Much lower					
Extremely low	Extremely low						
Vulnerability leve ↑	Extremely low	Much lower	Lower	Medium	High	Much higher	Extremely high
Consequence level →							

Thus, it is possible to present a risk matrix or graph that shows the likelihood score plotted against the score for each of the identified risk event consequences. It should be noted that consequences may vary significantly depending on whether the context is domestic or international. Hence, the NRA approach proposed in the IMF Methodology also allows some consequences to be measured against both the absolute scales and against the gross domestic product.

Table 1.4. Examples of scoring for indicators of likelihood linked to intrinsic properties or products, services, jurisdiction, etc.

Likelihood descriptor	Measurement scale for economic activity	Provides products, services, assets, or other circumstances	Likelihood of an event or activity occurring annually – descriptor	Likelihood of an event or activity occurring annually – as potential probability	Likelihood of an event or activity occurring annually – as an indicative frequency	Indicator score
Extremely higher likelihood	1 tln +	Extremely sophisticated range and volume	Almost certain	More than 95% chance	At least once per year	7
Much higher likelihood	100 bln -1 tln	Extensive range and volume	Very likely	More than 75% chance	Occurs at least once every two years	6
Higher likelihood	10-100 bln	Attractive range and volume	Likely	More than 50% chance	Occurs at least every 3-4 years	5
Medium likelihood	1-10 bln	Normal range and volume	Possible	More than 30% chance	Occurs around once every 3 years	4
Lower likelihood	100 mln -1 bln	Not particularly attractive range or volume	Unlikely	Less than 30% chance	Might occur once every 5 years or so	3
Much lower likelihood	10-100 mln	Very limited range or volume	Rare	Less than 10% chance	Might occur once every 10 years	2
Extremely low likelihood	0-10 mln	Almost none	Almost incredible	Less than 5% chance	Might occur less than once every 20 years	1

Table 1.5. Examples of scoring for indicators of likelihood linked to general controls or mitigants-

Likelihood descriptor	Mitigant implemented across:	Ability of non-residents to do something	Police officers per 100,000 of population	Indicator score
Extremely high likelihood	< 10% of business activity or no requirements	Unlimited plus – may have special privileges	< 30	7
Much higher likelihood	≥ 10-25% of business activity	Unlimited – at least same ability as residents	≥ 30	6
Higher likelihood	≥ 25-50% of business activity	Almost unlimited – but with some additional administrative requirements	≥ 62.5	5
Medium likelihood	≥ 50-70% of business activity	Limited – with some minor limitations and conditions	≥ 125	4
Lower likelihood	≥ 70-85% of business activity	Very limited – usually requiring official approval or authorization	≥ 250	3
Much lower likelihood	≥ 85-95% of business activity	Extremely limited – some prohibitions, or always requiring official approval or authorization	≥ 500	2
Extremely low likelihood	≥ 95% of business activity	Impossible. Effectively prohibited.	≥ 1,000	1

Table 1.6. Examples of scoring for indicators of likelihood for vulnerabilities linked to weaknesses in AML/CFT controls

Likelihood descriptor	Reporting entities per AML/CFT supervisory staff member	For perceptions of performance quality and controls	Annual ML prosecutions per POC (if known) or GDP	Compliance with FATF Recommendations	Indicator score
Extremely high likelihood	No supervision	Abysmal	None	NC or not scheduled for 2004 methodology assessment	7
Much higher likelihood	≥ 100	Very poor	< 0.06	PC (ineffective implementation)	6
Higher likelihood	≥ 52	Poor	≥ 0.06	PC (or never assessed, but is scheduled for 2004 methodology assessment)	5
Medium likelihood	≥ 26	Adequate	≥ 0.12	Has been assessed previously, but not according to the 2004 methodology, scheduled 2004 methodology assessment	4
Lower likelihood	≥ 13	Good	≥ 0.24	LC (ineffective implementation)	3
Much lower likelihood	≥ 6	Excellent	≥ 0.48	LC (effective implementation)	2
Extremely low likelihood	6 or less	Best	≥ 0.96	B	1

Table 1.7. Examples of some pre-determined scales for scoring consequences

Consequence - Descriptor	Descriptor - Amount of ML or TF activity	Estimated ML activity scale	Estimated ML activity scale as % of GDP	Estimated TF activity scale	Estimated geographic reach	Estimated effect on a "system" or an "objective"	Indicator score
Huge or severe	Huge value	>$100 bln	> 20%	>$10 mln	More than one continent or global	Very serious, long-term impairment of system functions (destroys or almost destroys system's functionality) OR achievement of the objective	7
Very Major	High value	>$50-100 bln	10-19.99%	>$5-10 mln	Regional countries OR within a continent	Serious medium-term effects that begin to impair system functionality (or which destroy or almost destroy an isolated part of the system) OR that begin to impair achievement of the objective	6
Major	Major value	>$10-50 bln	5-9,99%	>$1-5 mln	Bordering countries only	Major, medium-term effects with potential to threaten system functions OR achievement of the objective	5
Moderate	Moderate value	>$1-10 bln	2.5-4.99%	>$100 thous -1 mln	National	Moderate, short-term effects not affecting system functions OR achievement of the objective	4
Minor	Medium value	>$100 mln -1 bln	1.25-2,49%	>$10-100 thous	Regional (within a country or some provinces or states)	Minor short-term effects on the whole system OR on achievement of the objective	3
Very Minor	Low value	≥$10-100 mln	0.625-1.249%	≥$1-10 thous	Local (within a city)	Minor short-term effects on isolated part of system OR on achievement of part of the objective	2
Negligible	Negligible value	<$10 mln	<0.625%	<$1 thous	Negligible OR within suburb, precinct, or small town	No noticeable harm – business as usual	1

Thus, the full-fledged NRA process, in accordance with the IMF Methodology, contains 7 stages and relies on the ability of the authorities to collect and submit statistical data, qualitative expert judgments, and use the collecting data tools from open Internet sources. The overall process is cyclical, based on the feedback from the participants of the working groups. The stages and objectives of each phase include:

1. **Preliminary stage and preparation of threat analysis:** Agree common research objectives, establish an NRA coordination mechanism, study the environment and threat indicators in the AML/CFT area, as well as fill out four questionnaires by the authorities (two on the available data and two on the national and cross-border ML/TF threats);
2. **ML/TF threat:** The IMF staff hold working meetings with the authorities to agree on the final reviews of the national and cross-border ML/TF threats, including estimates of the magnitude and nature of the national and cross-border flows of criminal proceeds;
3. **Preparation for vulnerability assessment:** The authorities prepare four templates for collection of statistical data (sector and firms profiles; international cooperation; criminal justice system; as well as FIUs and reporting) and three questionnaires (sectors and firms; FIUs and law enforcement agencies; criminal justice system). The IMF staff collect generally accessible vulnerability information and combine all vulnerability and threat information for a preliminary likelihood analysis, including at the sectoral level;
4. **ML/TF vulnerability and likelihood assessment** The IMF staff hold working meetings with the authorities to agree on the final opinions on the ML/TF vulnerability, including a list of major factors that increase and reduce likelihood. The results are combined with similar outcomes on the threat to achieve preliminary opinion on the overall likelihood of various ML/TF risk events, including sectoral risks.
5. **Consequences and overall risk assessment preparation:** the authorities fill in two questionnaires on the ML and TF consequences, the IMF staff collect publicly available information related to the ML/TF consequences, add all the information on the consequences to a preliminary consequence analysis, and combine it with the likelihood results for creating preliminary heat maps of risk events, including at the sectoral level.
6. **ML/TF consequences and risk analysis:** The IMF staff hold working meetings with the authorities to agree on the final opinions on the ML/TF consequences. The revised heat maps show the level of risk for each generic risk event; for the sectors that are presented in separate working groups, the general levels of risk and priorities for mitigation are discussed and agreed upon.
7. **Final stage:** the IMF staff provide a preliminary national risk assessment that is sent to the authorities for review and approval before being published.

The NRA methodology provides a number of standardized findings to help the authorities understand the ML/TF risks. This includes a table that assesses the national criminal proceeds by the crime category, summarizing the risk matrix of the main factors that increase and reduce risks, heat maps for risk events, sectors and enterprises, summary tables for sectors and enterprises, and a national risk assessment document:

a. **the summary table of the national criminal proceeds** shows the estimated level of proceeds generated and also adds up average assessments to provide an overall assessment of the amount of criminal proceeds generated in the country. The

median and overall scores are also reflected as a percentage of a country's GDP. This information may be supplemented with estimates related to the nature and source of proceeds in terms of the proportion of generation in cash, financial and physical assets, and related to domestic and transnational organized crime groups and other offenders.

b. **the final risk matrix** provides likelihood assessments for each analytical risk module and associated risk events and assessments of the consequences for these events. The matrix also establishes a list of key factors that increase and reduce risk assessment (i.e., strengths and weaknesses), thus providing authorities with detailed guidance on how to address individual factors to mitigate the major risks.
c. **heat maps** show the level of risk for all generic risk events and any additional events detected by the authorities, by referring to the likelihood levels and the consequences of each ML/TF occurrence. Heat maps are also created to show the ML/TF risk level for sectors and types of enterprises in the sector.
d. **the summary tables** for sectors and enterprises provide such information as: number of enterprises (reporting to RE); general and average RE assets; assessment of likelihood inherent in RE to be used in ML/TF transactions; assessment of adequacy of the AML/CFT controls and ML/TF net risk. The summary of the RE can be filtered to produce individual results, such as, for example, 10 companies with the highest probability of being used for cross-border ML or TF.
e. **The NRA document** describes, in sufficient detail, the main risks and their factors for the target audience, as well as the process used to reach such conclusions.

1.3.2. World Bank Methodology

The World Bank Group has developed an analytical risk assessment tool to guide countries in conducting their ML/TF risk assessment at the national level. The development of the World Bank Group's National Risk Assessment Tool ("tool") was commenced by the Financial Markets Integrity team in 2007 and incorporated the intellectual contributions of a wide range of experts, as well as experience in assisting many countries in performing their NRAs.

The tool comprises several Excel-based and interrelated modules that enable countries to assess their ML/TF threats and vulnerabilities. **"Threats"** here refer to the scale and characteristics of the proceeds of criminal activities or terrorist financing in the jurisdiction. **"Vulnerabilities"** refers to weaknesses or gaps in a jurisdiction's defenses against ML and TF. Threats or vulnerabilities may exist at the national or sector level, and all together determine the ML/TF risk level in a jurisdiction.

The objectives of the tool are the following:

- to guide jurisdictions in assessing their ML/TF risks, with a view to helping them use the information gained to design a more effective, risk-based AML/CFT regime;
- to contribute to capacity building in the country, not only for assessing the ML/TF risks but also for improving the data and information collection framework and practices;
- to raise awareness and trigger interaction and cooperation among the stakeholders from governments and the private sector.

Although the tool takes these factors into account, it is not aimed for:

- a quantitative estimate of the size of the illicit economy or financial flows in the country;
- assessing the risks of predicate crimes (drug trafficking risk, fraud risk, corruption risk, etc.);
- making cross-country comparisons of the ML/TF risks.

General Structure of the Tool

The tool consists of nine modules that make it possible to assess ML and TF risks. The tool is centered around seven modules that focus on the money laundering risk assessment. In addition, the tool includes a module to assess the risk of terrorist financing and another module to assess the risks of financial inclusion products.

National Vulnerability Module (Module 2) and the modules designed for the vulnerability assessment of various sectors (Modules 3 to 7) have a unique and relatively complex logic that utilizes weighted averages, built-in preconditions, and formulas. However, the modules for ML risk assessment, TF risk assessment and risk of financial institutions' products rely on relatively simple matrix based structures.

During the NRA process, the country establishes a national Working Group (WG) to undertake the risk assessment. This WG divides into several teams, each of which focuses on one of the modules. Table 1.8. presents the three main parts of the tool and lists the modules in each part.

Table 1.8. The National Risk Assessment Tool's Main Parts

ML risk assessment	TF risk assessment	Financial inclusion product risk assessment
Module 1 – Threat Assessment Module 2 – National Vulnerability Module 3 – Banking Sector Vulnerability Module 4 – Securities Sector Vulnerability Module 5 – Insurance Sector Vulnerability Module 6 – Other Financial Institutions' Vulnerability Module 7 – DNFBP Sectors Vulnerability	Module 8 – National TF Threat and Vulnerability	Module 9 – Financial inclusion product risk assessment

Fig. 1.4. (provided below) depicts the tool structure.

ML Risk Assessment (Modules 1-7)

The seven modules that help assessing the national money laundering risk are closely interrelated. Essentially, the overall national money laundering risk is determined by assessing: (1) the national threat of money laundering; and (2) the national vulnerability to money laundering.

ML Threat Assessment Module

The Threat Assessment Module helps determine the national money laundering "threat level", which ranges from "low" to "high" on a five-point scale. In the Threat Assessment Module, the Working Group identifies the main predicate offenses, origins and flows of criminal proceeds, and money laundering techniques and trends in a jurisdiction. The module also facilitates systematic collection of data on money laundering threats and analysis of cross-border money laundering threats. The higher the threat of money laundering, the higher the national money laundering risk is.

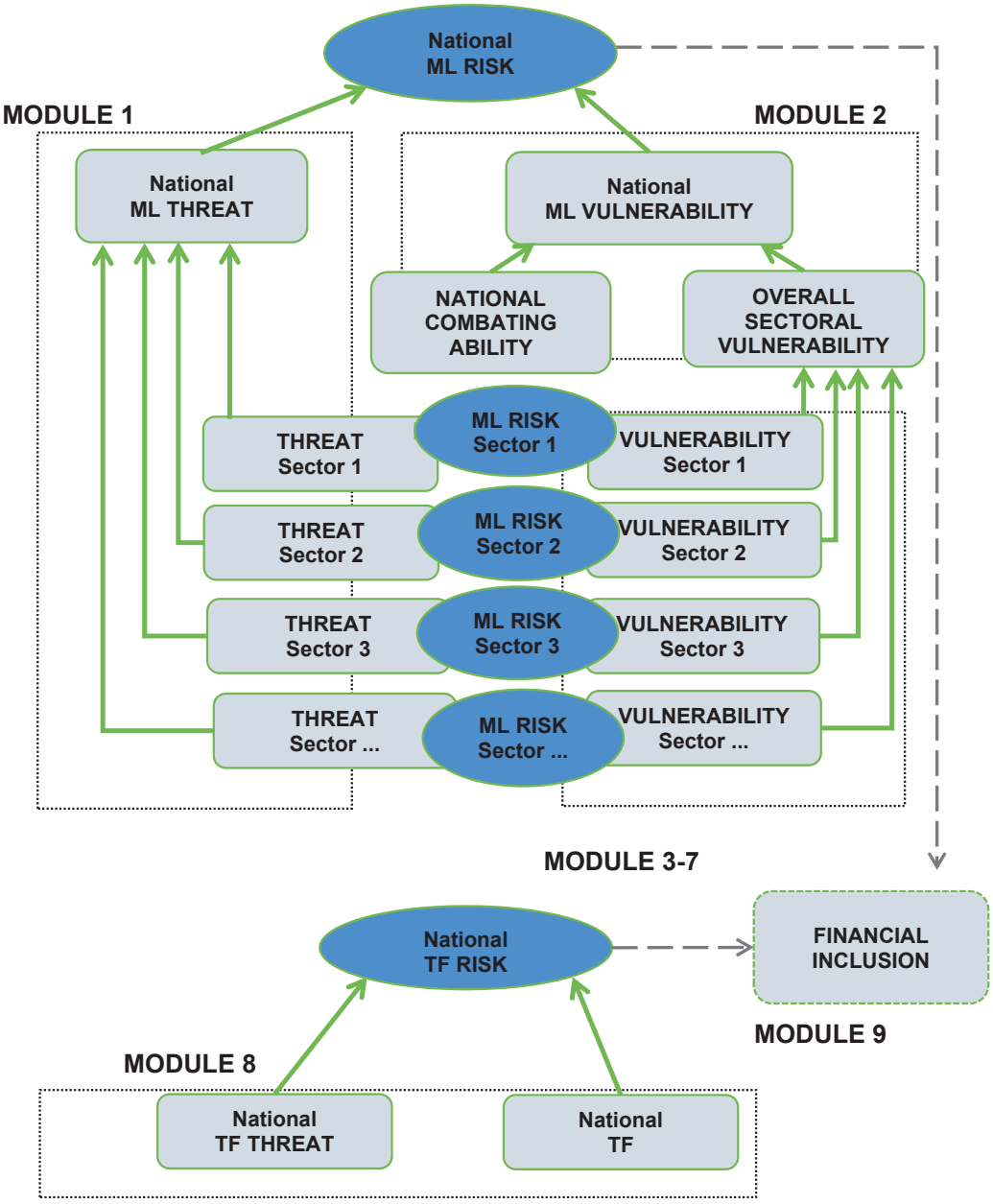


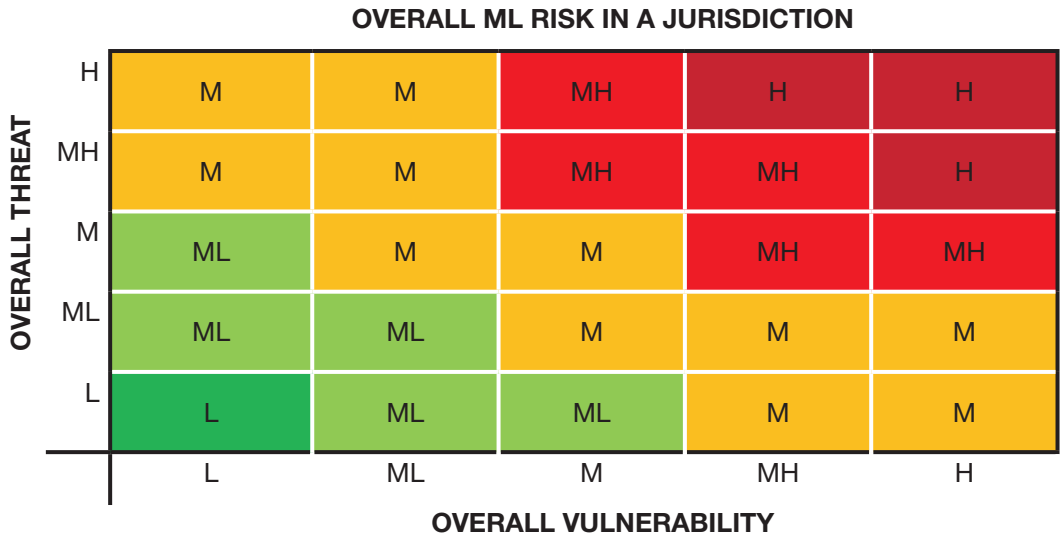
Fig. 1.4. NRA Tool Overall Structure

ML Vulnerability Assessment Modules

On the other side, the National Vulnerability assessment is based on the analysis of the national combating ability as well as the vulnerability of various sectors to money laundering. Combining the vulnerabilities of the relevant sectors and taking the deficiencies in national combating ability into account, the National Vulnerability Module yields a "vulnerability score" (which ranges from 0.0 to 1.0, and corresponds to one of five levels ranging from "low" to "high").

The overall money laundering risk level is set at a level where the results of the threat assessment and the vulnerability assessment intersect (see Fig. 1.7). For example, if the threat has been assessed as "medium" and the vulnerability has been assessed as "medium-high", the money laundering risk will be "medium high".

This means that although the threat level in the assessed jurisdiction is at a medium level, the overall money laundering risk is medium-high, given the higher vulnerability level (the weaknesses in the country's defense mechanisms). In Figure 1.5, overall risk levels have been color-coded, with low levels green, medium levels yellow, and high levels red.



Note: L = low; ML = medium-low; MH = medium-high; H = high.

Fig. 1.5. Overall ML risk in a jurisdiction

Performing assessment: a closer look at the National Vulnerability Module

To further demonstrate how the National Risk Assessment Tool works, the design of one of the modules – the National Vulnerability Module – is explained in more detail next.

The National Vulnerability Module provides a methodological process, based on an understanding of the causal relations among vulnerability factors (variables) relating to the regulatory, institutional, and economic environment in a jurisdiction. Fig. 1.6 shows the structure of the National Vulnerability Module.

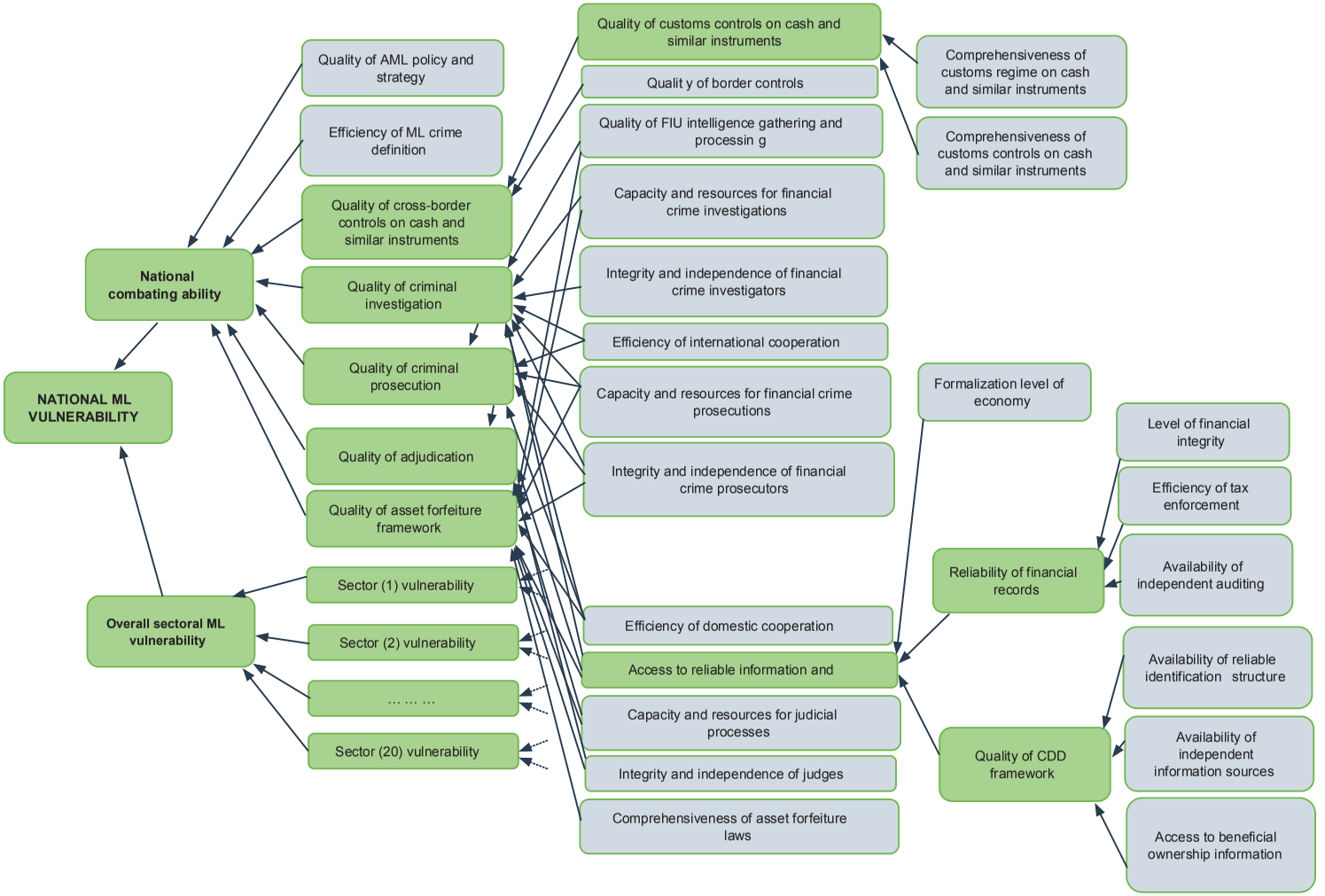


Fig. 1.6. ML Vulnerability Module structure

The overall National Vulnerability Module is composed of two major parts: the overall sectoral vulnerability, which is determined by the outcomes of the vulnerability assessments of the various sectors, and the national combating ability (ML prevention and combating). The national combating ability is a comprehensive assessment based on 22 input variables assessed by the WG. These variables attempt to capture the high level factors in a country such as the quality of the judicial processes, the effectiveness of the law enforcement, domestic and international cooperation. The ratings given to these input variables by the assessors, as well as the built-in assumptions and properties of the tool such as weights and pre-conditions all together generate an overall score for national combating ability. The tool also contains some intermediate variables, which are assessed by the tool automatically based on the entries for input variables. The relationship between the variables can be seen in Fig. 1.6, which captures the structure of the National Vulnerability Module. Colors are used to distinguish the input variables from the intermediate variables. The gray boxes are the input variables, and the green boxes are the intermediate variables.

Figure 1.7. (below) illustrates the structure through a partial snapshot of the lower section of the network diagram for the National Vulnerability Module. As an example of an input variable, consider Efficiency of Tax Enforcement (the second variable at the top of the column in Fig. 1.8). If a country's tax enforcement regime is efficient, this will naturally have a positive effect on the country's ability to combat ML. But this effect is indirect, as can be seen by tracing the various connections through the chart. Effective and efficient tax enforcement improves the reliability of financial records and books, which in turn helps trace the POC flow in ML cases. Availability of reliable financial and identification data will enable authorized agencies to have access to reliable information and evidence and thus achieve greater success in their criminal investigations. In this way, the Efficiency of Tax Enforcement can have a tangible effect on a country's ability to combat money laundering.

The Efficiency of Tax Enforcement is just one of three input variables combining to affect the reliability of the financial records and books in a country. Others are Level of Financial Integrity and Availability of Independent Auditing. By assessing all three of these input variables and combining the results in an intuitive and realistic way, a good impression of the Reliability of Financial Records/Books in the country can be determined. To do so, it is not necessary to perform a separate assessment of the intermediate variable Reliability of Financial Records and Books. This illustrates clearly the difference between input variables, which require input from the WG, and intermediate variables, which do not require such input, but are only an intermediate result of input variable assessment.

As an example, the following four steps explain the use of the National Vulnerability module to give a better idea on Part 1 of the NRA tool (ML risk assessment).

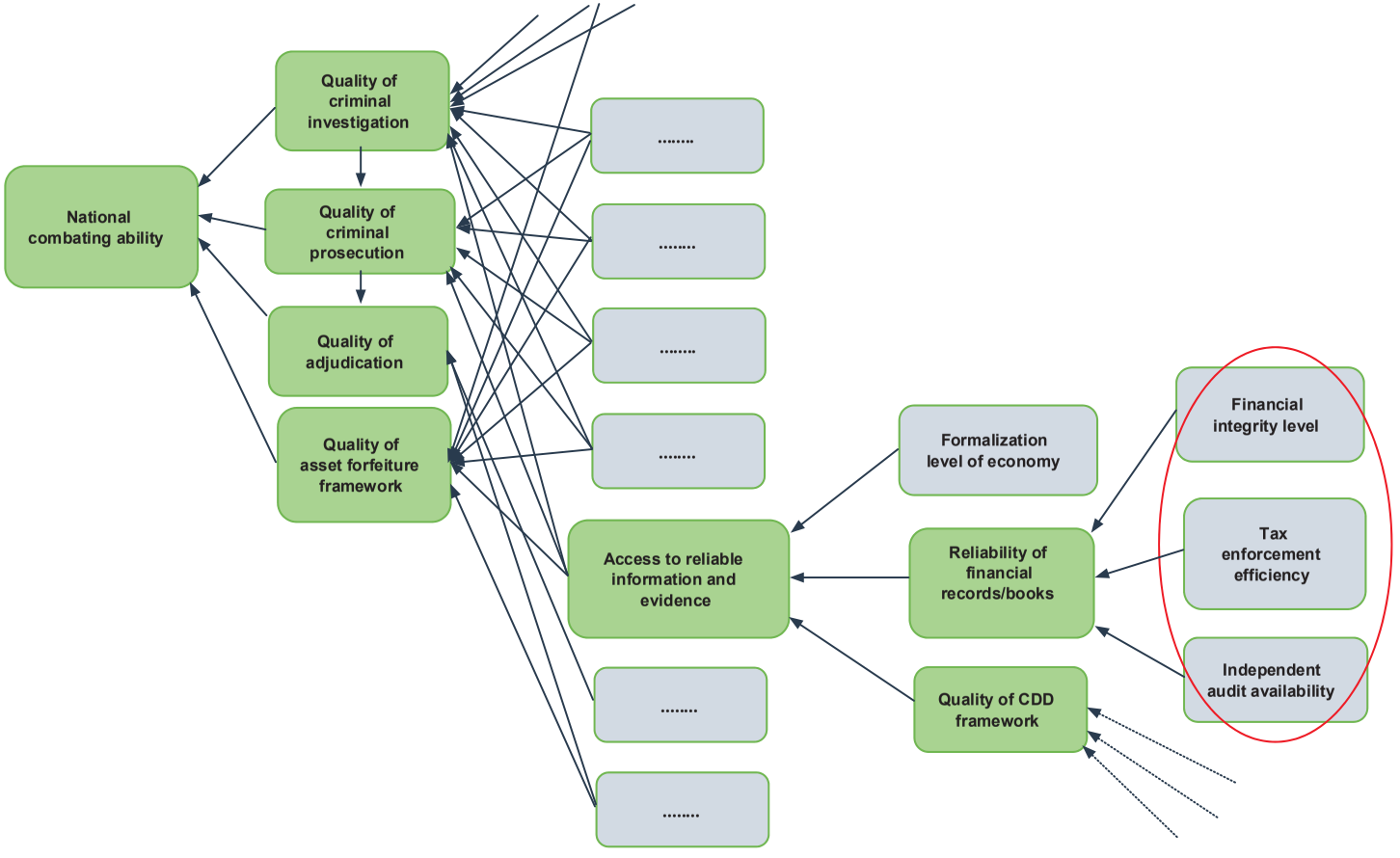


Fig. 1.7. Detailed structure of the national ML vulnerability assessment module (the essence of the input and intermediate variables)

Step 1. Assessing the input variables in the National Vulnerability Module

The WG assesses the input variables using the guidance manual that is part of the NRA Tool package. A separate guidance manual document has been prepared for each module. The guidance manual explains the objective of assessing the variable, provides criteria that can be used to perform the assessment, and suggests information sources that may help to underpin the assessment rating. After considering the assessment criteria, the WG needs to assign a score that ranges from 0.0 to 1.0. For example, a rating of 0.3 corresponds to a low level. Table 1.9. presents an excerpt from the guidance manual for Module 2 – National Vulnerability to assess the efficiency of domestic cooperation.

Table 1.9.Domestic cooperation efficiency assessment criterion

Variable Description
This variable assesses whether, when required, the country's relevant AML agencies cooperate efficiently and coordinate domestically with each other to combat money laundering.
Assessment criterion
Relevant AML agencies involved in combating money laundering, are able to cooperate and coordinate effectively if: • The FIU, intelligence services, investigators of financial crime, asset forfeiture investigators, regulators, customs and tax authorities and, when appropriate, the prosecutors of financial crimes, meet regularly to share information and discuss joint initiatives, especially when they have joint committees and structures that meet regularly to exchange intelligence and information. • There is a legal framework that allows for joint investigations by relevant investigative units and such investigations are undertaken, where required. • There is efficient cooperation between relevant AML agencies and reporting entities. • There is a fully functional interagency cooperation committee or similar high-level committee in the AML area, such as the National AML/CFT Coordination Committee.
Possible sources of information and data
• Experience of relevant domestic AML agencies. • Information on any operational coordination and cooperation issues among law enforcement, FIU, prosecutors, judicial authorities and supervisory agencies. • Information on cooperation between relevant AML agencies and reporting institutions. • Information on an interagency cooperation committee or similar high-level committee in the AML area, such as the National AML/CFT Coordination Committee. Which agencies are represented on this committee? How often does this committee meet? How effectively does it work? What have been the outcomes of the committee's activities so far? • How many joint investigations have been conducted so far? Please provide details.
Assessment
• Based on the assessment criteria and the information/data collected, the following rating was assigned for this variable.

Excellent	Close to Excellent	Very High	High	Medium High	Medium	Medium Low	Low	Very Low	Close to Nothing	Does not Exist
1.0 ☐	0.9 ☐	0.8 ☐	0.7 ☐	0.6 ☐	0.5 ☐	0.4 ☐	0.3 ☐	0.2 ☐	0.1 ☐	0.0 ☐

It is important that the NRA Tool is used as part of a process that includes a broad range of stakeholders. A key element in the assessment is the discussion that takes place during assessment of the variable. Once a rating of a variable has been decided on, the WG is advised to record the discussion, grounds, and documentary sources for the assigned rating. This is crucial, as the process needs to capture the available data and statistics supporting the assessment. The record made at the time will contribute to the assessment report that countries are advised to draft as a result of the NRA tool process. A Worksheet for Records has been included in the Guidance Manual to help WG structure their documentation.

Step 2. Making entries in the National Vulnerability Excel File

Once the assessment for each of the 22 input variables has been established and the ratings for all the variables have been determined, the assessment results can be inserted into the Excel file of the NRA Tool. Each module has its own Excel file.

Once a rating has been inserted, the entry will be automatically color-coded to show how the rating will affect the national ML vulnerability. High ratings that relate to the combating ability have a positive effect on the national vulnerability and will appear in green.

The vulnerability ratings for the different sectors (banking, securities, insurance, remittance, lawyers etc.) also need to be inserted into the National Vulnerability Excel file (see Fig. 1.8). For these ratings, it should be noted that a higher vulnerability rating of a sector negatively impacts the overall national vulnerability outcome. The WG assigns a weight to the sector, depending on its importance in the country's economy, which also affects the sector vulnerability scores.

Fig. 1.9 shows the ratings inserted for the first year or scenario in the Excel file for the National Vulnerability Module. The NRA Tool is designed to accommodate entries for up to 10 years or 10 different scenarios, which allow for entries from different assessment years as well as for scenario analysis.

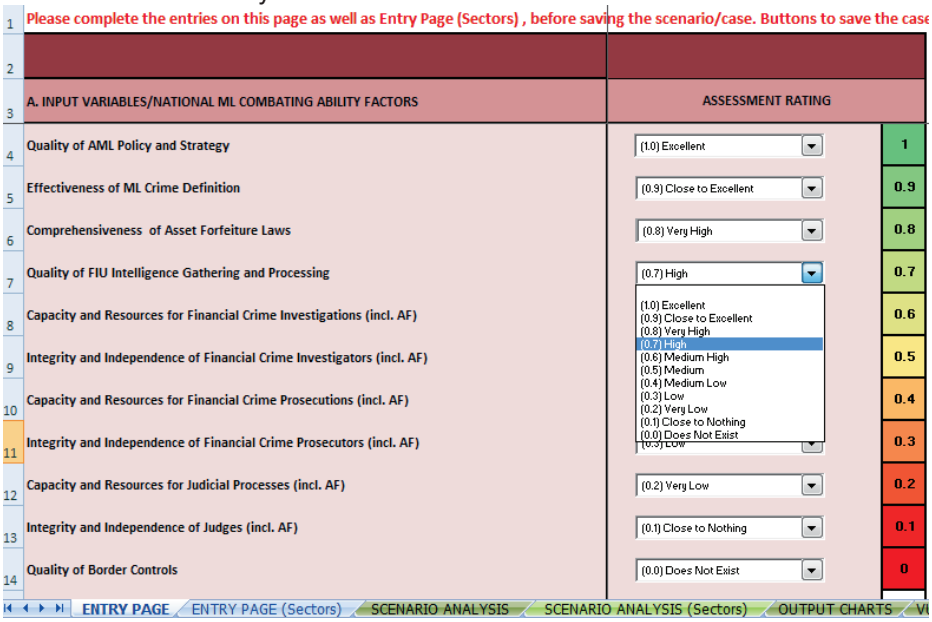


Fig. 1.8. Entering ratings for the input variables in the Excel file

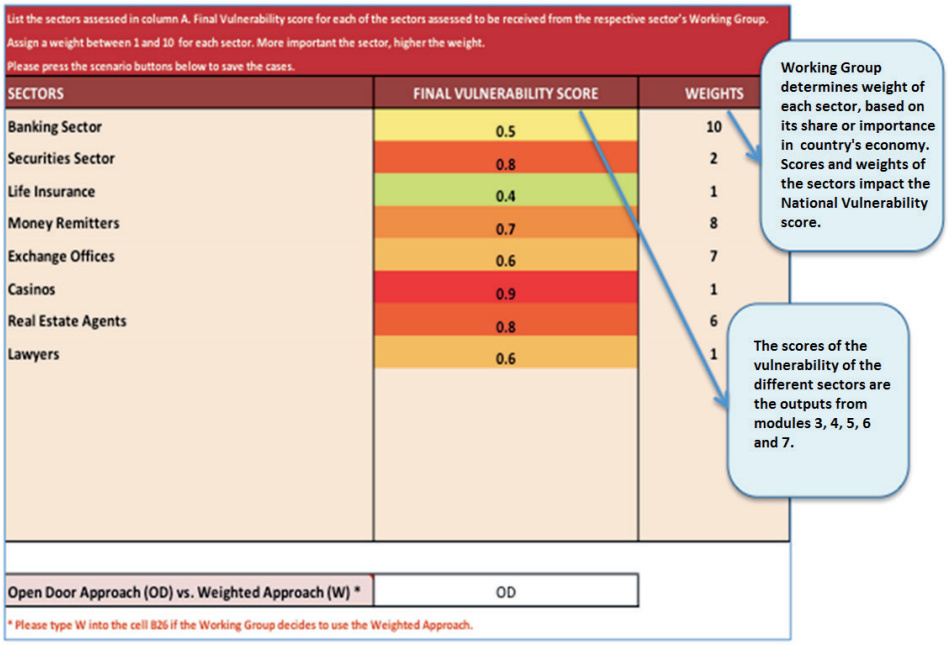


Fig. 1.9. The vulnerability scores of the different sectors affect the rating of the national vulnerability

Step 3. Determining the outcome of the National Vulnerability Assessment

Once the ratings for all the input variables have been entered, the tool calculates the ratings for the intermediate variables (such as Quality of AML Policy and Strategy, Quality of Criminal Investigation, or Quality of Criminal Prosecution), based on the assessment ratings of the input variables, network structure, weighted averages, and defined conditions.

Then a similar calculation takes place, generating a score for the National Combating Ability. This is then combined with the outcomes of the vulnerability assessments of various sector modules to arrive at the final National Vulnerability level, as shown in Fig. 1.10.

The outcomes of the assessment are presented in two output pages. One output page presents bar charts indicating the levels of national vulnerability and other main assessment outputs, and allows for a comparison of the assessment results for 10 years (or 10 different scenarios) (see Fig. 1.10). The other output page contains a Vulnerability Map, which provides a quick visual summary of the assessment results (see Fig. 1.11). This color-coded map highlights the level of vulnerabilities resulting from the various components of the anti-money laundering environment and illustrates the linkages between the various nodes.

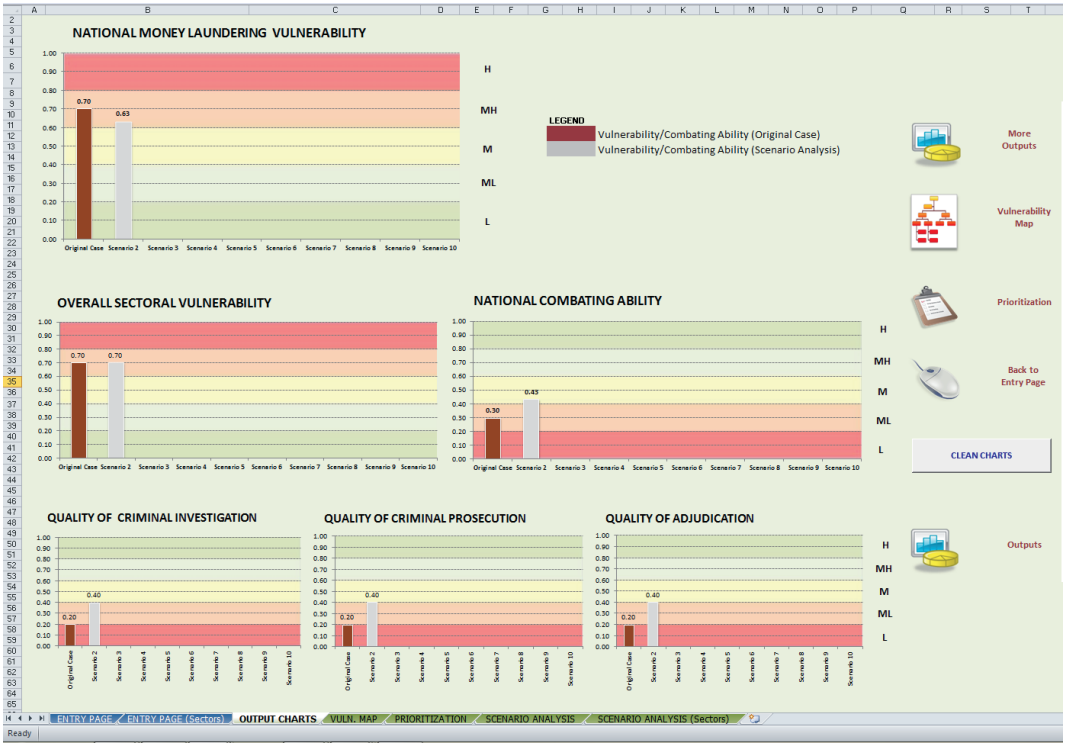


Fig. 1.10. Example of the assessment outputs for the national ML vulnerability

Step 4. Prioritizing/sequencing potential actions and designing the action plan

NRA tool generates a priority ranking to help guide relevant authorities to prioritize actions to strengthen the national ML combating ability factors and AML controls in the country. This helps the relevant authorities in deciding on what needs to be done first to improve the national combating ability. Fig. 1.12 shows such priority rankings.

The lower the ranking a variable receives, the higher the priority should be to improve in that area. In other words, if a variable is given a ranking of 1 (which also has the darkest red color), the associated item needs to be addressed first to improve the country's vulnerability to ML. The ranking is calculated by the formulas in the Excel file, which in turn are based on the potential impact of each item on national vulnerability (taking into account the current state of the item). As an example, in the screenshot from the tool shown in Fig. 1.12, the variable Quality of AML Policy and Strategy has the highest priority for improving national combating ability.

Priority rankings do not necessarily correspond to the assessment ratings assigned to variables during the assessment process. A variable that receives a more favorable rating than other input variables may still end up having a higher priority and therefore require more attention. This is because the rating assigned by the WG, though essential, is not the only determinant of the national vulnerability level and the priority ranking. Other factors, such as the network structure with its input (primary) and intermediate (derivative) variables will also influence the ultimate vulnerability level and priority rankings. As mentioned, these factors can be viewed by the WG.

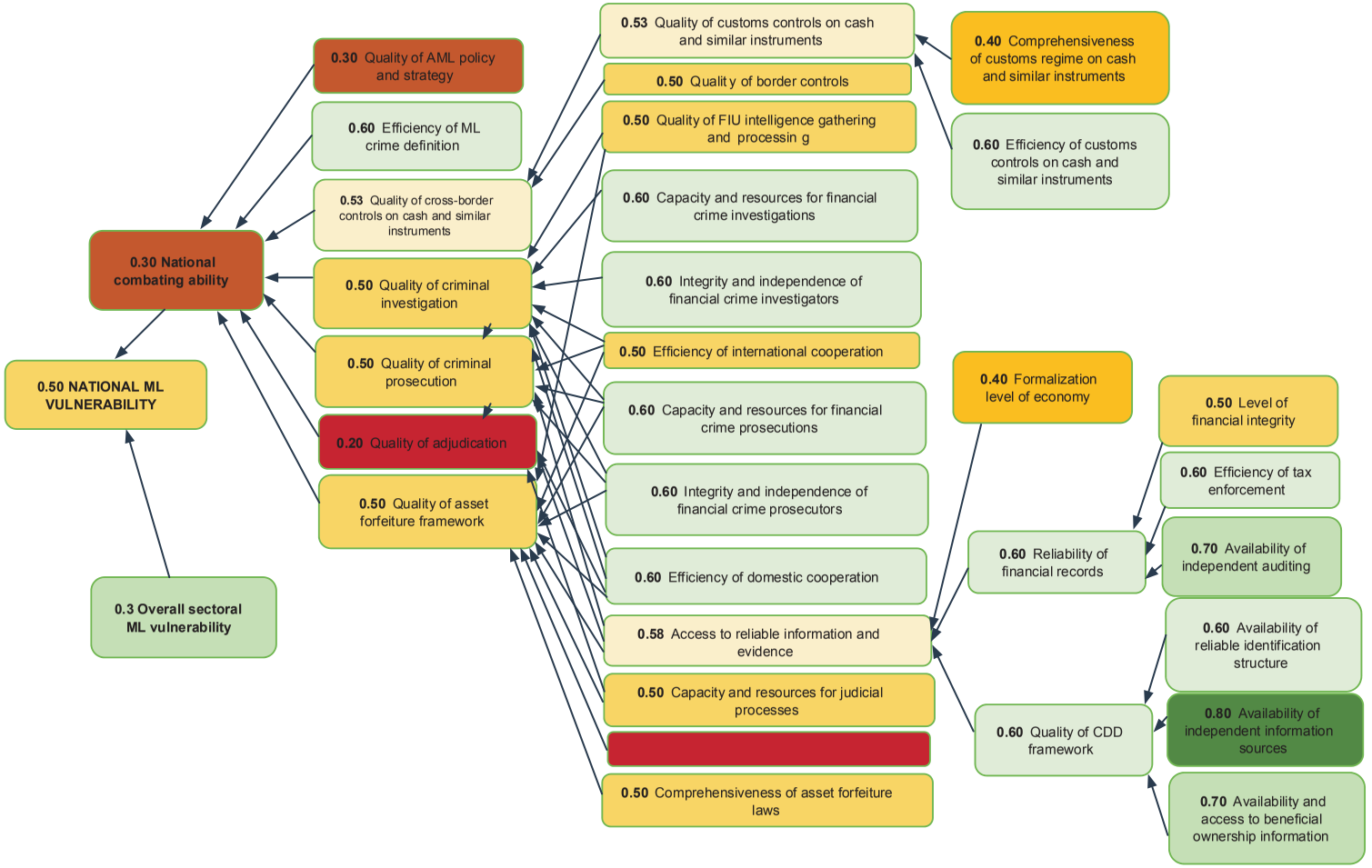


Fig. 1.11. Example of the National Vulnerability Map

	A	D
81	PRIORITY RANKING FOR INPUT VARIABLES/NATIONAL ML COMBATING ABILITY FACTORS - LAST CASE/SCENARIO*	PRIORITY RANKING**
82	Quality of AML Policy and Strategy	1
83	Effectiveness of ML Crime Definition	2
84	Comprehensiveness of Asset Forfeiture Laws	10
85	Quality of FIU Intelligence Gathering and Processing	11
86	Capacity and Resources for Financial Crime Investigations (incl. AF)	3
87	Integrity and Independence of Financial Crime Investigators (incl. AF)	5
88	Capacity and Resources for Financial Crime Prosecutions (incl. AF)	6
89	Integrity and Independence of Financial Crime Prosecutors (incl. AF)	7
90	Capacity and Resources for Judicial Processes (incl. AF)	8
91	Integrity and Independence of Judges (incl. AF)	4
92	Quality of Border Controls	18
93	Comprehensiveness of Customs Regime on Cash and Similar Instruments	17
94	Effectiveness of Customs Controls on Cash and Similar Instruments	15
95	Effectiveness of Domestic Cooperation	14
96	Effectiveness of International Cooperation	12
97	Formalization Level of Economy	9
98	Level of Financial Integrity	19
99	Effectiveness of Tax Enforcement	16
100	Availability of Independent Audit	
101	Availability of Reliable Identification Infrastructure	13
102	Availability of Independent Information Sources	
103	Availability and Access to Beneficial Ownership Information	
104		
105		

ENTRY PAGE | ENTRY PAGE (Sectors) | OUTPUT CHARTS | VULN. MAP | PRIORITIZATION | SCENARIO ANALYSIS | SCENARIO

Fig. 1.12. Example of priority rankings for the National Vulnerability Module

TF Risk Assessment Module (Module 8)

The TF Risk Assessment Module largely follows the same logic as the ML Assessment Modules in terms of performing an intuitive and methodical analysis. The structure of the module is shown in Fig. 1.13.

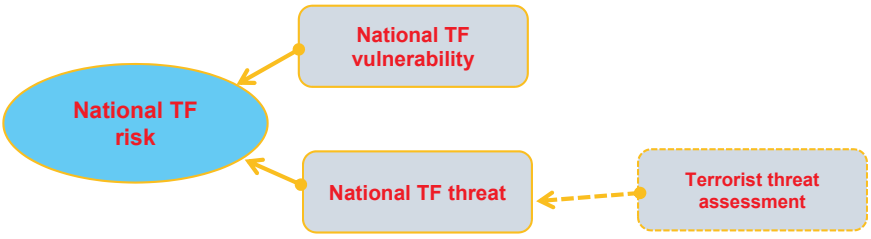


Fig. 1.13. Structure of the TF Risk Assessment Module

The module consists of three areas of analysis, as follows:

1. First, the level of the terrorist threat for the jurisdiction is assessed through review of quantitative and qualitative information on terrorist acts in a jurisdiction, such as enforcement data, intelligence sources, and terrorism research. The rationale for

this assessment is that the level of the terrorist threat impacts the TF level. It should be emphasized that this is not the focus of the module.

2. Second, the direction of transfer of terrorist financing funds, as well as their sources and channels, are analyzed:
   a. *Directions.* By determining the direction of the funds, the WG assesses whether funds are generated in the home jurisdiction but used for terrorist operations elsewhere, or the other way around. Another possibility is that funds simply pass through a jurisdiction;
   b. *Sources.* The assessment then turns to the TF sources. Financing may come from legitimate sources (such as nonprofit organizations, or import/export businesses) or from criminal activities (such as natural resource theft or drug trafficking).
   c. *Channels.* Subsequently, the WG should examine which channels are being used to transfer terrorist funds. In addition to using enforcement and intelligence data, an estimate must be made of undetected terrorist funds, based on qualitative indicators.
3. The last part of the module supports the assessment of the strength of a jurisdiction's defense mechanisms: the controls that have been adopted to detect and counter TF.

Based on the analysis in the module, the WG must then make an overall assessment of the TF risk in a jurisdiction.

Financial Inclusion Product Risk Assessment Module (Module 9)

The Financial Inclusion Product Risk Assessment Module aims to assist national authorities by providing a logical, user-friendly framework for evaluating the ML and TF risk in their jurisdiction that arise from financial inclusion products (current, new, or emerging). The module can also be used by regulators to design financial products or features with low ML/TF risk, or to assess whether an existing financial product can be classified as low-risk. The general structure of the module is shown in Fig. 1.14.

In the first section of the Tool, regulators answer key questions about the specific product features of the financial inclusion product. In the second section, regulators answer key questions about the overall ML and TF risk environment in the country, taking into account the potential threats of ML/TF in the country and the associated control measures in place for financial inclusion products. Given the inputs received by authorities from these two sections, the third section provides authorities with the initial ML/TF risk level regarding each specific product feature. Following this risk assessment, the tool offers guidance questions to authorities on how they can mitigate any potential high risks.

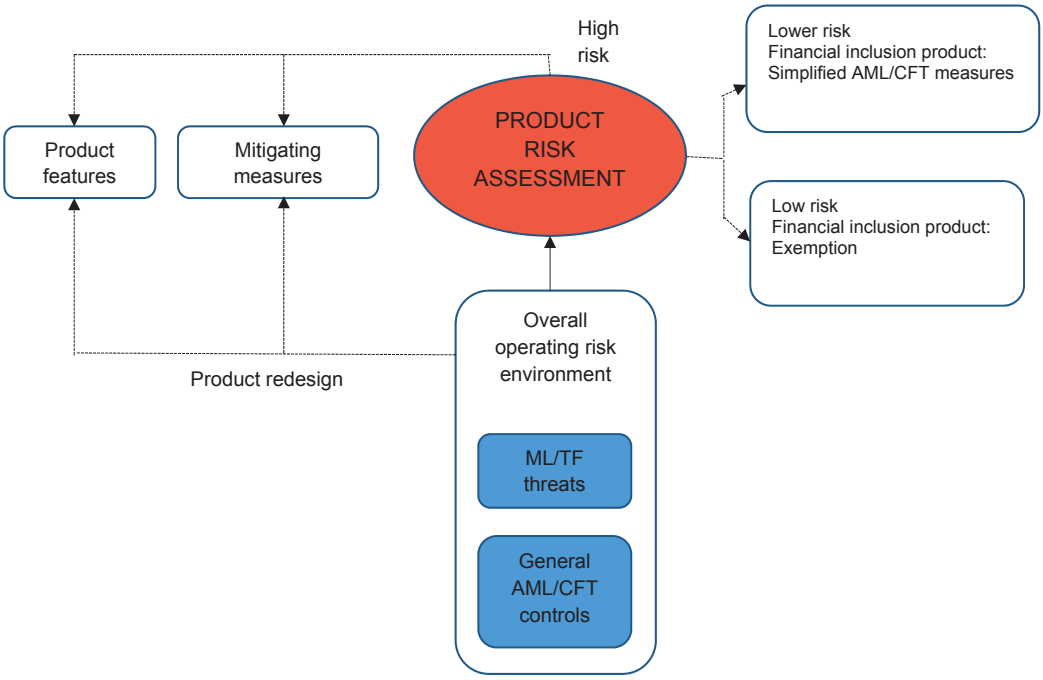


Fig. 1.14. Structure of the Financial Inclusion Product Risk Assessment

The process of assessing the risk posed by financial inclusion products suggested by the tool is not a static one. Rather, it is a dynamic process by which product features and mitigation measures can be fine-tuned, depending on the outcome of the risk assessment.

The structure of the Financial Inclusion Product Risk Assessment Module is different from the rest of the NRA Tool modules. The assessment in this module utilizes the findings and assessments of other modules, rather than feeding into the NRA. Financial inclusion products also need to be assessed separately in the relevant sectoral modules in order to capture their impact on national vulnerability.

1.3.3. Risk Assessment Methodology at the EU Level

A risk means the ability of a threat to exploit the vulnerability of a sector for the purpose of ML or TF. A risk falls within the scope of the supranational assessment as soon as it affects the internal market because of its characteristics – whatever the number of MS concerned (i.e. even if it may concern only one Member State). The scope covers both known risks and those that did not materialize before.

FATF recommends that countries shall consider the capacity and AML/CFT experience of each sector when they decide to conduct NRA. ML and TF risks shall be identified, assessed and understood, and measures to prevent ML/TF shall be commensurate with the risks identified.

On the basis of these recommendations, Directive (EU) 2015/849 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing" recognizes the importance of a supranational approach to risk identification. It tasks the Commission to conduct the review of specific risks that could arise at the European level and could affect the internal market ("supranational risk"). The Commission shall therefore conduct such Supranational Risk Assessment on ML and TF (SNRA).

A risk identification is also conducted at the national level by each Member State so that to ensure proper risk identification and risk mitigation of national specific risks. A third layer of risk identification is provided by sectors themselves, taking into account risk factors including those relating to their clients, countries, products, services, transactions or delivery channels.

These three layers of risk assessments (and where appropriate risk mitigation) allow building a comprehensive awareness and analysis of the ML/TF risks in the European Union. These are complementary and have the same level of relevance as regards, respectively, the sectorial, national and supranational approach to risk assessment.

Even though national and sectorial risk assessments, among other sources, may prove to be essential building blocks for the SNRA conducted by the Commission, it cannot be considered as a mere compilation of these ones. The SNRA exercise shall therefore be understood as a separate work stream. This is a pre-requisite for an efficient exercise consistent with the mandate of Directive (EU) 2015/849, especially when the Commission will make recommendations to Member States on the measures suitable for addressing the identified European ML/TF risks. **In carrying out the NRA, Member States shall also make use of the findings of the SNRA report.**

The **aim of SNRA** is to define methodological guidelines, governance, working arrangements and road map in order to support the conduct of the risk assessment and the interactions with relevant stakeholders in terms of inputs, expertise and advice.

The objective and scope of the risk assessment is defined in Article 6 of Directive (EU) 2015/849.

The "evaluation" of the identified and assessed risks (outcomes of the risk assessment) is out of the scope of these methodological guidelines and shall be considered within the framework of the overall risk management process leading to the identification of mitigation measures to fill the identified residual risks.

Roles and Responsibilities on EU Supranational Risk Assessment

Role of the Commission

Following the mandate given by Article 6 of Directive (EU) 2015/849, the Commission is responsible for drawing up the SNRA report and for defining the mitigating measures.

The Commission will conduct the assessment by:

- organizing the work at European level and involving the appropriate experts;
- making the joint opinions of the European Supervisory Authorities (ESAs) as well as the SNRA report available to the Member States and obliged entities;
- defining the mitigating measures, making recommendations to Member States on the measures suitable for addressing the identified risks.

In that context, though the Commission will rely on the expertise of several stakeholders, it will have a decisional power to validate the outcomes of the SNRA discussions.

An Inter-service Group of the Commission will act as a steering group for this exercise.

Role of the Ad Hoc Working Group

In order to define a risk assessment methodology, an Ad Hoc Working Group (ADHWG) composed of volunteers from Member States was set up in February 2014. The role of the ADHWG is to support the development of the methodology for carrying out the identification, assessment and evaluation of the supranational ML/TF risks as provided for in Directive (EU) 2015/849. The ADHWG will follow the approach defined by FATF in its "Guidance on National Money Laundering and Terrorist Financing Risk Assessment" published in February 2013. Following the finalization of the methodology, the ADHWG will be consulted on methodological implementation issues and changes in case of need.

Role of other stakeholders

During each step of the NRA process, the Commission will involve the relevant experts from Member States[24] and European bodies as defined in the Directive. Where appropriate, the Commission will also involve representatives from the private sector, NGOs or academics in the process. Input and relevant information could be requested to the following stakeholders through ad hoc processes (public consultation, questionnaires, preparation of background papers, bilateral meetings, etc.).

Expert Group on ML and TF (EGMLTF): EGMLTF is a permanent Commission expert group composed of national administrations with the mandate of assisting the Commission, e.g. in preparation of the policy definition and providing expertise to the Commission when preparing implementing measures. EGMLTF has the capacity to draw on expertise available nationally.

⇨ EGMLTF may provide data relating to national risk assessments and more generally information on risks, threats and vulnerabilities. The role of EGMLTF in regard of the SNRA is also to appoint national experts for the different workshops.

European Supervisory Authorities (ESAs): the ESAs (European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority) are tasked under Article 6(5) of Directive (EU) 2015/849 with the responsibility of

24 Throughout this document, indications about the composition of the Member States experts groups designated to conduct the risk identification and risk assessment are provided for sake of information. However, the appointment of the most relevant experts is left to the appreciation of each Member State by considering the specific expertise required for each dedicated phase of the risk identification and assessment. It may include representatives of supervisory authorities, financial intelligence units, customs, gambling sectors, ministerial authorities, law enforcement, etc.

issuing a joint opinion on the ML/TF risks affecting the Union's financial sector.

Considering the key role the ESAs play in the identification of risks related to the financial sector, they participate directly in the discussions held within the ADHWG. In addition, regular contacts are organized between the Commission services responsible for the SNRA and the working group of the ESAs in charge of the joint opinion.

- ⇨ ESAs may provide data relating to distinctive features of ML/TF risks from a supervisory perspective, ML risks associated with the financial sectors' systems and controls, taking into account the various typical sectorial business models, strategies and cultures.

Other financial supervisory authorities not represented in the ESAs: considering the wide range of actors responsible for financial supervision, contacts will be held with other supervisory authorities not represented in the ESAs.

EU Financial Intelligence Units (EU FIUs): FIUs cooperate at the EU level through a group called the FIU Platform whose main task is to facilitate cooperation among the EU FIUs. The work of the FIU Platform and the EGMLTF should be closely coordinated.

- ⇨ The FIU Platform may provide data relating to national risk assessments, distinctive features of ML/TF risks from an FIU perspective (annual reports), aggregated data on suspicious transactions reports.

Sectorial specific expert groups: the Commission manages a number of groups of Member State experts covering the different sectors exposed to the ML/TF risks. Those networks may provide useful information and data regarding their respective sectors.

- ⇨ Such experts group may be consulted especially for preparing the assessment of the sectors' vulnerability.

Europol: Europol is an EU agency which supports law enforcement authorities by gathering, analyzing and disseminating information.

- ⇨ Europol may provide data relating to organized crime threat assessments (e.g. "organized crime threat assessment report" which includes analysis of ML threats). It may also provide analyses and intelligence work on AML/CFT from a law enforcement perspective.

Eurostat: Eurostat is a Directorate General of the European Commission which provides statistics at European level that enable comparisons between countries and regions.

- ⇨ Eurostat may provide data relating to series of indicators for the different stages of the AML chain, from the filing of a suspicious transaction report through to conviction (ML report 2013). It may also provide statistical data on economy, sectors and products.

FATF and FATF-Style Regional Bodies (FSRB): FATF is an inter-governmental body which sets standards and promotes effective implementation of legal, regulatory and operational measures for combating ML, TF and other related threats to the integrity of the international financial system. FSRBs have been established for the purpose of disseminating FATF Recommendations throughout the world. The main task of the FSRBs is to devise systems for combating ML/TF risks in their respective regions.

- ⇨ The FATF and FSRBs conduct evaluations of the AML/CFT systems of the Member States and are developing studies of typologies – the most common schemes used by criminals for ML/TF – that will provide useful information to feed the SNRA.

Other relevant stakeholders: such as Non-Governmental Organizations (NGOs), private sector representative bodies at the European level (DNBPs, financial sectors etc.) and other public or private sector organizations may also provide useful information.

The conceptual framework for the SNRA methodology is shown in Fig. 1.15.

Because of their specific features, FT and ML risks will be considered and assessed within two separate work streams.

The proposed methodology is based on the following consecutive actions:

1. The identification of ML and TF mechanisms that could constitute ML/TF risks at EU level. These are intended as ML/TF mechanisms going beyond the specificities of national jurisdictions, whether they arise in one or several Member States and which may represent a risk from an internal market perspective.

2. Threat assessment is a clear approach to assessment by sectors and scenarios in all sectors mentioned in Art. 2 and 4 of Directive (EU) 2015/849. In this specific application, the assessment focuses on the estimated intent and capability of criminals to exploit existing or innovative mechanisms for ML and TF. The assessment will be based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available intelligence (qualitative and quantitative inputs) and in light of the agreed approach to threat assessment (clearing house threat assessment reconciliation method). The Commission, which will have a decisional power to validate the outcomes of the SNRA discussions, will assess the strategic level of threat to be respectively:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

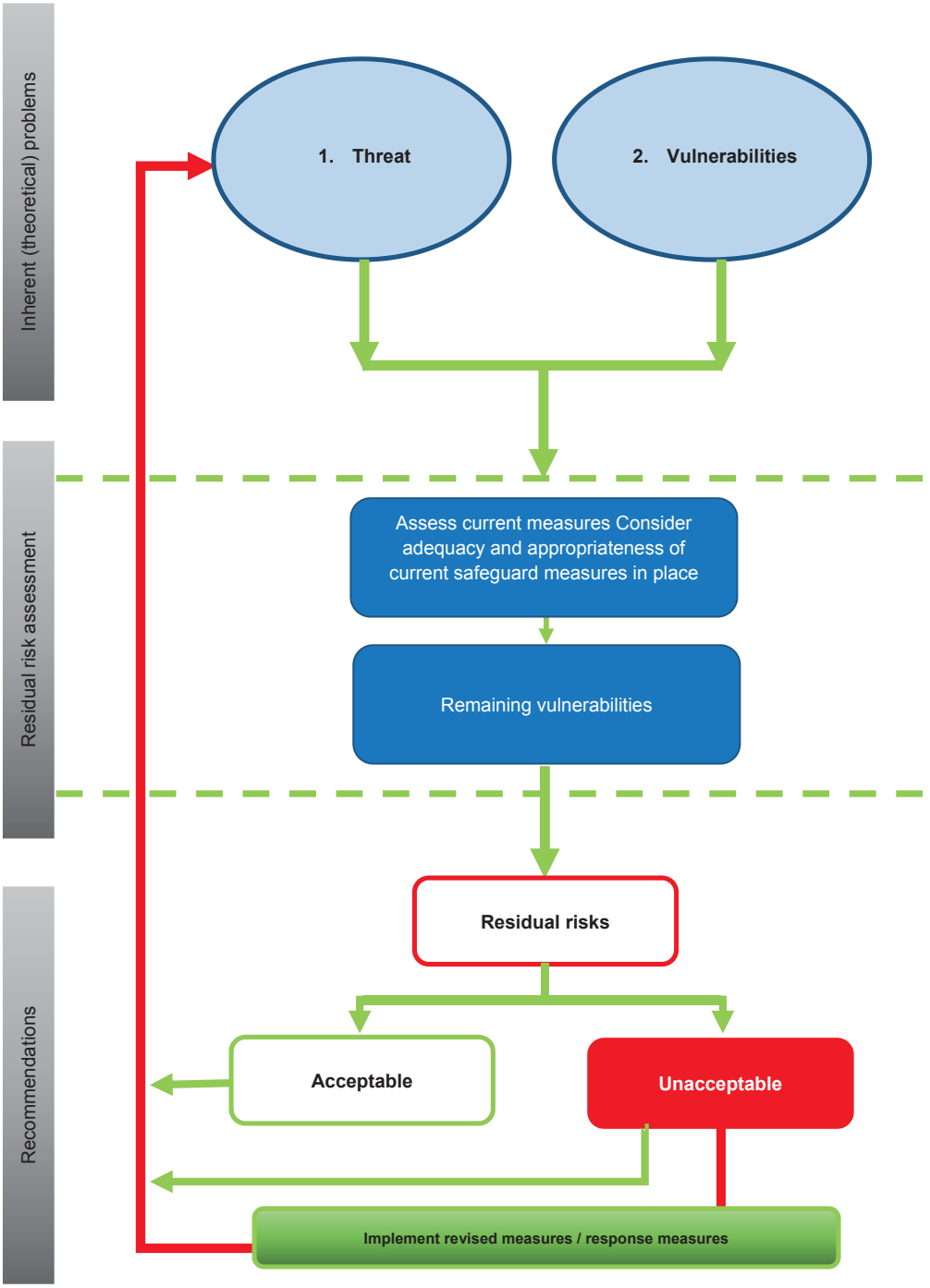


Fig. 1.15. Conceptual structure of the SNRA methodology

3. Assessment of the vulnerability level – by sector to ML/TF mechanisms. The vulnerability assessment will focus on the assessment of the existing safeguards in place. Based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available intelligence (qualitative and quantitative inputs) and in light of the agreed approach to vulnerability assessment (clearing house vulnerability assessment reconciliation method), the Commission, which will have a decisional power to validate the outcomes of the SNRA discussions, will assess the strategic level of vulnerability to be respectively:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

4. Determination of the residual risk on the basis of interplay of estimated threats and vulnerabilities for each type of ML/TF modus operandi. The assessment will be built on a risk based assessment by sector. For each sector considered a set of pre-defined ML/TF mechanisms will be assessed in terms of risk as combination of the identified level of threat and vulnerability.

For the purpose of the first SNRA round, the "impact/consequences" component was regarded as constantly significant and therefore was not assessed.

The proposed methodology consequently only looks at the threats and vulnerability components. While it is important to understand the consequences associated with the ML/TF activities, from a methodological point of view it is particularly challenging to measure their consequences in quantifiable or numerical terms. For the purpose of this risk assessment it is therefore assumed that ML/TF activities generate constant significant negative effects on the transparency, good governance and the accountability of public and private EU institutions, cause significant damage to EU countries national security and have both direct and indirect impact on the EU economy. From a methodological point of view, as the impact/consequences component is assumed to be a fixed high value for the specific purpose of this risk assessment, the residual risk for each scenario will be determined by a combination of the identified level of threat and vulnerability.

SNRA process description

The process can be summarized by the following steps:

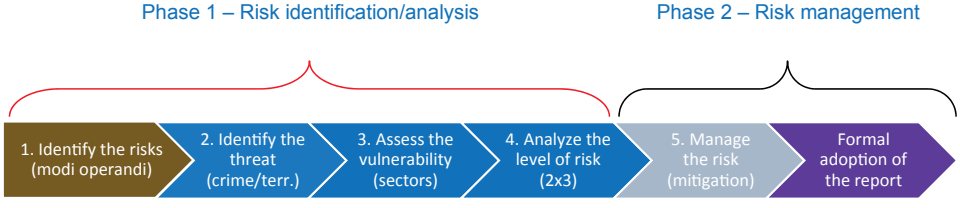


Fig. 1.16. SRNA implementation stages

The roadmap for Stage 1 "risk identification/analysis" foresees the following consecutive actions:

Step 1: risk identification.

The first step consists in identifying the exact scope in terms of ML/TF risks to be assessed at a later stage of the risk assessment process. For the specific purpose of the SNRA as defined in Directive (EU) 2015/849, risks identification should be intended as defining a list of known or suspected ML/TF threats along with the related sectors exploited by criminals to successfully perpetrate ML and/or TF activities. The risk of ML and TF is not the same in every case. Accordingly, a holistic risk-based approach should be used. While the risks identification process will rely largely on known threats, it is important to give due consideration to innovative or emerging threats for which it is reasonable to assume a lack of consolidated safeguards in place. At this stage, the objective is to identify the nature of the risks scenarios and those which are the most relevant considering the scope of the risk assessment. At this stage, the level of risks identified is not assessed.

Step 2: threat component

This second step consists in assessing the level of threat (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the scenarios identified in Step 1[25]. The assessment will be based on the estimated combined assessment of intent and capability of criminals to change or transfer illegitimate or legitimate funds (in the case of TF). The assessment of the threat level for each identified risk should lead to a threat assessment level common to the EU as a whole. At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method. The Commission will validate the outcomes of the threat assessment clearing house reconciliation method[26].

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat[27]) successful or foiled, and the perceived attractiveness of ML/TF through a specific mechanism. While the broad intent to ML/TF is assessed as being constantly high, intent to use specific ML/TF modus operandi differs depending on the attractiveness and the known existence of AML/CFT safeguards.

The "capability" component of the threat is understood as the capability of criminals to successfully change or transfer the ML proceeds of crime and to successfully transfer illegitimate or legitimate funds to financially maintaining a terrorist network. The assessment of the capability component will consider the ease of using a specific ML/TF modus operandi for (technical expertise and support required), the accessibility and relative costs of using a specific modus operandi.

25 The threat and vulnerability assessment is built around a four scale rating. Different rating can be considered but this latter presents the advantage (compared to a two or three scale rating) to capture better qualitative differences between different risks. The resulting risk level is also based on a four scale rating.

26 The clearing house reconciliation method has proven its efficacy in the framework of several EU risk assessments in the field of aviation security. For those risk assessments requiring a common EU position, which is the case for the supranational ML/TF risk assessment, the clearing house reconciliation method has proved its efficacy in providing the necessary working arrangements facilitating the achievement of a common position.

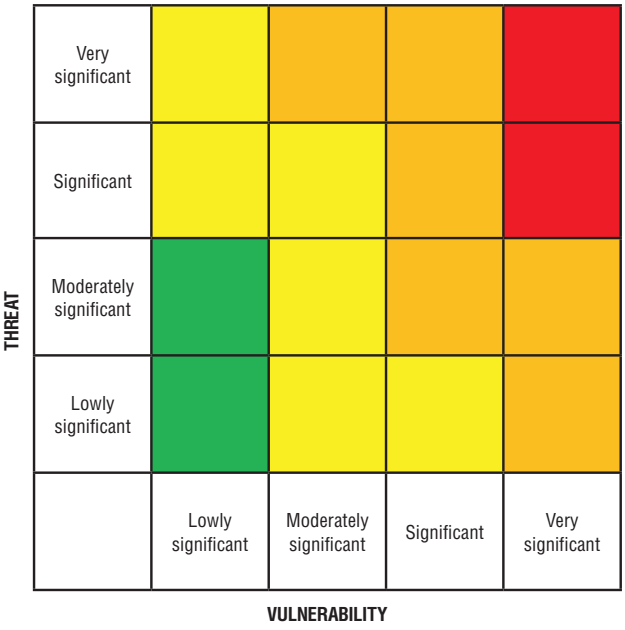
27 It measures the concrete occurrence of the threat on the territory. The data used originate from the evidence available on the subject of reports to the particular offense or class of offenses.

Step 3: vulnerability

This third step consists in assessing the level of vulnerability (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the scenarios identified in Step 1.

For each of the scenario identified in Step 1, the vulnerability assessment will **focus on the existence and effectiveness** of **safeguards** in place. The more effective the safeguards in place, the lower the vulnerabilities and risk are.

The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in Step 1, required to implement the AML/CFT legislation.



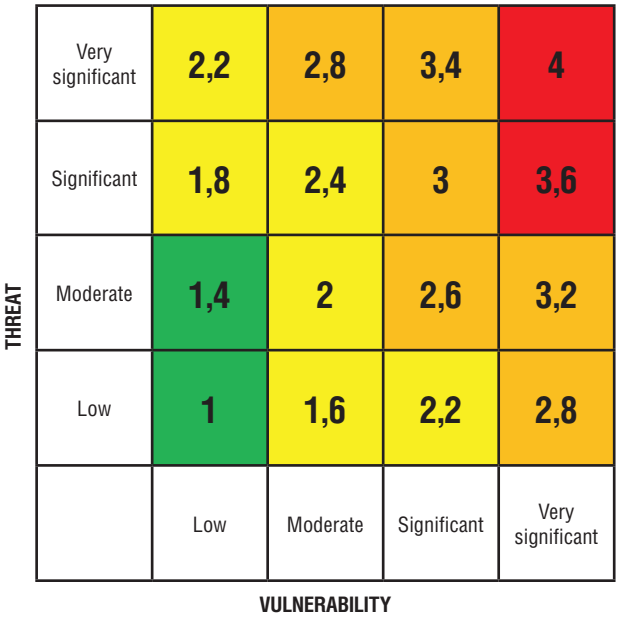
For the specific purpose and scope of the SNRA, the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the wide nature of the ML/TF risks to be considered in the SNRA, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other AML authorities and international cooperation, including between AML supervisors.

Assessment of ML/TF vulnerabilities of the system as a whole will be based on the data collected and analyzed by the relevant supervisory authorities, FIU and national authorities.

Step 4: residual risks

The outcomes of steps 2A/B (ML/TF threat assessment) and 3A/B (ML/TF vulnerability assessment) will determine the risk level for each identified risk (Steps 1A/B), as combination (matrix approach) of the assessed threat and vulnerability level.

The risk matrix determining this risk level is based on a weighting of **40 % (threat) / 60 % (vulnerability)** – assuming that the vulnerability component has more capacity in determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given modus operandi – thus impacting ultimately the level of threat.



RISK	
1 – 1,5	LOW
1,6 – 2,5	MODERATE
2,6 – 3,5	SIGNIFICANT
3,5 – 4,0	VERY SIGNIFICANT

Involvement of Private Sector and Civil Society

The Commission will consult the private sector and civil society during the process. It will organize dedicated workshops with the four main groups of private sector stakeholders (financial sector, legal professions, other obliged entities, non-governmental organizations). The Commission will organize those workshops in two stages:

- Following the risk identification: consultation on the basis of already identified risks and collection of feedback regarding risk identification;
- Following the finalization of the risk assessment: consultation on the outcome and possible mitigating actions.

AML/CFT Reassessment/Ex Novo Assessment

Based on available intelligence and information, the Commission will propose further rounds of the risk assessment to reassess the evolving threat situation or new emerging threats. The Commission ensures an updating of the risk assessment every two years, or more frequently if appropriate.

Unless there are exceptional circumstances, the first update of the SNRA would take place 2 years after issuing of the initial SNRA report (i.e. June 2019). This first update will be drawn up through a lighter procedure. Such lighter procedure will imply gathering of information by a written procedure (e.g. questionnaire) and will focus on implementation of the Commission recommendations concerning mitigating measures, and evaluation of the risks following the mitigation.

The Commission will then assess the experience gained and, if need be, adapt its methodological approach. The second update (June 2021) would likely follow the full standard methodology for a more comprehensive assessment. It will consist in assessing the relevance of the first risk assessment outcomes by including new emerging risks.

1.4. Approaches to Assessment of ML Short- and Long-Term Effects

The ML effects can manifest themselves in short-term distortions of demand for a variety of products, services or assets, in both real and financial sectors of the economy. The use of successfully laundered assets has considerably wider and more long-term negative social, economic and political implications that affect citizens, business, national and international interests, including promotion of further criminal activity and thus further increase in the amounts of proceeds laundered.[28] To date, the analysis of dedicated publications and world practices summarizes a wide range of ML into 24 categories (Tables 1.10 and 1.11).[29]

All 24 ML effects shown in Tables 1.10 and 1.11 do not necessarily have an **immediate (short-term) effect**, but may occur with a certain time lag **(in the long-term period)**. In view of this, it is worth focusing on the successive, detailed examination of the short- and long-term effects of money laundering on the economy, society and the political area. As to the effects of terrorist financing, they are different for different jurisdictions and most negatively manifested in the countries that become objects to terrorist acts.

In the context of the consequences for the economy, ML negatively affects: the real sector (the production and consumption area); business activity; relative prices; savings; productivity; employment and growth. ML also adversely affects the financial sector – its liquidity, reputation, integrity and stability. The public sector experiences an adverse effect of ML through unpaid taxes as well as through threats in the area of illegal privatization processes. The monetary sector may be hit trough large and uncontrolled capital flows, as well as through increasing volatility of interest rates and exchange rates.

From the standpoint of social destruction caused by ML, it includes: increasing crime level; increasing corruption and bribery; contamination of legal business with ties with illegal businesses.

The political sector feels the undermining (buying up) of political institutions (authorities, state institutions, organizations) and institutes (legal norms, “rules of the game”).

28 Masciandaro D. Money Laundering: The Economics of Regulation / D. Masciandaro // European Journal of Law and Economics, 1999. – № 7 (3). – P. 225–240.

29 Unger B. The Scale and Impacts of Money Laundering / B. Unger. – Cheltenham, UK; Massachusetts, USA: Edward Elgar Publishing, 2007. – 228 p.

Table 1.10. Characteristics of the short-term effects of ML

Short-term effects	Indirect			Real sector	Financial sector	Public & Monetary sector
	Economic	Social	Political			
1. Losses to the (predicate crime) victims and gains to the perpetrator				x		
2. Distortion of consumption and savings	x			x		
3. Distortion of investment	x			x		
4. Artificial increases in prices	x			x		
5. Unfair competition	x			x		
6. Changes in imports and exports	x			x		
7. Changes in output, income, and employment	x			x		
8. Lower public sector revenues	x					x
9. Changes in demand for money, exchange rates, and interest rates	x					x
10. Increases in exchange- and interest-rate volatility	x					x
11. Greater availability of credit	x			x		
12. Higher capital inflows	x				x	x
13. Distortion of economic statistics			x			x

Summarizing of international scientific and practical experience of ML risk assessment at the national level enables specifying the characteristics of their short-term effects in the context of those stated in Table 1.10.

Losses to the (predicate crime) victims and gains to the perpetrator Money laundering is associated with the commission of a predicate offense (fraud, theft, drugs, tax evasion). This means that resources obtained through committing of a predicate crime are illegally and unfairly transferred from the control of the victim to the offender. The illegal nature of the proceeds of crime renders the laundering activity necessary in order to make the wealth appear as if it was derived by legitimate means, thus securing offenders from prosecution by the law enforcement agencies. Thus, ML makes crime worthwhile (rewards criminals). It helps give legitimacy and even respectability and gives financial and economic leverages (power) to most deviating (from behavioral point of view) members of society.

Table 1.11. Characteristics of the long-term effects of ML

Long-term effects	Indirect			Real sector	Financial sector	Public & Monetary sector
	Economic	Social	Political			
1. Threatens privatization	X		X			X
2. Changes in foreign direct investment	x			x		X
3. Risks for the financial sector, liquidity	x	X			X	
4. Profits for the financial sector	x				X	
5. Reputation of the financial sector		X		x	X	
6. Illegal business contaminates legal business	x		X	x	X	
7. Corruption and bribe		X	X	x	X	
8. Negative/positive effect on growth rates	x			X		
9. Undermines political institutions and institutes			X			x
10. Undermines foreign policy goals			X			x
11. Increases crime		X	X			x

The majority of predicate crimes directly affect the entities of the real sector of economy. For example, a predicate, like drug trafficking, has a direct negative impact on GDP as a result of: drop in labor productivity of drug addicts; their premature mortality; minimizing the consumption of other (except for drugs) goods, works and services produced in the real sector of economy; additional costs for the law enforcement, judicial and penitentiary systems; significant growth of criminal manifestations on the part of drug addicts; losses of insurance companies that compensate for the consequences of crimes committed by drug addicts; additional costs for companies and individuals to install external security systems; much lower education among drug addicts; lower marriage and fertility level; higher level of corruption (to cover the illegal activities of drug trafficking).

Distortion of consumption and savings. Given that the results of a predicate crime transfer money from the victim to the offender, the use of these funds by the offender differs from those areas in which the corresponding revenues could be used by their

real owner. It is about the existence of certain behavioral advantages in spending money by criminals and also that these advantages differ significantly from the advantages of ordinary citizens (legal business entities).

First of all, it should be noted that the ML activities are closely related to acquisition of assets such as real estate, diamonds, luxury cars, antiques and other luxury items. It is luxury items that allow concealing large volumes of illegal funds. At the same time, ordinary citizens would have spent money stolen from them on their daily expenses, on planned investments or on savings. In general, the net result for the economy from ML transactions is loss of money due to a disturbance in the structure of consumer demand and the amount of savings[30].

Brigitte Unger, following the analysis of 52 high-profile criminal cases for over 400 thousand euros each, distinguishes four behavioral groups of criminals on the basis of their spending of the proceeds from predicate crimes (Fig. 1.17):

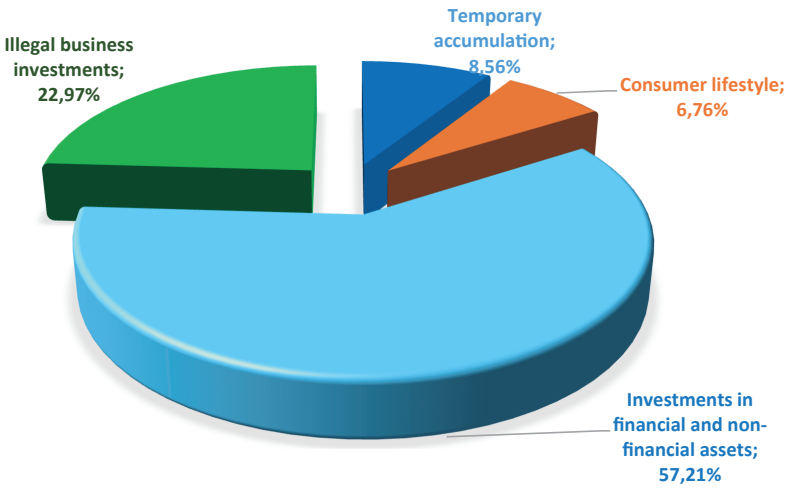


Fig. 1.17. Areas of spending criminal proceeds

For financial investments, ML is a prerequisite, since before investing, the entity has to confirm legality of the money origin (taking into account the regulations for financial markets established in all countries of the world with a developed stock exchange infrastructure). ML is also needed in case of illegal business investing, since establishing of a business, becoming a shareholder with a significant share in the capital requires availability of clean money. Thus, it can be suggested that, at least for the developed countries, 80% of criminal proceeds require laundering, based on the criminals' behavioral preferences. In addition, ML is much more important for organized crime than for individual offenders, primarily in view of the scale of the illegal proceeds they operate.

It can be stated beforehand that criminals (in the context of consumption and/or savings) behave like ordinary people. Organized criminal groups, like wealthy legal members of

30 Walker, J. Estimates of the Extent of Money Laundering in and through Australia in 1995. Paper prepared for the Australian Transaction Reports and Analysis Centre, September 1995, Queanbeyan: John Walker Consulting Services. - P. 61.

society, save and invest most of their money, while unorganized criminals tend to spend their incomes on current consumption, like the poorer population groups. To accurately assess how POC laundering changes the structure of consumption and savings, we need article-specific comparisons of behavior of criminals and legal households (business entities). Today, such a comparison has not been done either in Ukraine or globally (at the level of international organizations). Therefore, any conclusions on the issue are preliminary, incomplete (primarily due to data latency) and require further research.

Distortion of investment. The negative ML effects on investing logically derive from the fact that in their investment preferences, money launderers are more likely to be driven by a desire to avoid control and detection than long-term investment efficiency. Advantages of criminals in the process of investing significant amounts of funds can have a devastating impact on the economy, since they result in redistribution of funds in favor of those assets that generate insignificant business activity, employment and gross added value[31].

When the desire to conceal the origin of funds begins to dominate the desire to obtain long-term investment income, it distracts income from long-term investment into the real economy sector and translates into speculative, risky and low-quality investments ("trash" assets).

ML causes irrational use of legal resources, due to distortion in relative prices of the assets that become a tool for legalizing "dirty" money. Unreasonable, speculative growth in prices for real estate items is one of the most striking examples. The real estate sector is one of the most attractive for ML transactions because of its non-transparency, as the value of a real estate item is usually difficult to assess. Given the above, investing in real estate is one of the most efficient methods of allocating (the first stage of ML) significant amounts of illegal origin money, since "astronomical" differences occur between the real estate purchase price and its subsequent re-sale (after its cosmetic refurbishment). In addition, it is possible to distinguish the following characteristics of the real estate market, which make it interesting for ML: safety of investment; complexity of assessing the objective value of property; traditional speculative activity on the specified market; ability to share possession and use; possibility of receiving "clean" income; possibility of being used for criminal activity.

The rate of POC turnover and liquidity of the corresponding forms of assets through which money is laundered become decisive factors for criminals. This is the main reason why the capital is allocated not optimally in comparison with the situation when allocation of resources takes into account the factors of fundamental (financial and economic) analysis of investment items.

Criminals, in addition to real estate, also invest their proceeds in acquisition of companies (legal entities) in order to subsequently obtain legal sources of money origin and mix them with illegal in the ML process. A large amount of criminal investment in the real economy is focused on cash-oriented types of economic activity: bars, cafes, restaurants, boutiques, brothels (in countries with legalized prostitution), hotel business, gambling, transportation. Another important factor in the use of legal entities for criminal purposes is a possibility of acquiring inactive (previously registered and with available basic permits, licenses) enterprises by third parties.

Artificial increases in prices. As outlined above, POC launderers are interested in investing in those areas (assets, goods, work, services) that allow the maximum disguise

31 Bartlett L. Brent. Economic Research Report For The Asian Development Bank: The negative effects of money laundering on economic development. [Electronic resource]. – Access mode: http://www.u4.no/recommended-reading/the-negative-effects-of-money-laundering-on-economic-development/

of the real origin of the funds. That is why, for these groups of assets, criminals agree to pay even an inflated price, as well as to buy unattractive property, to maximize legalization of their illegal activities using legal business entities of the real sector of economy. The above behavioral motives are the main factor for artificial price growth in some sectors of economy for individual assets (land, buildings, apartments, shares), goods, work, services. Excessive prices are beneficial for those who launder profits, since they allow allocating a larger amount of money. At the same time, the overwhelming majority of the legal population is experiencing substantial loss in income by acquiring the necessary assets at an irrationally high (legally speaking) level of prices.

Unfair competition. The Thomas Gresham law, also know as the Nicolas Copernicus law: "Bad money drives out good" can be fully applied to describe the consequences of ML transactions, paraphrasing it like "dirty money drives out clean". Possession of illegal funds is dangerous because one can be identified and convicted of committing a predicate crime. The desire to convert illegal proceeds into other assets is accompanied by a desire to give them the appearance of legal wealth.

While reaching the above goal, criminals embark on unfair competition for assets with legal entities, winning over them. Usually, the party which launders criminal proceeds is guided not by fundamental factors (real or book value of assets, rate of return, profitability), but rather by the possibility of obtaining benefits in terms of concealing the real location and source of the income with which the said assets are acquired. All of this causes artificially increased prices, the level of which becomes inaccessible to the party trying to keep good faith in competition.

Changes in the foreign economy sector (in imports and exports). ML transactions also distort data on imports and exports in a country. In view of the above, persons who launder criminal proceeds are prone to consuming (usually imported) luxury goods. Such trends result in a problem with a negative balance of payments. The said imports do not generate internal economic activity, employment, and may decrease domestic prices (deflation) due to diversion of money stock to foreign trade, which, in turn, decreases productivity of domestic enterprises, and is the reason for an increasing negative balance of a country.

At the same time, ML can significantly distort export and import prices. The most common tactics used in ML is buying imported goods at excessive prices and exporting domestic goods at underrated prices. For example, an importer of the fixed production assets (equipment, machinery) may agree with a non-resident seller of Ukraine that the purchase price of such equipment will be 30% higher than the usual market price. In this case, arrangements are made for the non-resident seller to credit the price surplus to the resident buyer's accounts opened in foreign banks in the name of the resident's associates. At the same time, in Ukraine, a resident receives the right for reimbursement of a larger amount of value added tax from the budget on the price of the imported fixed production assets. Where such transactions are effected recurrently (have a permanent nature), this leads to artificial distortion of export-import prices.

The mechanism described above relates to the problem of "transfer pricing", counteracting which has been a practice for several dozen years in developed countries[32]. It should be noted that in Ukraine this practice has spread since the first years of its independence, but only in July 2013 its was legislatively settled through passing of the

32 Baker W. Raymond, The Biggest Loophole in the Free-Market System // The Washington Quarterly. Autumn 1999, pp. 29-46 [Electronic resource]. – Access mode: http://www.brookings.edu/~/media/research/files/

law "On Amending the Tax Code of Ukraine with Regards to Transfer Pricing". The above changes came into effect on 1 September 2013[33].

Changes in production, income, and employment. ML also adversely affects the output (production of goods, works and services), income, and employment by distracting resources, as outlined above, from the sectors that generate high levels of productivity (light, food, machine-building industry, etc.) to the sectors that "sterilize" economic activity (speculation in the real estate market; trade in precious metals, stones and products therefrom; trade in antiques, etc.). The multipliers of the "sterile" sectors of economy are smaller in terms of output, income and employment, and thus generate net losses for the economy compared to situations where money would be spent (invested) in non-sterile sectors.

Lower public sector revenues. ML can have devastating effects in the context of mobilization of tax payments. The proceeds laundered in most developed countries are defined as proceeds from tax evasion by falsifying financial and economic reports and providing false data to the fiscal authorities on the item of taxation. As noted above, tax crimes are not considered predicative for laundering purposes in Ukraine today.

At the same time, an increasing number of committed predicate crimes and related ML facts requires increased public expenditures to ensure systemic prevention and countering these phenomena, which, in its turn, further reduces the revenues at the disposal of the public sector.

In 1999, Gideon Yaniv developed a mathematical model that demonstrates the interconnections between ML and tax regimes.

A conclusion from this model is that the ML motivation increases with decreasing tax rates and where the financial monitoring regime in the country is weak[34].

An important aspect that is often omitted in the dedicated literature is that ML can also increase public sector revenues. The above said does not contradict the basic intention of criminals who, being interested in legalization of their own income, pay all taxes from the legal entities controlled by them. The essence of the legalization scheme is that taxes are paid from non-existent income of cash-oriented legal business entities controlled by criminals. The liberal taxation system paradoxically "provokes" the said method of legalizing criminal cash flows and causes a real increase in the revenues to all levels of budgets, but such budget revenues are essentially quasi-legal and depend on the level of criminal activity within a particular jurisdiction. In addition, the liberal tax regime, coupled with the inadequate system for preventing and combating money laundering, is becoming a major factor for the growing attractiveness of national jurisdiction for resident and non-resident (transnational, extraterritorial) crime, which causes an avalanche-like level of criminalization of all spheres of life in a fiscally liberal country. The above applies primarily to offshore jurisdictions in the world, whose tax regimes are the most liberal. That is why, in the system of primary financial monitoring measures, one of the first items of detection (signs of mandatory detection) is financial transactions with offshore counterparties.

Changes in demand for money, exchange rates, and interest rates. ML causes changes in demand for money. Thus, according to a special survey conducted at the end of the

articles/1999/9/ autumn%-20co-rruption%20baker/baker.pdf

33 "On Amending the Tax Code of Ukraine with Regards to Transfer Pricing": Law of Ukraine of 04.07.2013, No. 408-VII // "Holos Ukrayiny" of 07.08.2013 - No. 145.

34 Yaniv, G. (1999). 'Tax Evasion, Risky Laundering, and Optimal Deterrence Policy'. International Tax and Public Finance, 1999, vol. 6, issue 1, pages 27-38.

1990s at the request of the IMF, it was found that a 10% increase in crime rates causes a 6% decrease in total demand for money in the country. In addition, a 10% increase in crime rates reduces the demand for the national currency by almost 10%, causing changes in currency exchange rates and interest rates[35].

Peter Quirk obtained the above results based on the following regression equation:

$$M_i = M_i(y, e_p, i_d, L_i)$$

The above equation suggests that the demand for money (M_i) is directly dependent on income (y) and inversely dependent on: the expected inflation (e_p), deposit rates (i_d), and scope of money laundering (L_i).

In another IMF-commissioned study by Vito Tanzi, there is empirical evidence for the US economy evidencing that in the mid-1980s, about 5 billion USD in cash was withdrawn from the US system annually due to POC laundering (0.1% of US GDP in monetary terms)[36].

Vito Tanzi, when studying the macro-level ML effects, paid much attention to the modeling of demand and supply parameters for money across countries, as well as to studying the relation between the emitted money supply and the one that is in circulation within a country. Unfortunately, there is no newer empirical-based research and the Tanzi models can not be considered adequate today, as the globalization of financial markets, the emergence of the Eurozone, decisive steps towards global centralization of policies in the post-crisis reform of the monetary and fiscal area in the countries have been further eroding the concept of independent national monetarism and the independence of national monetary aggregates.

It is necessary to add emergence of the latest digital money surrogates (including virtual currencies – decentralized crypto units), which, due to their extraterritorial (global) nature, have already cast doubt on the ability of national monetary, fiscal and financial regulators to influence the exponential nature of their uncontrolled development.

Illegal inflows and outflows of capital from the economy of a particular jurisdiction can significantly affect the amount of money in circulation, and hence the price of the national currency, its exchange rate and the central bank interest rate, through which the latter tries to influence price stability in the country.

Greater availability of credit. Infusion of illegal proceeds into an economy results in easier access to credit resources for legal entities, entrepreneurs, and enterprises. This results from money laundering through a country's banking system, growth of deposits (formed due to laundered criminal proceeds), which causes an increase in the amount of liquidity that banks can lend to their clients. If the effect of infusing criminal proceeds into the economy is significant, it can lead to a significant reduction in the interest rates on loans, even when the central bank's interest rate remains invariably high. This problem is especially relevant for countries with a backward economy and underdeveloped, non-liquid, rudimentary markets of financial services.

Higher volatility of capital inflow and outflow. POC launderers channel their money for laundering to the countries whose regulatory AML regimes are least effective, which becomes the main reason for the influx of large capital flows, the real source of which is an aggregate of predicate crimes committed in other countries of the world. Taking into account the results of the analysis, highlighted above, and taking into account the main

35 Quirk, Peter J. (1997). Money Laundering: Muddying the Macroeconomy, Finance and Development, 34 (1), p. 3.

36 Tanzi, V. (1997), Macroeconomic Implications of Money Laundering, in E.U. Sanova, Responding to Money Laundering, International Perspectives, Amsterdam: Harwood Academic Publishers, pp. 91-104.

areas of investment and integration of laundered criminal proceeds, it can be concluded that the global investment of money laundered (or that is in the process of laundering) is less beneficial for the recipient country compared to how the flows of clean (non-criminal) capital could be invested.

Considering the influence of ML on capital flows, five main directions, which are illustrated in Fig. 1.18, should be distinguished:

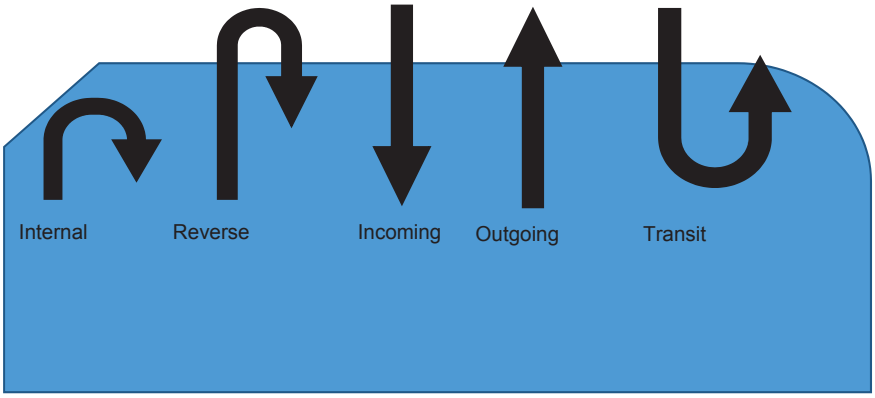


Fig. 1.18. Capital movement in the ML context

Internal flows of ML relate to cases where the proceeds of crime (as a result of a predicate offense) are laundered or spent within a country and upon laundering are integrated (invested) into real and financial assets within a national jurisdiction.

Reverse flows of ML relate to cases where criminal proceeds are acquired within a national jurisdiction, then the proceeds are withdrawn outside its limits (smuggling of currency assets, transfer pricing schemes and other means), are laundered outside the national jurisdiction, and upon laundering, return to the country for their further integration (investing) into real and financial assets.

Incoming flows of ML related to a predicate crime in a foreign jurisdiction (whose AML regime is more effective compared to the regime of the country to which flows of criminal proceeds are infused) are laundered and integrated within the national economy.

Outgoing streams of ML are usually associated with the "escape" of criminal capital beyond a national jurisdiction for the purpose of its further laundering and integration in other countries (primarily in numerous offshore jurisdictions of the world).

Transit flows of ML use this country solely for POC laundering transactions, after which the legalized proceeds are withdrawn and integrated in other countries.

Economically, the impact assessment of each of the five capital flow directions will be different, since the directions, whose predicate basis of proceeds are crimes committed within a national jurisdiction (internal, reverse, outgoing), can be considered more negative. However, two of the three areas (internal and reverse) mentioned above envisage integration of the proceeds laundered within a national jurisdiction, and hence certain positive economic effects that will arise when the laundered proceeds are invested in real assets, which will result in creation of additional jobs, payment of additional taxes to the budget, etc. Similar comments can be applicable to the consequences of the incoming

flow of criminal proceeds for a national jurisdiction, which will be even more positive from a purely economic point of view (detached from the analysis of moral components), since they do not envisage committing of crimes within this jurisdiction.

The purely accounting approach to assessing the impact of capital flows associated with criminal sources of their origin is short-sighted, non-visionary, and success-myopic. Anyone well-meaning must study any phenomenon in the short-, medium-, and long-term perspective to adequately assess the whole range of associated risks. Therefore, whereas in the short-term perspective it is possible to derive some positive accounting effects by the "cost-benefit" method, in the medium- and even more so in the long-term run, the consequences will be clearly negative, since they will include covert (masked) criminal takeover of the real sector of economy (real and financial assets), corruption erosion of state institutes at all levels (criminal takeover of the state decision-making and implementing centers), criminal and oligarchic monopolization of the most important (and thus the most liquid financially) spheres of social life, etc.

Distortion of economic statistics. Depending on the type of predicate crimes, the proceeds of which are being laundered, the consequences of the legalization phenomenon for the economic statistics data will be different. The most dangerous predicates from the standpoint of macro-level statistics are the crimes associated with the masking of the taxation item in order to avoid tax payments especially in large amounts. This type of fiscal predicates has a direct negative impact on the reliability of the system of national accounts, based on which the most important managerial decisions in the state are made.

One of the most relevant examples of distorted state macro statistics for Ukraine is the hidden population employment in illegal business or illegal employment in legal business. By benefiting from such employment at the average monthly salary level in the national economy, the illegally employed population is adding to the statistical ranks of the unemployed, receiving state financial assistance for this. The phenomenon of "envelope wages" is also associated with the employment level described.

Equally relevant is the phenomenon of transfer pricing (underrating/overrating of export and import prices) as the main factor in distortion of statistical data in the foreign economic area, which, in turn, distorts orientations for balancing a country's trade and payment balance, which determines the monetary methods of regulation of the national currency value, the inadequacy of which may become a factor in inflation or deflationary processes.

In addition, it should always be remembered that ML entities are guided in their activities by the criteria of minimizing the detection probability and minimizing penalties rather than by the rate of return on an investment item or the current and future value of assets, etc. All this leads to distortion of the state policy macroeconomic reference points, weakening the effectiveness of the state's main regulatory levers (plans, forecasts, programs, financing, tariffs, interest rates, tax rates, bonuses, discounts, benefits, etc.). All this results in the loss of the institutional capacity of the state to influence the main parameters of economic development in the country, to increase entropy processes, disorganization, chaotization, and exponentially growing social tensions, the consequences of which are unpredictable and have an uncontrollable chain character.

Overcoming this statistical problem should start with **development of an adequate system of indicators of the state statistical reporting in the field of financial monitoring, both at micro and macro levels**. Only in the case of an adequate assessment of the threats generated by the ML/TF phenomena, it is possible to more or less adequately adjust the state regulatory policy and management decisions that make up this policy.

The short-term effects of ML usually last for one to two years, while the duration of the long-term effects (Table 1.11.) is measured over a five-year or longer period. Some effects (influences) can remain latent (hidden) for more than a decade before manifesting themselves in full force. Dedicated AML/CFT information sources identify **eleven long-term ML consequences**, each of which is discussed in more detail below.

Threatens privatization. ML has potentially devastating consequences for a country's privatization processes, given that these transactions, or rather the illegal proceeds used in these processes, violate the rules of fair competition in terms of changes of the ultimate beneficiaries for the facilities that were previously state property[37].

In the long run, distorted and criminalized privatization processes cause increasing presence of persons involved in organized crime in the real economy (presence of nominal directors acting on behalf and in the interests of organized crime representatives, corrupt officials who are the real ultimate beneficial owners (controllers)).

Reputational risks of the country, changes in foreign direct investment and capital flows. Damaged reputation of a country's financial sector, which generally begins to be associated with flows of illegal proceeds, results in a significant flight of foreign direct investment from the country concerned. Direct investment also stops on the part of the domestic investor, because reputational risks undermine trust of both external and domestic investors, the said risks breed a feeling of insecurity of the right to private property and ineffectiveness of the rule of law in the country, where all areas of life become increasingly absorbed by organized crime.

On the other hand, a country associated with an ineffective law enforcement system, with a high level of corruption, with the criminal takeovers of its main institutes becomes very attractive for illegal capital and can benefit substantially from it, especially when illegal foreign capital is invested in the real sector of the economy of such a country, and does not just transit through its jurisdiction. The above process received the name "Seychelles Effect" in the dedicated literature, since the Seychelles were the first to actively compete for the attraction of foreign investments of criminal origin[38]

Attractiveness of national jurisdictions for criminal capital can be referenced through different international lists and ratings that measure the progress or regress of a particular country in the field of shadowing, decriminalization, deoffshorization, decorruptionalization, and other criteria. One of the most important benchmarks for global ML deterrence is a list of Non-Cooperative Countries and Territories introduced in 2001 by the FATF.

Risks for the financial sector liquidity. The long-term impact of ML transactions on the financial sector is one of the most significant. Significant flows of illegal money directed through bank circulation channels can significantly change the characteristics of a country's banking system liquidity. The liquidity changes in an unpredictable way, as the laundering entities are guided by specific considerations (independent from general-market, and therefore unpredictable).

Given the integrated and interconnected modern financial system, a dramatic flight of liquidity from banks can lead to uncontrolled adverse multiplier effects for other participants of the financial services market and real economy, thus creating preconditions for a systemic crisis and monetary instability in a country.

37 McDowell J. (2001). The Consequences of Money Laundering and Financial Crime: Economic Perspectives. Economic Perspectives, fn Electronic Journal of the U.S. Department of State, Vol. 6, No. 2, May 2001 pp 6-8.

38 Rawlings, G. and Unger B. (2005). Competing for Criminal Money. Paper prepared for the Society for the Advancement of Socio-economics, Budapest 30 June – 2 July 2005.

Polar opposite opinions also have the right to exist and are fairly rational from a mercantile and utilitarian point of view. Banks and investment funds may even want to have POC launderers among their clients. Clients of the proceed-laundering financial institutions focus less on higher yields on the financial products they buy, but above all on a higher level of anonymity and secrecy of their transactions. Anonymity (secrecy) is a product for which ML entities are even prepared to pay extra; in other words, they are willing to accept even a negative rate of return on a financial institution's basic products and services in exchange for a possibility to channel flows of proceeds derived from illegal sources through this institution. For banks in bad faith, such clients are a source of additional liquidity, especially in times of crisis of its acute shortage.

In today's globalized world, the borders in the area of foreign trade in goods, work and services, population migration, transfers of financial assets, etc. are becoming ever more blurred. Therefore, the issue of cross-border monitoring of illegal liquidity flows through the global financial system becomes even more relevant than ever before.

Financial sector reputational risks. The vast majority of researchers are unanimous in assessing the negative impact of ML on the financial sector reputation. To date, there is a significant number of ways by which illegal proceeds can penetrate legal financial institutions.

ML weakens development of the financial sector for two reasons: firstly, relevant financial transactions erode financial institutions from within, as there is a direct link between ML and fraudulent activity; secondly, the trust of bona fide clients is fundamental to development of financial institutions, while money laundering can destroy the trust and reputation capital almost instantaneously.

Undermining the reputation of several financial institutions simultaneously can collapse a country's financial system in general, especially in the countries where the concentration of bank capital is quite significant and one of the system banks comes under high-profile financial investigations on financial monitoring issues.

Since the domestic system of financial monitoring is bank-centered, NRA should pay special attention to the reputational risk consequences specifically for banking institutions.

The structural peculiarity of the reputational risk is that its consequences manifest themselves through a cascade of other banking risks. Being a separate banking risk that arises when providing financial services to clients with a non-transparent ownership structure and/or shady sources of capital origin, the risk of involving a bank in ML processes is manifested through emergence and implementation of other types of bank risks. In this context, the reputational risk can be classified as a category of related (complex) risks.

Corruption and bribe growth. ML generates corrupt acts not only in the financial sector, but also in all the socio-economic activity segments. Firstly, corruption and bribery affect officials of the financial institutions through which illegal proceeds are laundered. Secondly, ML also afflicts with corruption the sector of Designated Non-Financial Businesses or Professions associated with professional support of questionable contracts and transactions (barristers, notaries, lawyers). Thirdly, ML afflicts with corruption the sector of state regulation and supervision over the activities of financial institutions, officials with the decision-making authority and power. The environment struck by rampant corruption begins to generate other ways of obtaining corrupt rents, creating a variety of obstacles, reasons, and grounds for this.

Thus, the corruption effect generated by the primary ML transactions subsequently generates multiplicative adverse effects on a much larger scale, gradually affecting all

decision-making centers in all sectors of socio-political and socio-economic life.

This results in deepening of the anticompetitive environment problem, destruction of incentives for legal economic activity, unprofitableness of legal business activities within fierce fiscal and monetary constraints, transition of business entities to the illegal system, deepening of shadowing, criminalization and illegalization of all spheres of life.

Influence on economic growth indicators. ML has a significant adverse impact on economic growth. ML violates the structure of consumer demand and the scale of savings, diverting funds from investment (long-term) areas of their spending to high-risk (speculative) areas with the maximum possible turnover, liquidity and time increment. This way, productive investment in the real sector of economy is replaced by sterile investment in the speculative and fictitious simulacra of the real economy.

At the same time, criminalization and corruption of all spheres of life destroys the principles of efficient business, generates additional criminal rents, deteriorates the conditions for doing business in the country, primarily due to vulnerability of the private property institute to illegal encroachment. And if a certain legal enterprise tries to withdraw from any links with the illegal sector entities, it falls into noncompetitive environment conditions, absorbed and controlled by organized economic crime, into conditions in which a legal economic entity becomes unprofitable, insolvent, loss-making, and, in fact, thrown out of the system of prevailing illegal contracts (tenders, orders, subventions, etc.), which determine the real "rules of the game".

In addition, due to the above-described devastating impact on financial institutions, as well as through destruction of the effective mechanisms for redistribution of the limited resources (monetary, material, capital, human), ML chills down the pace of economic growth in the country even further, thus sterilizing its future.

Influence on the crime rate growth. The volume of criminal proceeds entering the official economy following their laundering increases with the growth of the economy illegalization (criminal shadowing) level. The growth in the total amount of laundered criminal proceeds occurs with a significant multiplier effect. Increasing criminalization in general and ML transactions in particular cause "contamination" of a country's legal economy and financial system in geometric progression.

A state's AML policy should be based on stepping up measures to prevent the use of professional mediators in provision of ML services. A more efficient ML deterrent system will increase the risks of white-collar intermediaries, and hence the cost of ML services. The rising cost of ML services will lead to a drop in the share of illegal proceeds to be laundered. The result will be an increased level of POC detection in the state (non-laundered proceeds are easier to identify than laundered) and reduced attractiveness of the country in terms of ML transactions within its jurisdiction.

Given the lack of complete information on the past ML and TF cases, application of risk management in this area is significantly complicated. The said incompleteness of information means that, unlike other risk management application areas, in the AML/CFT area it is very difficult to build systems for carrying out meaningful probability assessments of a substantial ML or TF risk, as well as the consequences of such risks. In addition, the ML and TF processes are often too complicated to conduct a detailed analysis of each risk event associated with each type of the ML and TF scheme.

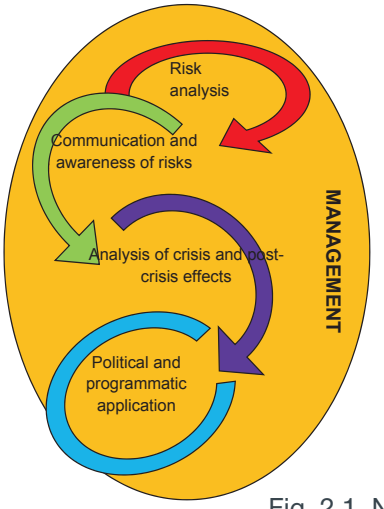
SECTION II.
METHODOLOGICAL PRINCIPLES OF NRA IN UKRAINE

Risk assessment is an important basis for managing them and building systemic guarantees of sustainability in Ukraine. The NRA is an important step in defining a common vision of the risk base, as well as an understanding of which risks should be taken into account, mitigated, neutralized and/or transferred (transferred to a supranational level). The NRA promotes development of recommendations and definition of priorities for strengthening the sustainability of certain types of economic activity, legal entities, sectors, products, services, communities and CMU with its institutions.

The NRA should be comprehensive and requires a sound management structure with agreed timelines and evaluation rules to ensure consistent, effective and reliable outcomes. It should also be understandable to all the participants and be consistent with the context of Ukraine, take into account a combination of quantitative and qualitative criteria for assessing latent (it is difficult to obtain timely and reliable information from reliable sources) phenomena and processes in the AML/CFT area. Efficient NRA should stimulate development of all the participants in the national AML/CFT system, focus their efforts on identifying the most common threats, vulnerabilities and on neutralizing the risks identified – first of all, those with a high probability of occurrence and significant negative impact on the state of affairs in the AML/CFT area. At the same time, it is necessary to distinguish between the **possibility of unpredictable one-off significant events that are risk generators** in the financial monitoring area (technological innovations in the financial services area may become triggers for such events) **and a large number of less resonant threats and vulnerabilities, which generate more regular risk events**. To this end, the NRA results should be actively discussed with the main stakeholders in policy and programmatic decision-making – SFME, law enforcement and intelligence agencies, as well as with RE.

NRA determines the optimum allocation of scarce resources to build sustainability of the system and its participants. By identifying and assessing the probability and impact of potential shock and crisis situations, risk assessment provides a basis for prioritizing in a way that is adapted to a specific country's context, environment, needs and benefits.

The methodology in this paper consists of five key components:



1. Managing the NRA process
2. Risk Analysis
3. Communication and awareness of risks
4. Analysis of crisis and post-crisis effects (impact assessment of the identified risks)
5. Political and programmatic application

Fig. 2.1. NRA methodology components

2.1. Managing the NRA process

When managing the NRA process, it is recommended that the following factors be taken into account :

Scope, goals, definitions and methodology:

- implement a comprehensive, exhaustive risk assessment approach in the AML/CFT area;
- definition and transfer of goals;
- agreement of the key terms and methodology.

Transparency and accountability:

- promoting transparency of the methodology used to assess the AML/CFT risks;
- disclosure of sources of data, information, and expert opinion;
- introduction of mechanisms for internal and external reporting and accountability.

Multilevel management, multilateral participation:

- identification and involvement of key stakeholder groups;
- identification of the lead coordinator, who will ensure proper cooperation among the stakeholders;
- clear definition of those responsible for the respective levels and components of risk assessment, implementation of the coordination process for all the NRA participants;
- maintaining training programs (seminars) on the use of risk assessment methodology and delegation of responsible persons from each NRA participant.

Fig. 2.2 shows the structural and logical scheme of the risk management process in the NRA context.

2.1.1. Scope, goals, definitions and methodology

Risk Assessment Approach

Risk assessment should cover their entire spectrum: ML/TF threats, vulnerabilities and risk consequences at the country level as a whole and in the context of the existing sectors, whose representatives form the AML/CFT system in Ukraine.

The risks identified should be divided into those relating to one-off large events **(intense risk)** and those associated with regular events of a smaller scale **(extensive risk)**. Equally important is distinction between **external and internal sources of risk formation** in relation to Ukraine. The assessment should facilitate identification of common features and relationship between different possible events, their sequencing, the potential of any event to launch new threats and multiply the negative effects of the impact at the national level, as well as possible implications in a cross-boundary context.

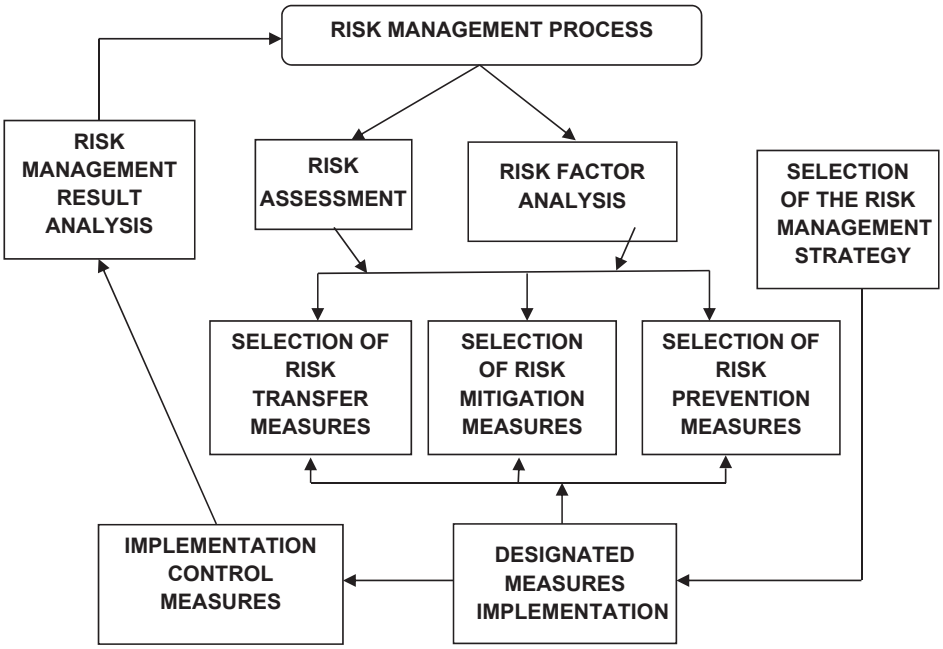


Fig. 2.2. Structural and logical scheme of the risk management process in the NRA context

Purpose of NRA

The general purpose of NRA is to identify policy development priorities, to program AML/CFT activities, and to finance measures aimed at preventing and mitigating the existing threats and vulnerabilities of the AML/CFT system, which are the main factors for manifestation of a corresponding risk and factors of its level.

It is worth noting that this risk assessment methodology can also be used to study **programmatic risks** – the risk of failing to achieve the goal or purpose set (in the Action Plan developed following the first phase of NRA) or causing damage through intervention (excessive complexity and scope of regulatory requirements, excessive scope of sanctions, etc.), or **institutional risks** – reputational losses, non-consideration of institutional gaps in the system (unresolved issues which prompted reforming of the law enforcement agencies, courts, regulators, or which were the result of incomplete or unstarted reforms, etc.).

The purpose should be clearly explained to the providers of data, information and expert opinion; so that the type and quality of the required data can be determined, as well as the most appropriate methodology and mechanisms for summarizing the information collected about risks and their components.

Clear definition of the main terminology

A general understanding of the basic terminology will help to maintain a consistent approach within NRA, which will facilitate consistency and comparability of results. General definitions will also contribute to transparency and accountability both in risk assessment and in definition of policy priorities. A helpful guidance to the terms can be found in Sub-section 1.2, Section 1 of this Methodology.

2.1.2. Transparency and accountability

In order to comply with transparency and accountability, the following steps should be followed:

- make the results easy to understand;
- record the methods used and uncertainty levels;
- justify the choice of inclusion or exclusion of certain risks;
- identify data sources;
- agree on a protocol on the use of expert opinion to avoid bias and conflict of interests;
- determine limitations on accuracy and completeness of data;
- consider independence of evaluation of the results.

While open access to the risk data and models is the ultimate goal, the decision on disclosure of data and risk assessment results should also be based on other considerations, such as cost of data provision, privacy, confidentiality, and security. Partial access to data, e.g., provision of access to specific ML vulnerability data, but not to other risk data, specifically that related to sources, methods, or TF channels, may be an intermediate option.

2.1.3. Multilevel management, multilateral participation

Leading the NRA process and its key stakeholders

The State Financial Monitoring Service of Ukraine should be (according to the Law) the NRA organizer and coordinator.

The four key stakeholder groups should be involved in the NRA process:

1. those contributing and providing information *(including expert practitioners, local and international scholars, AML/CFT system participants, etc.);*
2. those who use the results to identify priorities and manage policy and programmatic solutions *(including SFME, RE, law enforcement and judicial systems, and CMU)*;
3. those who are immediately exposed to the risks identified – responsible for preventing and countering the relevant risks and factors causing them *(including a broad private sector and government agencies)*;
4. stakeholders whose assets or resources can be adversely affected by the consequences of identified risks.

Thus, the NRA participants should include all the entities that are participants of the AML/CFT system without exception and other stakeholders who can facilitate accomplishment of the NRA tasks, namely:

- SFME:
  - the National Bank of Ukraine;
  - the Ministy of Finance of Ukraine;
  - the State Financial Monitoring Service of Ukraine;
  - the Ministry of Justice of Ukraine;
  - the Ministry of Economic Development and Trade of Ukraine;
  - the Ministry of Infrastructure of Ukraine;
  - the National Securities and Stock Market Commission;
  - the National Financial Service Markets Regulation Commission.
- Reporting entities:
  - banks;

- non-banking institutions;
- specially designated reporting entities.

- Law enforcement authorities (including prosecution authorities) and judicial authorities:
  - the Prosecutor General's Office of Ukraine;
  - the Security Service of Ukraine;
  - the Ministry of Internal Affairs of Ukraine;
  - the National Police of Ukraine;
  - the State Fiscal Service of Ukraine;
  - the National Anti-Corruption Bureau of Ukraine;
  - the State Border Guard Service of Ukraine;
  - the Foreign Intelligence Service of Ukraine;
  - the Supreme Court of Ukraine;
  - the State Judicial Administration of Ukraine.
- other government authorities possessing the information required to accomplish the NRA tasks:
  - the National Agency on Corruption Prevention;
  - the National Agency of Ukraine for finding, tracing and management of assets derived from corruption and other crimes;
  - the Ministry of Foreign Affairs of Ukraine;
  - the State Audit Service of Ukraine;
  - the State Statistics Service of Ukraine;
  - others (if required).
- industry associations and self-regulatory organizations, experts, researchers, scholars, etc.:
  - the League of Insurance Organizations of Ukraine;
  - the Association of Ukrainian Banks;
  - the Association «The independent Association of Ukrainian banks»;
  - others (if required).

The Platform for participation of each participant in NRA is the Sectoral Risk Assessment Working Group in the AML/CFT system.

The working group includes representatives of the SFMS, all SFME, law enforcement and judicial authorities, other state bodies, institutions and organizations.

In accordance with the tasks assigned to the working group it has the right to:

- involve, employees of the SFMS, as well as independent experts for the consideration of issues related to its activities;
- organize thematic workshops, meetings and other measures on the sectoral risks assessment issues;
- invite representatives of executive authorities, other state bodies, enterprises, institutions and organizations to their meetings.

Importance of interactions in the NRA context

The list of advantages of a joint risk assessment includes:

- increasing the amount of available information (from a large number of sources), and thus the ability to conduct NRA more efficiently;
- reduction of the analysis cost;
- reduction of bias on the part of individual participants or individuals;
- general agreement on which risks should be prioritized;

- ability to use a wide range of tools in different sectors and at different levels of the AML/CFT system to neutralize the risks identified.

Coordination of different assessments

Where possible, NRA should also take into account the results of supranational (international), subnational or public and other expert assessments.

Need of training

Training on the methodology of risk assessment, data collection, analysis, and communication, as well as capacity building for better understanding of the risks, where there is lack of information, should be taken into account. The main aspects of the previous NRA should also be documented, disseminated, and studied.

2.2. Risk Analysis

At the stage of risk analysis during NRA, it is recommended to focus on the following four tasks:

Threat identification and analysis

- identification of threats that may have adverse or destructive effects on people, assets and economy;
- creation of a certain range of threats scenarios and identification of occurrence likelihood for selected risk events;
- Data collection and dissemination.

Analysis of vulnerabilities and impact consequences

- identification of sectors, types of predicate crimes, legal business forms and financial inclusion products with increased vulnerability to ML/TF;
- identification of the main factors contributing to existence of a vulnerability;
- assessment of the potential negative effects of using identified vulnerabilities.

Risk evaluation

- risk assessment based on the analysis of threats, vulnerabilities and their occurrence consequences;
- uncertainty level assessment.

Risk monitoring and reassessment

- threat and vulnerability monitoring, and periodic data update;
- Identification of potential future risks.

2.2.1. Threat identification and analysis

How should a threat be identified?

Consultations with scholars, private sector, community, academics and other experts will help ensure coverage of all the relevant threats. Clear criteria should be used to determine **which events are sufficiently substantial or inevitable** for analysis.

Substantial events are those that can affect things that are valued by individuals, community, or government agencies. To determine which events are inevitable, the assessment may decide to exclude, for example, events that are likely to not occur in the next five years.

It is important to include both extensive and intensive risks. Extensive risks can have a more immediate impact on vulnerable sectors, institutions, products, and services than less likely intense risks.

What should be included in the scenario?

During NRA, it is recommended to consider:

- The type of the threat, primary and subsequent threats.
- Occurrence – where it occurs and what areas are affected.
- Intensity is how strong an event is, and what can exacerbate it (for example: gaps in the main institutes and institutions that regulate AML/CFT compliance, violation of the financial monitoring cycle, etc.).
- Time – seasonality? How long does the event last?
- The reason – what is the cause or trigger? How will the event unfold in time?
- Caution – can there be preventive measures? Is there time to prepare?
- Who is directly affected and in which way – people, assets, environment?
- Interdependence and transformation – what and who can be indirectly affected?
- References to previous events – what kind of experience can be drawn from historical events?
- Additional information – level of staff readiness, data reliability, relevance and accuracy, etc.?

During the AML/CFT system threats evaluation, it is necessary to pay attention to:

- threats arising from the types of predicate crimes;
- threats that arise due to certain types of professions;
- threats that arise due to different organizational and legal forms of management (types of legal entities);
- threats associated with FIU typological studies.

How can likelihood be determined?

For random events such as terrorist attacks: vulnerability analysis for sectors, legal business forms, products and services to be used for TF, behavior analysis for radical groups that promote their interests, analysis of economic and social trends, as well as threats.

For economic events: monitoring economic indicators and trends.

Expert opinions can also be used to determine likelihood, but care should be taken to watch out for biased judgments.

How is data collected?

Data collection will deepen during NRA. Sources of information include national monitoring systems and historical archives, international databases and data from think tanks. The private sector can also be a reliable source of data and may have strong, up-to-date models for analyzing the data. The data should be collected in a harmonized format so that it can be disseminated among the NRA participants.

2.2.2. Analysis of vulnerabilities and impact consequences

How should vulnerability be assessed?

Vulnerability includes principles of impact and sustainability. People, assets and environments, sectors, business forms, products and services that are exposed to every threat should be identified.

What are the main factors to be analyzed?

Factors to be analyzed include those reported in the previous NRA Report and MONEYVAL Report, following the 5th round of mutual assessment of the Ukrainian AML/CFT system, including:

- analysis of cross-border risks, risks caused by the non-profit organizations sector and legal entities;
- detailed analysis of risks caused by fictitious enterprises, shadow economy and use of cash;
- FT risk analysis (national and intenational);
- relevance and updating of information on the beneficial ownership;
- the issue of implementation of a united administrative reporting in the AML/CFT area.

The data sources that can assist in the analysis are provided in the tables of **comprehensive administrative reporting** in the AML/CFT area (Annexes).

Other useful resources can be found in the World Development Reports[39] and OECD sustainability Systems Analysis materials[40]. sustainability trends are also important – factors such as migration, population poverty, technological changes, changes in culture and norms, factors of the national economy and its internal and external environment, may affect the AML/CFT system sustainability profile after some time or at different moments of time. A political and economic analysis should also be included.

2.2.3. Risk evaluation

How are threats and vulnerabilities compared to produce consequence assessment?

The impact of risk situations can be direct or indirect, and is best assessed with respect to the valuesof individuals, communities, and governments. To facilitate analysis, it is better to calculate the impact in monetary terms. First, assess the probable nature and extent of harm to people, assets and economy. Then, calculate this assessment by measuring the costs of responding to these shock events, either through assistance to the affected sector, population, the cost of restoring or replacing the lost or damaged assets (or insurance of assets in the risk zone), maintaining or restoring lost means of subsistence and/or repairing of or adaptation to the harm caused. Finally, economic losses must be added, including costs associated with economic damage and adverse impact on factors such as economic growth.

39 World Development Reports [Electronic resource]. – Access mode: https://openknowledge.worldbank.org/handle/10986/2124

40 sustainability Systems Analysis [Electronic resource]. – Access mode: http://www.oecd.org/dac/conflict-fragility-resilience/risk-resilience/

How about uncertainty?

Both the likelihood of threat occurrence and the possible consequence of its occurrence (or cost) are subject to uncertainty. This can be demonstrated by using ranges. For example, the impact (or cost) of a potential event can be expressed as "from UAH__ to UAH__". In the cases where uncertainty is critical, further expert examination and analysis can be useful to reduce uncertainty.

2.2.4. Risk monitoring and reassessment

How are risks to be monitored?

Risks arise, and threats evolve. In order to keep the risk assessment updated, it is useful to make the assessment a regular (periodic) event. Early warning (prevention) mechanisms for different types of risks are also important to provide a proactive response, which in most cases will be cheaper and more effective.

It may also be useful to conduct two risk assessments – one for threats that may arise in the current time frame (possibly up to 3 years) and the other one for a longer time interval. Then, each time the current risk assessment is updated, the threats that were included in the long run should be reviewed to see if they need to be moved to the current risk assessment process.

2.3. Communication and awareness of risks

An important NRA component is a communication strategy and availability of information on the risks identified to all the stakeholder groups. In view of this, it is recommended to focus on the following three aspects:

Internal and external communication

- communication on the NRA results and ensuring their use to determine the priorities of the NRA system development.

Strategies for informing the public

- implementation of communication strategies targeting the system participants, whose assets, resources, areas of responsibility are at risk.

Tools for interpreting risk analysis

- the use of tools that will make risk assessment easy to understand.

2.3.1. Internal and external communication

How and why the NRA results can be reported to politicians?

Ideally, the NRA results should be used to raise awareness of the key policy makers and corrective managerial decision-making centers in the AML/CFT systems. This can be achieved by providing results to people's deputies, ministers, SFME heads, heads of law enforcement and judicial authorities at a formal or informal session (working meeting), and by disseminating results among neighboring countries and regional associations in case of cross-border risks. Senior officials in ministries and other central executive agencies should be involved in the NRA process from the outset. Risk assessments should also be disseminated among those who were responsible for providing responses, including representatives of the REs, DNBPs, NPOs and NGOs, depending on the context.

A better knowledge of the risk profile should lead to identification of the priority action areas to enhance sustainability of the resource provision for the institutional development of the AML/CFT system and will help raise awareness of the risk among public policy actors, as well as regulatory and legal acts and standards, both at the state and sectoral levels. It should also help in communication with international organizations in the context of providing financial and/or technical assistance to Ukraine to build institutional capacity and sustainability of the national AML/CFT system.

The NRA findings should also inform the country's strategy, including the choice of policies and programs:

- identifying priorities, based on the need to address the highest-likelihood risks and most adverse consequence risks; and
- strengthening sectoral sustainability to the NRA-identified threats and vulnerabilities associated with ML/TF.

Who else should be notified about the NRA results?

The main business leaders of the private sector associations should be notified of the NRA results.

Associative structures and self-regulatory organizations can be useful in further promoting measures designed to neutralize threats and vulnerabilities in the AML/CFT system, as well as to facilitate awareness raising among the public. The private sector has strong incentives to promote institutional capacity building and risk sustainability, and may therefore be a key ally and partner in this context.

2.3.2. Strategies for informing the public

Strategy of informing the public

Risks should also be communicated to the public, focusing on the citizens who, as RE clients, should understand the need to enhance precautions and client due diligence to be implemented as part of improvements in the AML/CFT system following NRA.

Relevant reports should be supported with the necessary detailed explanations regarding the content and need of individual regulations aimed at building the institutional capacity and sustainability of the AML/CFT system, and thus at enhancing reliability and reducing reputational risks of the financial institutions which have citizens as their clients.

How should risk management roles be reported?

NRA-related research and methodological developments by the FATF, IMF, World Bank and EU Commission demonstrated that the most efficient way to manage risks is to divide them into components that form these risks (threats, vulnerabilities, and consequences). It allows managing these risks pro-actively (by preventing) and re-actively (by countering) at the proper level.

Studies evidence that one should not expect individualized solutions by individual persons to the risks identified. Such expectations create distorted incentives and may encourage excessive regulation of the sector by the relevant regulator. Instead, there is a need for a more holistic approach to risk management in the AML/CFT area, which focuses on interaction between different types of risks and between strategies intended for managing the risks identified.

As part of the risk-awareness strategy, it will be useful to report who or which ministry is responsible for managing each high-likelihood risk with a potential for substantial adverse consequences. This will help provide incentives to pay due attention to addressing these risks and help maintain public accountability.

2.3.3. Tools for interpreting risk analysis

What tools can be used to efficiently inform about NRA?

All stakeholders need clear, consistent, and clear messages to internalize information, change their understanding, and move towards appropriate mitigation measures in the context of each AML/CFT risk identified and its components.

For policy makers and for those who are responsible for communication, the risk heat matrices, through which the NRA results are visualized, can be very useful:

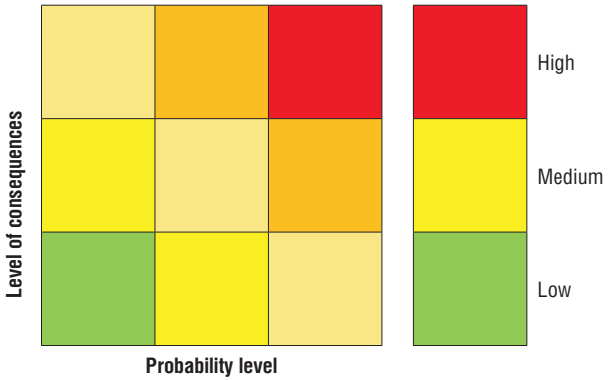


Fig. 2.3. Heat matrix of assessed risk

Інші корисні інструменти підвищення обізнаностOther helpful awareness raising tools include: theoretical and practical training; adding the risk awareness module on the risks identified and assessed following NRA to the postgraduate education curricula and advanced training of specialists in the AML/CFT area; media campaigns on introducing measures to build institutional capacity and increase the AML/CFT system sustainability; comprehensive statistical (administrative) reporting in the AML/CFT area.

2.4. Assessment of the identified risks consequences

In assessing the consequences of the risks identified, the focus is recommended to be placed on the following two aspects:

Impact assessment

- Conducting a structured, substantive assessment of the effects of the risks identified;
- NRA periodic updating.

Quantitative analysis

- Collection and dissemination of data on economic, social, political and macro- and micro-sectoral consequences of the risks identified;
- Collection and dissemination of data on the efficacy and effectiveness of the mitigating measures designed to neutralize the risks identified, build up institutional capacity, and increase the national AML/CFT system sustainability.

Why is impact assessment important?

A structured, well-planned consequence assessment of the risks identified can help identify the strengths and weaknesses of the NRA process, especially through information on:

- nature and degree of the threats identified;
- the impact of the ML/TF risks on the economy, social and political areas, on the micro and macro sectors;
- efficiency of the mitigating measures approved by the Action Plan following the previous NRA round.

Assessing potential consequences can also give impetus to the start of the NRA process, thus forming future policy and programmatic solutions in the country.

The consequences of the risks identified also provide an opportunity to assess the actual level of individual, sectoral, and institutional sustainability in the AML/CFT system, the impact of the government policies and resource support, as well as contribution of the relevant system participants to the overall system performance.

How should the consequences of the risks identified be assessed?

The NRA data in relation to the consequence assessment will be more complete if it includes details on external risks (in relation to the national AML/CFT system, Ukraine takes these risks into account, but can not reduce them without involving supranational level participants) and internal risks, as well as on extensive risks, which occur often, are localized, and have less severe consequences, and also intense (rare or innovative) risks due to rapid FinTech development.

However, the frequency of data collection and drawing of administrative reports, when developing data formats for the next NRA round, should be a matter of a reasonable compromise between all the stakeholders in the AML/CFT system in order to avoid excessive complexity and unnecessarily narrow periodicity in building the empirical basis for quantitative analysis of the phenomena and processes related to assessment of threats, vulnerabilities and consequences in the AML/CFT area.

2.5. Political and programmatic application

The use of NRA results should aim at:

- selection of the risks to be accepted, prevented, reduced, or transferred to the supranational level for their solution;
- determining priority areas for changes;
- specifying the necessary management decisions aimed at mitigating the consequences of the risks identified, neutralizing the factors that determine existence of these risks, as well as building the institutional capacity and increasing the national AML/CFT system sustainability.

How can risk assessment be used in policy setting and program development?

NRA helps:

- identify the most substantial threats and vulnerabilities in the AML/CFT system;
- identify economic, social, political and macro- and micro-sector consequences of the risks identified;
- weigh the relative costs and benefits of different strategies to mitigate the impact of the risks identified;
- prioritize measures designed to mitigate the risks identified;
- develop appropriate institutional changes and programmatic decisions for strategy implementation, including implementation of measures to build institutional capacity and increase the national AML/CFT system sustainability.

How should AML/CFT policy makers take into account the risks identified and prioritize measures to neutralize their consequences?

The analysis of the regulatory costs and benefits of introducing regulatory innovations will be a useful tool in determining whether risks should be accepted, prevented, mitigated, or transferred to the supranational level. However, regulatory losses are not the only factor to take into account. Policy makers and AML/CFT professionals should also take into account other factors that are assessed in a particular context, in particular economic, social, political, and macro- and micro-sectoral effects of the risks identified. Taken together, all these factors will help determine whether the risks assessed can be accepted or whether they require an urgent regulatory response.

How should issues related to unacceptable country risks be resolved?

Ideally, policy and programmatic decisions should aim at preventing (proactive activities) all unacceptable risks; however, this is often impossible, including due to budget restrictions. Prevention may also be institutionally impossible, especially if the risk results from external, global shock situations, cross-boundary events, or significant financial and technological innovations that are devastating to the traditional AML/CFT deterrence system.

Therefore, in most cases, optimum strategies should focus on building the sustainability of the RE, SFME, law enforcement and judicial systems in the risk area by coordinating political and programmatic work, which will include:

- capacity building for those at risk
- mitigating threats and vulnerabilities, and
- where possible, through strategies for transferring (transferring) the risk to a supranational level for resolution and settlement.

SECTION III.
NRA STAGES IN UKRAINE

Taking into account the existing NRA information analyzed in Section 1 of this Methodology and given the depth of the financial services market, peculiarities of its development, and level of corruption in Ukraine, it is advisable to combine statistical (quantitative) and qualitative methodologies, focusing on the qualitative data based on expert opinions in various AML/CFT areas.

The use of each type of data has its advantages and disadvantages, and the advantage of one may be used to supplement the disadvantages of another. While quantitative data has the advantages of being impartial, consistent, and easier to measure and compare, statistics alone is often not enough to analyze the highly complex components of the AML/CFT regime, and a generally low level of currently available AML/CFT data makes quantitative statistics difficult to rely on as the sole information source for analysis. Qualitative data has the advantage of being based on the opinions of AML/CFT experts who are familiar with the system, its complexities, and shortcomings. Qualitative data, however, may suffer from the disadvantages of relying on subjective prejudices.

Therefore, it is a combination of qualitative and quantitative data that can produce the best assessment results.

NRA in Ukraine is proposed to be conducted in four stages: preliminary stage, risk identification, analysis, risk assessment and risk management.

I. Preliminary Stage

The preliminary stage (practiced by IMF and implemented during the first NRA in Ukraine) provides for identification of specific NRA participants, designation of points of contact for each participating authority, receiving of key documents from each NRA participant, and, as appropriate, distribution and filling out of questionnaires and their subsequent analysis. Questionnaires are usually required to structure the data available to a certain NRA participant. In all instances, the authorities are not expected to generate or create new data. Rather they are asked simply to indicate which data they already have available.

The point of contact at each NRA participating authority should be willing and able to liaise with the SFMSU of Ukraine and other government agencies and data holders. The activities of the point of contact will include obtaining and submitting data via data collection tools.

Significant role in coordinating the actions of NGO participants should be played by the Council for Preventing and Countering Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of Proliferation of Weapons of Mass Destruction, established by the CMU Resolution dated 08.09.2016, No. 613. The Council is an interim consultative and advisory body of the CMU. The Council consist of: the State Financial Monitoring Service of Ukraine, the Presidential Administration of Ukraine, the Secretariat of the Cabinet of Ministers of Ukraine, the Ministry of Finance of Ukraine, the Ministry of Economic Development and Trade of Ukraine, the Ministry of Foreign Affairs of Ukraine, the Ministry of Justice of Ukraine, the Ministry of Infrastructure of Ukraine, the Ministry of Internal Affairs of Ukraine, the State Audit Service of Ukraine, the State Fiscal Service of Ukraine, the Antimonopoly Committee of Ukraine, the State Treasury of Ukraine, the State Border Guard Service of Ukraine, the State Regulatory Service of Ukraine, the Foreign Intelligence Service of Ukraine, the Prosecutor General's Office of Ukraine, the Security Service of Ukraine, the National Securities and Stock Market Commission, the National

Financial Service Markets Regulation Commission, the National Anti-Corruption Bureau of Ukraine, the Secretariat of National Security and Defense Council of Ukraine, the National Bank of Ukraine, the High Specialized Court of Ukraine for Civil and Criminal Cases, the League of Insurance Organizations of Ukraine, the Association of Ukrainian Banks, the Association «The independent Association of Ukrainian banks».

II. Risk identification stage

At the stage of risk identification, it is necessary to determine the AML/CFT system threats and vulnerabilities.

The risk identification process begins with compiling a list of possible threats or threat factors derived from the known or likely threats or vulnerabilities caused by the main payment methods, means, and mechanisms used, as well as a list of the key sectors used for these purposes, and main reasons why the ML cases are not investigated and money launderers are not arrested, apprehended, and deprived of their assets and property.

Identification of threats and vulnerabilities may be informed, e.g., by materials of international organizations (including the latest MONEYVAL mutual assessment report for Ukraine), typologies, reports from law enforcement and judicial authorities, information and analytical materials and administrative data from SFME and other AML/CFT state authorities, as well as of research organizations and associations of reporting entities, interviews (surveys) with officials of law enforcement authorities, SFME, self-regulatory organizations, private sector.

Threat identification should be carried out using the following structure (where the appropriate data is available):

1. Evaluation of the scale and nature of socially dangerous acts that precede ML:
   - identifying the key types of socially dangerous acts that precede ML;
   - identifying the number of criminal cases related to socially dangerous acts;
   - identifying the regional distribution of criminal cases related to socially dangerous acts;
   - the scale and nature of terrorist activities and terrorist groups in the country;
   - the scale and nature of terrorist activities and terrorist groups in the neighboring countries, regions and sub-regions.
2. Evaluation of the scope of proceeds of crime:
   - identifying the scope of the proceeds that are objects of criminal cases related to socially dangerous acts;
   - form of the proceeds (assets and property or the right of their ownership) obtained by committing of a socially dangerous act;
   - identifying the scope of the proceeds obtained by committing socially dangerous acts;
   - duration of the period when the proceeds of crime were in existence;
   - location of the proceeds of crime;
   - owner of the proceeds of crime;
   - sources of origin of the proceeds of crime;
3. Identifying the tools, methods, and ways aimed at concealing or disguising the illegal origin of the proceeds (typology):
   - identifying the ML tools – the type of the asset used for ML;
   - identifying the ML methods – the action on the type of the asset used for ML;
   - identifying the ML ways – action to disguise the sources of origin of the proceeds.

- identifying the characteristics of the person involved in ML;
- identifying the locations of legalized proceeds;
- identifying the ML time and its duration.

4. Identifying the actual scope of legalized means:
   - identifying the scope of legalized means;
   - identifying the number of criminal cases related to ML;
   - identifying the scope of most popular forms of legalized proceeds;
   - identifying the whereabouts of laundered proceeds;
   - identifying the owners of laundered proceeds;

Following review of information, a list of external and internal threats is drawn up; also, it is advisable to consider drawing up a list of intense (random, substantial, one-off) and extensive (multiple) threats.

External threats are formed outside the AML/CFT system and cannot be countered only through the national financial monitoring system participants' efforts.

External threats can cover any events on the financial market or in the economy and are specifically related to:

- emergence of new financial products and/or services;
- emergence of new financial institutions and/or intermediaries;
- stepped up activities of organized crime groups;
- commitment of predicate or other crimes;
- commitment of illegal activities;
- increased level of economic crime.

Internal threats are formed inside the AML/CFT system and are countered by the financial monitoring system participants' own efforts.

Internal threats may cover events related to the functioning of the AML/CFT system, namely:

- absence of intention to improve the regulatory framework or significant time asymmetry in implementation of the updated international AML/CFT standards;
- insufficient regulation and supervision of the reporting entities;
- absence or irrelevance of programs aimed at improving the knowledge of all the AML/CFT system participants.

Based on the analysis of the threats identified, the AML/CFT system **vulnerabilities** are determined.

1. Identifying vulnerable areas of the financial sector:
   - identifying vulnerable areas of financial assets for ML;
   - identifying adequacy of client identification procedures;
   - identifying efficiency of procedures for detection of suspicious financial transactions;
   - identifying completeness of the system for informing the FIU and law enforcement agencies on suspicious transactions;
2. Identifying vulnerable areas of the non-financial sector:
   - identifying vulnerable areas of DNFBP to ML;
   - identifying adequacy of client identification procedures among DNFBP;
   - identifying efficiency of procedures for detection of suspicious financial transactions by DNFBP representatives;
   - identifying completeness of the system of informing the FIU and law enforcement agencies by DNFBP on suspicious transactions;

3. Identifying gaps in supervision over REs:
   - identifying efficiency of the system of sanctions for violations of the AML/CFT legislation;
   - preventing criminals and/or criminal organizations from establishing control over REs;
   - RE identification and verification of the data on the ultimate beneficial owner (controller), his business reputation, source of origin of wealth and funds which formed the authorized capital, etc.
4. Identifying gaps in the financial investigation process:
   - identifying a possibility of obtaining information from financial institutions and DNFBPs;
   - assessment of timeliness of obtaining information from financial institutions and DNFBPs;
5. Identifying gaps in the criminal proceeding and justice process:
   - identifying a possibility of obtaining evidence for criminal proceedings;
   - assessment of the speed of the criminal proceedings;
   - identifying the number of criminal cases and court decisions.

According to the FATF Methodology, special attention should be paid to the risk assessment of the use of legal entities and non-profit organizations for ML/FT.

The risk assessment of using various types of legal entities (organizational and legal forms of management) – reporting entities clients' in conducting ML and FT operations through them is carried out by the SFME through interviews of supervised reporting entities. During interviewing of supervised reporting entities, special attention should be paid to the following issues:

- what organizational and legal forms of management (types of legal entities) occupy the largest share among the reporting entities clients;
- in which organizational and legal forms of management (types of legal entities) that are clients, beneficial owners presented high-risk individuals (PEPs, high-risk countries);
- to what organizational and legal forms of management (types of legal entities) that are clients, reporting entities high risk is set;
- financial transactions of which organizational and legal forms of management (types of legal entities), which are clients, have caused suspicion of reporting entities, and information of which was submitted to the FIU;
- what legal and organizational forms of management (types of legal entities) reporting entities was refused to establish business relations/conducting financial transactions;
- other issues that may affect the risk assessment of the use of legal entities for the ML/FT purpose.

Non-profit organizations risk assessment use for ML/FT is carried out by the FIU jointly with the law enforcement authorities (the State Fiscal Service of Ukraine, the Security Service of Ukraine, the Prosecutor General's Office of Ukraine).

During risk assessment of using non-profit sector for ML/FT, a review of the non-profit sector is used, which is periodically conducted by the FIU, and special attention is paid to analyzing the following issues:

- non-profit sector structure;

- number of received STRs from reporting entities by the FIU (in the context of signs), participants of which are non-profit organizations;
- specification of STR signs with the participation of non-profit organizations;
- refusal to conduct financial transactions with the participation of non-profit organizations to reporting entities;
- case referrals submission to the FIU, concerning financial transactions with the participation of non-profit organizations to law enforcement authorities;
- etc.

The identification stage should be dynamic to ensure the possibility of addressing new or previously unidentified risks and their factors at any stage of the assessment process.

III. Risk Analysis

Analysis is the main NRA stage. It determines the nature, sources, likelihood and consequences of the threats and vulnerabilities identified.

The objective of this stage is to obtain comprehensive understanding of each risk, which is a combination of threat, vulnerability and consequences, in order to assign some sort of relative values.

Risk analysis takes into account the relevant nature and sources of risk pertinent to the overall situation and conditions in the country in the broadest sense, which influence how risks evolve. Such factors include political, economic, geographical and social aspects, as well as other structure-shaping factors and specific circumstances for risk existence.

The probability analysis consists in determining the likelihood that a possible risk will occur regardless of the available measures currently taken to prevent or reduce such a risk.

The likelihood should be determined and referred to one of the following categories:

- **low** (the chances for risk occurrence are virtually non-existent, but it cannot be maintained that they are absent altogether);
- **medium** (there is likelihood of risk occurrence under the circumstances, but the frequency of this risk occurrence is low);
- **high** (the probability of risk occurrence under the circumstances and the frequency of this risk occurrence are high).

Analysis of consequences requires full understanding of the consequences associated with the above activity, which will assist in reaching conclusions about the relative importance of each identified risk. The consequences of this illicit financial activity are often viewed at the national or international level but also affect the regional, local and individual levels.

Both impacts and harm (which are constituents of consequences) can be further categorized into types, such as physical, social, environmental, economic and structural. From a national perspective, one of the main ML and TF consequences is their negative effect on transparency, good governance and accountability of public and private institutions.

Analysis of consequences involves determining the severity of harm or potential losses, which may occur if a possible risk occurs.

The consequences should be referred to one of the following categories: **low; medium; high.**

Risk categorization also differentiates them by their impact on the economy, financial system, and society, i.e. identification of direct and indirect consequences (a detailed overview is provided in Section 1 of this Methodology).

IV. Risk Assessment and Management

The evaluation stage consists in determining (based on the results of the previous NRA stages) the following threat-specific characteristics:

- overall risk level;
- efficiency of the measures currently taken to prevent or mitigate the risk;
- net risk level.

The overall risk level is calculated using the formula: **"overall risk level = the level of the consequences of a risk event occurrence * the level of likelihood of a risk event occurrence"** and has the form of the following heat table/matrix:

Likelihood				
	High likelihood = 3	3	6	9
	Medium likelihood = 2	2	4	6
	Low likelihood = 1	1	2	3
		Low - 1	Medium - 2	High - 3
		Consequences		

Fig. 3.1. Overall risk level matrix

Thus, the overall risk level may have the following grades:

Overall risk level	
1	**Low** (the risk will most likely not occur and, if occurs, will have low consequences) (1-3 points)
2	**Medium** (the risk may likely occur with medium consequences) (4-6 points)
3	**High** (the risk exists with high consequences) (7-9 points)

Fig. 3.2. Overall risk level scale

Once the overall risk level is determined, the available measures currently taken in Ukraine to prevent or mitigate the risk are identified and assessed for their efficiency and to determine vulnerability to the risk and a corresponding **net risk level**.

Efficiency of the currently taken preventive or mitigating measures should be determined and referred to one of the following categories:

- **effective measures** – measures have been developed in the required scope, documented, and their implementation is regularly controlled; cases of not implementing or of inadequate implementation have not been identified; regular and detailed trainings take place. **The risk is mitigated by more than 75%;**
- **improving measures** – measures have been developed, but not all of them; some measures have been documented; implementation of the measures is controlled, but not regularly. Trainings take place, but are not regular. **Risk mitigation from 75% to 50%** due to the increased negative impact of the above descriptive characteristics

related to development of the regulatory measures;

- **unreliable measures** – most measures have not been developed or documented; the facts of documented measures are absent or sporadic; implementation of the measures is not controlled or almost not controlled; absence of developed measures; absence of trainings. **Risk level does not mitigate** due to the increased negative impact of the above descriptive characteristics related to development of the regulatory measures.

According to the results of the measures effectiveness assessment that are currently being taken in Ukraine to prevent or reduce risk, each category of measures is assigned a score:

Effectiveness of measures	
1	Effective measures
2	Improving measures
3	Unreliable measures

The net risk level is calculated using the formula: "net risk level = overall risk level * efficiency of available measures" and takes the form of the following table/matrix:

		Net risk level		
Overall risk level	High = 3	3	6	9
	Medium = 2	2	4	6
	Low = 1	1	2	3
		Effective = 1	Improving = 2	Ненадійні = 3
		Effectiveness of the available measures		

Fig. 3.3. Net risk level matrix

Net risk level	
7-9	High
4-6	Medium
1-3	Low

The results thus obtained are consolidated into the following table/matrix:

Table 3.1. Recording the NRA results

No.	Threat	Vulnerability	Level of risk likelihood occurrence	Comments on the level of risk likelihood occurrence	Risk manifestation consequences level	Comments on risk manifestation consequences level	General risk level	Mitigation measures effectiveness level	Comments on mitigation measures effectiveness level	Net risk level
Identified risk										

Scope of Financial, Material, Technical, and Human Resources

NRA implementation should be funded from the costs allotted to its relevant participants under the Law on the State Budget for the appropriate year and other sources provided for by legislation.

The scope of funding, material, technical, and human resources required for NRA implementation should be determined during the preceding year with due regard for the state budget capabilities and involvement of international technical assistance.

Challenges still to be addressed

Gathering and analyzing information is a fundamental basis for risk assessment, as well as for the development and measurement of appropriate actions to build institutional capacity and improve the AML/CFT system sustainability. Very often, information and analysis are fragmented between different forms of data systems (monitoring and early warning, assessment, impact analysis, and cost-benefit analysis systems) that are pursued on different scales, in different time frames, and involving a multitude of uncoordinated parties. In addition, an overall analysis of how sector-level threats and vulnerabilities affect formation of cumulative national AML/CFT risks is done very rarely.

Thus, the problem is how to construct a general analysis system which, based on an approach focused on absorbing the maximum possible and appropriate set of data, will combine and populate three key dimensions of data collection and analysis for a meaningful NRA and for implementation of an effective and efficient risk-based approach in the national AML/CFT system:

- fusion of different data and analysis forms: a combination of surveillance, early warning, assessment, and analysis of the negative consequences of the risks identified;
- combination of different subject areas: synthesis of risk analysis in the AML/CFT area;
- use of data and analyses with different parameters: information that may vary by:

- scale (from the self-employed to the global level);
- time frames (from daily information on suspicious financial transactions coming from the RE to reviewing global trends of economic development, financial markets, regulatory and supervisory institutes and institutions;
- coordination and synthesis of analytical information from a large number of stakeholders, entities with thematic, sectoral, and global mandates and methods for collecting relevant data.

SECTION IV. SECTORAL ML/TF RISK ASSESSMENT

4.1. General aspects of sectoral risk assessment

Scope of application

For NRA purposes, sectors are defined in accordance with the provisions of the Law. In particular, based on the reference definition of the "financial monitoring" concept, provided in Clause 48, Part 1, Art. 1 of the Law, AML/CFT measures are carried out both at the SFME and at the RE level. At the same time, consideration was given to provisions of Part 2, Art. 5 of the Law, which define the exhaustive list of the RE, and provisions of Art. 14 of the Law, which govern the issues of state regulation and supervision in the AML/CFT area, by assigning a corresponding RE category to each SFME; also, obligation were specified for each SFME to perform regulation and supervision, taking into account of AML/CFT risk assessment to determine appropriateness of the measures carried out by RE to mitigate the existing risks in their professional activities (Clause 3, Part 2, Article 14 of the Law).

A separate block of sectoral risk assessment is devoted to analysis of comprehensive administrative reporting indicators in the context of all the state authorities which are participants of the national AML/CFT system, including law enforcement and judicial systems.

Sectoral risk assessment model

International risk management standards, specifically FATF guidances, define risk as a function of likelihood of negative events. The occurrence likelihood of these events is a function of coexistence of a threat and vulnerability to this threat. In other words, risk events occur when threat exploits vulnerability and breeds negative consequences:

$$\boldsymbol{R = f[(T), (V)] \times C}, \text{ where}$$

R – risk function; T – factor (variable) associated with the threat identified; V – factor (variable) associated with the vulnerability identified; C – a factor associated with negative consequences caused by coexistence of threats and vulnerabilities.

The proposed sectoral risk assessment model uses the FATF guidances on risk assessment methodology and is based on numerous international risk assessment recommendations in various sectors that are presented by a wide range of REs.

At the same time, the methodology for assessing the ML risk and the TF risk in the corresponding sector is different, first of all, in the specifics of threats, vulnerabilities, and consequences advised to be analyzed and assessed by each SFME with respect to the RE sector under its supervision. The specified distinction is made to avoid mixing of two different risk mitigation environments in the overall risk level.

Gathering information

Sources of information for assessment of sectoral ML and TF risks include data templates designed to generalize the status and dynamics of the quantitative assessment criteria in the context of the SFME functionality (**Annex 3**), law enforcement agencies (**Annex 4**) and the judicial system (**Annex 5**) in the AML/CFT area.

Corroborating information

For further consultations and discussion of the issues related to ensuring reliability

assessment of the findings on identified threats, vulnerabilities and their consequences in the aforementioned sectoral context (SFME, law enforcement authorities and judicial system), the SFMSU as the NRA coordinator initiated and submitted the issue of establishing a Sectoral Risk Assessment Working Group in the AML/CFT system (the Working Group) for consideration of the 4th Meeting of the Council for Preventing and Countering Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of Proliferation of Weapons of Mass Destruction (the Council). The Provision on the Working Group was approved by the decision of the 4th Council Meeting of 16.02.2018.

The main tasks of the Working Group are:

- analyze information on the activities of financial monitoring entities, state agencies involved in the AML/CFT system operation;
- resolve challenges that arise in identifying ML/TF risks (threats), analyze, assess and develop measures aimed at preventing and/or reducing negative consequences;
- review proposals for improving the NRA methodology conducting;
- analyze the ML and TF impact on the society, social relations, and financial and economic system to identify appropriate measures to prevent and counter the existing threats;
- discuss issues related to the development of comprehensive administrative reporting in the AML/CFT area.

The Working Group includes: the State Financial Monitoring Service of Ukraine, the Ministry of Finance of Ukraine, the Ministry of Economic Development and Trade of Ukraine, the Ministry of Justice of Ukraine, the Ministry of Infrastructure of Ukraine, the National Bank of Ukraine, the National Securities and Stock Market Commission, the National Financial Service Markets Regulation Commission, the Ministry of Internal Affairs of Ukraine, the State Fiscal Service of Ukraine, the Prosecutor General's Office of Ukraine, the State Property Fund of Ukraine, the National Agency of Ukraine for finding, tracing and management of assets derived from corruption and other crimes, the National Police of Ukraine, the National Anti-Corruption Bureau of Ukraine.

Structure

The NRA report should take into account the results of the sectoral risk assessment and, in view of this, it is advisable to present it in following components:

1. Internal threats general overview;
2. External treates general overview;
3. Overview of the national sectors in AML/CFT area represented by the relevant reporting entities categories. The above review is carried out by the SFMEs in relation to those reporting entities whose activities they regulate and supervise. When forming this review, it is strongly recommended that the SFMEs use the developed and agreed administrative reporting template provided in **Annex 3** (for quantitative sector assessment), as well as **the qualitative scoring methodology** for assessing sectoral ML and TF risks, described in **Para 4.2 and 4.3, Section 4** of this Methodology respectively. The final scores for assessing the private sector risks should be broken down into three components: threat, vulnerability and consequences – separately for ML and TF.
4. Review of the overall contribution of the law enforcement agencies to the effectiveness and efficiency of the national AML/CFT system operation. When

developing the review, the law enforcement agencies are strongly advised to use the developed and agreed template for administrative reporting, provided in **Annex 4**.

5. Review of the overall contribution of the judicial system to the effectiveness and efficiency of the national AML/CFT system operation. When developing the review, it is strongly advised to use the developed and agreed template for administrative reporting, provided in **Annex 5**.
6. Overview of the legal forms and formations sector (various organizational and legal forms of legal entities pursuing their activities in Ukraine).

4.2. Qualitative scoring methodology for assessing sectoral ML risks

The sectoral ML risk assessment methodology covers 21 risk factors in three categories: nature of the threat from crime, vulnerability and consequences. Each risk factor should be analyzed and rated on a scale from 1 to 9. Each risk factor should be assigned an appropriate rating – low, medium or high (as shown in the tables below). The analysis and assessment should be based on the results of professional analysis and judgments of the relevant SFMEs regarding the RE sectors subordinated to and regulated by them.

It is proposed to consider five risk factors that should be taken into account when assessing threats from crime. The average rating of these five factors generates an overall assessment for the "Threat" module.

To assess the overall sector ML vulnerability, 12 factors are proposed for consideration and assessment. The relevant factors are grouped into five subsections: preventive measures; regulation; national interaction and coordination; relations with high-risk countries; and transparency and accountability for the movement of funds. The average of these 12 factors generates an overall assessment for the "Vulnerability" module.

Four factors are proposed for consideration when assessing the ML consequences to assess the relevant sector. The average of these 4 factors generates an overall assessment for the "Consequences" module.

Threats

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Simple ML methods are used	Relatively complex ML methods are used	Very complex ML methods are used
from 1 to 9	There is only a threat of internal (national) crime	Predominantly, there is an internal threat of crime with some involvement of non-resident accomplices	There is an internal threat of crime with significant involvement of non-resident accomplices
from 1 to 9	Lack or minimal focus of serious organized criminal groups on the sector (suspected or proven fact)	A certain focus of serious organized criminal groups on the sector (suspected or proven fact)	Significant or systematic focus of serious organized criminal groups on the sector (suspected or proven fact)
from 1 to 9	ML cases in the sector are absent or isolated	Moderate number of ML cases in the sector	Substantial number of ML cases in the sector
from 1 to 9	Minimum impact of ML-related predicate crimes	Medium impact of ML-related predicate crimes	Substantial impact of ML-related predicate crimes

AVERAGE SCORE	from 1 to 9

Vulnerabilities

Preventive measures

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Most REs have a good understanding of their ML risks and relevant mitigation programs	Some REs have a good understanding of their ML risks and relevant mitigation programs	Few REs have a good understanding of their ML risks and relevant mitigation programs
from 1 to 9	Most REs reliably and duly verify their staff honesty/integrity.	Some REs reliably and duly verify their staff honesty/integrity.	Few REs reliably and duly verify their staff honesty/integrity.
from 1 to 9	Most of the sector's REs have systems and procedures to validate legitimacy of their clients, their UBOs, their associates and related individuals.	Some of the sector's REs have systems and procedures to validate legitimacy of their clients, their UBOs, their associates and related individuals.	Few of the sector's REs have systems and procedures to validate legitimacy of their clients, their UBOs, their associates and related individuals.

Regulation

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	The sector's REs operate within the regulatory framework that is strong and compliant with the AML international standards; the level of risk-based regulation and supervision is high	The sector's REs operate within the regulatory framework that is medium and partly compliant with the AML international standards; the level of risk-based regulation and supervision is high	The sector's REs operate within the regulatory framework that is weak and non-compliant with the AML international standards; the level of risk-based regulation and supervision is high
from 1 to 9	SFME broadly covers the supervised REs with inspections and actively participates in mitigating the ML risk in the sector.	SFME partly covers the supervised REs with inspections and periodically participates in mitigating the ML risk in the sector.	SFME has limited coverage of the supervised REs with inspections and does not participate in mitigating the ML risk in the sector.
from 1 to 9	It is difficult to establish a fictitious RE	There are some difficulties in establishing a fictitious RE	It is possible to establish a fictitious LSFM.

National cooperation and coordination

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	National cooperation and coordination between the SFME-regulator, SFMSU, and law-enforcement authorities in the context of ML prevention and counteraction are mostly efficient with a small number of necessary improvements.	National cooperation and coordination between the SFME-regulator, SFMSU, and law-enforcement authorities in the context of ML prevention and counteraction are predominantly efficient, but some improvements are necessary.	National cooperation and coordination between the SFME-regulator, SFMSU, and law-enforcement authorities in the context of ML prevention and counteraction are inconsistent and not always efficient.

Connection to high-risk countries

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	A limited number of REs pursue their activities with partners from high-risk ML countries	A moderate number of REs pursue their activities with partners from high-risk ML countries	A significant number of REs pursue their activities with partners from high-risk ML countries
from 1 to 9	REs effect financial transactions in insignificant absolute and relative volumes with counterparts from high-risk ML countries	REs effect financial transactions in medium absolute and relative volumes with counterparts from high-risk ML countries	REs effect financial transactions in significant absolute and relative volumes with counterparts from high-risk ML countries

Cash flow transparency and accountability

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Most of the sector's REs have strong domestic practices for UBO transparency and accountability in identifying the sources of funds and the clients' wealth.	Half of the sector's REs have strong domestic practices for UBO transparency and accountability in identifying the sources of funds and the clients' wealth.	Few of the sector's REs have strong domestic practices for UBO transparency and accountability in identifying the sources of funds and the clients' wealth.
from 1 to 9	High-risk financial transactions are rarely effected	High-risk financial transactions are effected non-systematically	High-risk financial transactions are effected systematically
from 1 to 9	Most REs have strong national practices for identification of national politically exposed persons, their associates and related persons	A medium number of REs have strong national practices for identification of national politically exposed persons, their associates and related persons	Few REs have strong national practices for identification of national politically exposed persons, their associates and related persons

AVERAGE SCORE	from 1 to 9

Consequences

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Criminal use has a minimum impact on the reputation, financial performance and activities of the sector's REs	Criminal use has a moderate impact on the reputation, financial performance and activities of the sector's REs	Criminal use has a substantial impact on the reputation, financial performance and activities of the sector's REs
from 1 to 9	Criminal use has a minimum impact on potential beneficiaries and/or individuals associated with the sector's REs	Criminal use has a moderate impact on potential beneficiaries and/or individuals associated with the sector's REs	Criminal use has a substantial impact on potential beneficiaries and/or individuals associated with the sector's REs
from 1 to 9	Criminal use of the sector's REs has a minimum impact on the Ukrainian economy, politics and society	Criminal use of the sector's REs has a moderate impact on the Ukrainian economy, politics and society	Criminal use of the sector's REs has a substantial impact on the Ukrainian economy, politics and society
from 1 to 9	Criminal use of the sector's REs does not impact national and/or international security	Criminal use of the sector's REs has a potential of a moderate impact on national and/or international security	Criminal use of the sector's REs has a potential of a substantial impact on national and/or international security

In determining the level of the sectoral ML risk, the SFME assessment should not be limited to the factors outlined in the table above. The table is a basic (minimum) reference template for organizing the necessary information for a qualitative scoring assessment.

Among other things, SFME should further elaborate on the following sector's characteristics:

- completeness and efficiency of the sector's legal regulation on the ML issues;
- general overview of the crime situation in the sector in the ML context;
- the status of implementation by the supervised REs of the legislative requirements for preventing and countering ML;
- efficiency of regulation and supervision of the REs on the ML issues;
- typical ML schemes using the sector's REs;
- any other information that would be useful for understanding of the sector risks.

The results of a qualitative scoring assessment of the sector received by the SFMEs should be logically grounded by means of the template described in Table 3.1.

A separate issue of sector risk assessment (based on recommendations of the Council of Europe MONEYVAL experts recorded in the Fifth Round Mutual Evaluation Report) should be **risk assessment of the use of different types of legal entities (organizational and legal business forms) – RE clients – in effecting ML transactions through them**.

In view of the above, it is advisable for SFME to conduct an appropriate national survey among the supervised REs of the relevant sector. In this case, the questionnaire should cover all the organizational and legal business forms approved by the State Committee of Ukraine on Technical Regulation and Consumer Policy Order dated 28.05.2004, No. 97 (as amended and supplemented)[41].

41 Classification of organizational and legal businesses forms [Electronic resource]. – Access mode: http://www.ukrstat.gov.ua/klasf/nac_kls/op_dk002_2016.htm

4.3. Qualitative scoring methodology for assessing sectoral TF risks

During conducting FT risk assessment, the main widely recognized FT methods should be taken into account:

- fundraising;
- transfer of funds;
- use of funds.

The process of identification, assessing and understanding the risk of each of these methods is based on the results of previous cases of terrorism manifestation conducted by individuals or organizations which are within the relevant jurisdiction or related one, and the study of the financial needs of these individuals and organizations to formulate conclusions on the probability of using each of the FT methods.

The FT risk assessment suggests the need for research and analysis of the following issues:

- FT crimes investigation;
- prosecution of persons who have committed an FT crime;
- use of effective, proportionate and compelling sanctions by courts to the persons convicted for FT;
- coordination between the relevant authorities.

With the aim to effectively studying and analyzing identified issues, by the relevant law enforcement authorities that carry out activities aimed at combating FT, conducting surveys, interviews with individuals directly involved in the investigation and prosecution of FT crimes.

The TF risk assessment methodology covers 21 risk factors in three categories: TF threat environment, vulnerabilities and consequences. It is recommended that each risk factor be analyzed and rated on a scale from 1 to 9. Each should be assigned an appropriate rating – low, medium or high (as shown in the tables below). The analysis and assessment should be based on the results of professional analysis and judgments of the relevant SFMEs regarding the RE sectors subordinated to and regulated by them.

It is proposed to consider three risk factors in assessing the TF threat environment. The average rating of these three factors generates an overall assessment for “Threat”. Twelve factors are proposed to be considered when assessing the overall vulnerability of the sector to TF. The said factors are grouped into five subsections: preventive measures; regulation; national cooperation and coordination; relations with high-risk countries; and transparency and accountability for the movement of funds. The average rating of these fifteen factors generates an overall score for “Vulnerabilities”. Five factors should be considered when assessing the consequences of terrorist financing activities for a sector. The average rating of these five factors generates an overall score for “Consequences”.

TF threat environment

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Link between Ukraine and jurisdictions that have a high risk of terrorism is absent.	Link between Ukraine and jurisdictions that have a high risk of terrorism is insignificant.	Link between Ukraine and jurisdictions that have a high risk of terrorism is significant.
from 1 to 9	Simple methods are used	Relatively complex methods are used	Very complex methods are used
from 1 to 9	Limited focus of terrorist groups, networks, units or individual militants on the sector (suspected or proven fact)	Moderate focus of terrorist groups, networks, units or individual militants on the sector (suspected or proven fact)	Substantial and systematic focus of terrorist groups, networks, units or individual militants on the sector (suspected or proven fact)
from 1 to 9	No TF cases related to involvement of the sector's REs (suspected or proven fact)	A moderate number of TF cases related to involvement of the sector's REs (suspected or proven fact)	A substantial number of TF cases related to involvement of the sector's REs (suspected or proven fact)

Vulnerabilities

Preventive measures

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Most state authorities have an adequate understanding of FT risks and relevant programs to mitigate them	Some state authorities have an adequate understanding of FT risks and relevant programs to mitigate them	A small amount of state authorities have an adequate understanding of FT risks and relevant programs to mitigate them
from 1 to 9	Most of the sector's REs have an adequate understanding of their TF risks and relevant mitigation programs	Some of the sector's REs have an adequate understanding of their TF risks and relevant mitigation programs	Few of the sector's REs have an adequate understanding of their TF risks and relevant mitigation programs
from 1 to 9	Most of the sector's REs perform reliable and due diligence of their clients based on the current lists of terrorists and sanctioned persons.	Some of the sector's REs perform reliable and due diligence of their clients based on the current lists of terrorists and sanctioned persons.	Few of the sector's REs perform reliable and due diligence of their clients based on the current lists of terrorists and sanctioned persons.
from 1 to 9	Most of the sector's REs have systems and procedures to validate legitimacy of their clients, their UBOs, their associates and related individuals.	Some of the sector's REs have systems and procedures to validate legitimacy of their clients, their UBOs, their associates and related individuals.	Few of the sector's REs have systems and procedures to validate legitimacy of their clients, their UBOs, their associates and related individuals.

Regulation

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	The sector's REs operate within a regulatory framework that is strong and compliant with the CFT international standards; the level of risk-based regulation and supervision is high	The sector's REs operate within a regulatory framework that demonstrates medium and partial compliance with the CFT international standards; the level of risk-based regulation and supervision is high	The sector's REs operate within a regulatory framework that is weak and non-compliant with the CFT international standards; the level of risk-based regulation and supervision is high
from 1 to 9	SFME broadly covers the supervised REs with inspections and actively participates in mitigating the TF risk in the sector.	SFME partly covers the supervised REs with inspections and periodically participates in mitigating the TF risk in the sector.	SFME has limited coverage of the supervised REs with inspections and does not participate in mitigating the TF risk in the sector.
from 1 to 9	It is difficult to establish a fictitious RE	There are some difficulties in establishing a fictitious RE	It is possible to establish a fictitious LSFM.

National cooperation and coordination

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	National cooperation and coordination between the SFME-regulator, SFMSU, and law-enforcement authorities in the context of TF prevention and countering are mostly efficient with a small number of necessary improvements.	National cooperation and coordination between the SFME-regulator, SFMSU, and law-enforcement authorities in the context of TF prevention and countering are moderately efficient, but some improvements are necessary.	National cooperation and coordination between the SFME-regulator, SFMSU, and law-enforcement authorities in the context of TF prevention and countering are inconsistent and not always efficient.

Connection to high-risk countries

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	A limited number of REs pursue their activities with partners from high-risk TF countries	A moderate number of REs pursue their activities with partners from high-risk TF countries	A significant number of REs pursue their activities with partners from high-risk TF countries
from 1 to 9	REs effect financial transactions in insignificant absolute and relative volumes with counterparts from high-risk TF countries	REs effect financial transactions in medium absolute and relative volumes with counterparts from high-risk TF countries	REs effect financial transactions in significant absolute and relative volumes with counterparts from high-risk TF countries

Cash flow transparency and accountability

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	Most of the sector's REs have strong domestic practices for UBO transparency and accountability in identifying the sources of funds and the clients' wealth.	Half of the sector's REs have strong domestic practices for beneficial ownership transparency and accountability in identifying the sources of funds and the clients' wealth.	Few of the sector's REs have strong domestic practices for UBO transparency and accountability in identifying the sources of funds and the clients' wealth.
from 1 to 9	High-risk financial transactions are rarely effected	High-risk financial transactions are effected non-systematically	High-risk financial transactions are effected systematically
from 1 to 9	Most REs have strong national practices for identification of national politically exposed persons, their associates and related persons	A medium number of REs have strong national practices for identification of national politically exposed persons, their associates and related persons	Few REs have strong national practices for identification of national politically exposed persons, their associates and related persons

Consequences

EVALUATION	LOW (1-3 points)	MEDIUM (4-6 points)	HIGH (7-9 points)
from 1 to 9	TF has a minimum impact on the reputation, financial performance and activities of the sector's REs	TF has a moderate impact on the reputation, financial performance and activities of the sector's REs	TF has a substantial impact on the reputation, financial performance and activities of the sector's REs
from 1 to 9	TF has a minimum impact on potential beneficiaries and/or individuals associated with the sector's REs	TF has a moderate impact on potential beneficiaries and/or individuals associated with the sector's REs	TF has a substantial impact on potential beneficiaries and/or individuals associated with the sector's REs
from 1 to 9	TF by the sector's REs has a minimum impact on the Ukrainian economy, politics and society	TF by the sector's REs has a moderate impact on the Ukrainian economy, politics and society	TF by the sector's REs has a substantial impact on the Ukrainian economy, politics and society
from 1 to 9	TF by the sector's REs does not impact national and/or international security	TF by the sector's REs has a potential of a moderate impact on national and/or international security	TF by the sector's REs has a potential of a substantial impact on national and/or international security

AVERAGE SCORE	from 1 to 9

In determining the level of the sectoral TF risk, the SFME assessment should not be limited to the factors outlined in the table above. The table is a basic (minimum) reference

template for organizing the necessary information for a qualitative scoring assessment.

Among other things, SFME should further elaborate on the following sector's characteristics:

- completeness and efficiency of the sector's legal regulation on the TF issues;
- general overview of the crime situation in the sector in the TF context;
- the status of implementation by the supervised REs of the legislative requirements for preventing and counteracting TF;
- efficiency of regulation and supervision of the REs on the TF issues;
- typical TF schemes using the sector's REs;
- any other information that would be useful for understanding of the sector risks.

A separate issue of sector risk assessment (based on recommendations of the Council of Europe MONEYVAL experts recorded in the Fifth Round Mutual Evaluation Report) should be **risk assessment of the use of different types of legal entities (organizational and legal business forms) – RE clients – in effecting TF transactions through them**.

SECTION V. PROTECTION AND INFORMATION USE

The information exchange during NRA is carried out in compliance with the requirements for the information protection which belongs to the restricted access information category.

Participants should guarantee the protection of restricted access information obtained during the NRA.

The information used during conducting the NRA is used solely for official purposes. Access to it by third parties is carried out in cases provided for by law. The receiving party is responsible for accessing, storing and protecting the information in accordance with the law.

Depending on the information contained in the NRA report, access to it may be fully or partly restricted.

In case the NRA report contains information with restricted access, the FIU makes a decision to prepare a public version of the NRA report that will be made public on the basis of the NRA report.

The FIU ensure the protection and storage of restricted access information obtained during the NRA process, and on the basis of which conclusions are drawn on the threats, vulnerabilities and risks of the AML/CFT system.

ANNEXES

Annex 1. Data collection template to conduct a general review of the environment of the Ukrainian AML/CFT system functioning.

Annex 2. Data collection template that FIU fulfill.

Annex 3. Data collection template that fulfills each SFME based on its sector (supervised by them types of reporting entities).

Annex 4. Data collection template by the law enforcement and intelligence authorities.

Annex 5. Data collection template on the judicial system.

Annex 6. Excerpts from Ukrainian recommendations according to experts' conclusions.

ANNEX 1. GENERAL COMPONENT

№	INDICATOR	2013	2014	2015	2016	2017	2018
General characteristics of Ukraine							
1	Population, persons						
2	Total area, sq. km						
3	Coastline, km						
4	The length of the land border, km						
5	Inland waterways, km						
6	Ports and trade terminals, units						
7	Road cover, km						
8	Railway coverage, km						
9	The number of individuals-entrepreneurs in terms of administrative (territorial) divisions of Ukraine						
10	The number of legal entities in terms of administrative (territorial) divisions of Ukraine						
11	The number of legal entities in terms of administrative and business forms of management						
12	The number of economic entities in terms of types of economic activity						
13	The number of active enterprises by the regions of Ukraine and types of economic activity						
14	Financial results of the enterprises activity						
Main macroeconomic indicators of Ukraine							
15	Gross Domestic Product (GDP)						
16	Gross National Income (GNI)						
17	Gross National Disposable Income (GNDI)						
18	Consumer Price Index (CPI)						
19	Inflationary Expectations						

№	INDICATOR	2013	2014	2015	2016	2017	2018
20	Index of production of basic industries (IPBI NBU - ahead indicator of GDP)						
21	**Employment level**						
22	**Unemployment rate**						
22.1	*Load of registered unemployed on each vacancy by professional groups*						
22.2	*The need of employers in employees to replace vacancies, in thsd. persons*						
22.3	*The number of registered unemployed, thsd. persons*						
23	**Salary:**						
23.1.	*Average monthly salary*						
23.2.	*Real wage indexes*						
23.3.	*Arrears of salaries*						
24	**Poverty:**						
24.1	Share of population whose average per capita equivalent total expenditures are lower than the actual (estimated) subsistence minimum,%						
24.2	Share of the poor, covered by state social support, in the total number of poor people,%						
24.3	Minimum salary level in Ukraine						
24.5	The subsistence level in Ukraine						
25	Consolidated budget revenues, mln.						
26	Consolidated Budget Expenditures, mln.						
27	Consolidated Budget Deficit, mln.						
Indicators of statistics of the external sector							
28	**Dynamics of Ukraine's Balance of Payments:**						
28.1	***Account of current operations***						
28.1.1	*Balance of goods and services*						
28.1.2	*Balance of primary incomes*						
28.1.3	*Balance of secondary incomes*						

№	INDICATOR	2013	2014	2015	2016	2017	2018
28.2	***Account of the capital operation***						
28.3	***Financial account***						
28.3.1	*The balance of direct investment*						
28.3.2	*Portfolio investment balance*						
28.3.3	*Balance of other investments*						
28.4	***Reserve assets***						
29	**Net international investment position of Ukraine, mln. USA**						
30	**Foreign trade in goods:**						
30.1	*Dynamics of the export structure*						
30.2	*Dynamics of the commodity structure of imports*						
31	**Distribution of foreign trade in goods and services by geographic regions:**						
31.1	*Distribution of goods export by the geographic regions*						
31.2	*Distribution of goods import by the geographic regions*						
32	The share of the main state trading partners of Ukraine in the total volume of goods turnover						
33	Dynamics of goods export by countries of the world						
34	Dynamics of import of goods in the world						
35	The index of prices in foreign goods trade of Ukraine						
36	Index of trade terms in foreign goods trade of Ukraine						
37	**Dynamics of** All Commodity Price Index						
37.1	Non-Fuel Price Index						
37.2	Fuel (Energy) Price Index						
38	Index of Economic complexity (country rating)						
39	**Ukraine's gross external debt, mln. USA**						
39.1	*Volume of short-term gross external debt, mln. USA*						
40	**Total State and State Guaranteed Debt (TSSGD), mln. UAH**						
40.1	*The share of foreign currency in the structure of the TSSGD, %*						
41	**The dynamics of the trade-weighted index of the US dollar, ind. points**						

№	INDICATOR	2013	2014	2015	2016	2017	2018
42	**Volume of illegal financial flows of Ukraine (GFI IFF), billion USA dollars**						
Indicators of monetary and financial statistics							
43	**Net foreign assets of NBU, mln. UAH**						
43.1	*Requirements of NBU to non-residents*						
43.2	*Obligations of the NBU to non-residents*						
44	**Net claims of the NBU to the central state management bodies, mln. UAH**						
45	**Monetary Base (M3), mln.UAH**						
45.1	*Cash in circulation outside deposit-taking corporations (M0)*						
46	**Assets of deposit-taking corporations, except NBU (credits), mln.UAH**						
47	**The liabilities of depository corporations, except the National Bank (deposits) mln. UAH**						
48	**The discount rate of the National Bank of Ukraine,% per year**						
49	**Exchange rates USD/UAH**						
50	**PFTS Stock exchange index, ind. points**						
51	**Total volume of trades on the PFTS Stock exchange mln. UAH**						
Crime control							
52	Organized criminal groups and criminal organizations were identified, including:						
	In state agencies						
	with transnational ties						
	in the budget sphere						
	in the banking system						
	in the financial and credit system						

№	INDICATOR	2013	2014	2015	2016	2017	2018
53	Identified persons were identified who committed crimes in organized crime groups and criminal organizations, including:						
	In state agencies						
	with transnational ties						
	in the budget sphere						
	in the banking system						
	in the financial and credit system						
54	Completed criminal proceedings on criminal offenses committed by the organized criminal groups and criminal organizations in the context of offenses under articles of the Criminal Code of Ukraine						
55	The number of criminal organizations against which criminal proceedings have been completed						
56	Sent criminal proceedings on criminal offenses committed by organized criminal groups and criminal organizations to the court with an indictment						
57	Closed criminal proceedings on criminal offenses committed by organized criminal groups and criminal organizations						
58	Identified amount of material damage						
59	Damages were reimbursed						
60	Seized property						
61	Number of criminal proceedings on criminal offenses committed by organized criminal groups and criminal organizations considered by the court						
62	The number of criminal proceedings, in which the fact of criminal offense commission by organized crime groups and criminal organizations was confirmed by a court order						
63	The number of convicted persons, total, including in the context of predicate crimes						
Ukraine in the world raitings							
64	Paying Taxes Reports of PwC and WB, rank						

№	INDICATOR	2013	2014	2015	2016	2017	2018
65	Henley & Partners Passport Index), rank						
66	Overall Best Countries Ranking of US News & World Report, rank						
67	Freedom in the World 2018 – Freedom House, rank						
68	Human Freedom Index - Cato Institute, rank						
69	Index of economic freedom - by The Heritage Foundation, rank						
70	Global Terrorism Index, rank						
71	Global Innovation Index, rank						
72	The Inclusive Development Index (IDI), rank						
73	Doing Business, rank						
74	Military Strength Ranking						
75	Quality of roads Index - World Economic Forum, rank						
76	Global Competitiveness Index- WEF, rank						
77	Human Development Index, HDI, rank						
78	Global Services Location Index, rank						
79	Country Brand Index - FutureBrand, rank						
80	The Legatum Prosperity Index, ранг						
81	Global Energy Architecture Performance Index, rank						
82	Corruption Perceptions Index, rank						
83	Investment attractiveness index of Ukraine (EBA), points						
84	Global Peace Index, rank						
85	Happy Planet Index						

ANNEX 2. QUESTIONNAIRE FOR THE FIU

No.	INDICATOR	2013	2014	2015	2016	2017	2018
The state of accounting of the reporting entities (RE) in the FIU and submitting by them information on suspicious financial transactions							
1	Number of the RE registered in the FIU by types of the RE*						
2	General number of the received and registered STRs submitted by the RE, including:						
2.1	number of the received and registered STRs submitted by banks						
2.2	number of the received and registered STRs submitted by non-bank financial institutions (by codes of type of non-financial institution)						
2.3	number of the received and registered STRs submitted by DNFBPs (by codes of type of DNFBPs)						
3	General number of the received and registered STRs received from RE in the context of regions *						
4	General number of the received and registered STRs by codes of signs of internal financial monitoring*						
5	Total amount of money in the received and registered STRs by codes of signs of compulsory financial monitoring*						
6	Total amount of money in the received and registered STRs by codes of signs of internal financial monitoring*						
7	Number of the received and registered STRs electronically by types of the RE*						
8	number of the received and registered STRs in paper by types of the RE *						
Creation by the FIU of case referrals and additional case referrals as well as cooperation with the law enforcement authorities							
9	Number of STRs received from the RE which became a ground for creation of case referrals (additional case referrals)						
10	Amount of money in the STRs which became a ground for creation of case referrals (additional case referrals)						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
11	Number of case referrals created and referred by the FIU to the law enforcement/intelligence authorities in the context of the law enforcement/intelligence authorities *						
12	Number of additional case referrals created and referred by the FIU to the law enforcement/intelligence authorities in the context of the law enforcement/intelligence authorities *						
13	Number of case referrals/additional case referrals related to ML created and referred by the FIU to the law enforcement/intelligence authorities						
13.1	Including on NPOs						
14	Amount of money in case referrals/additional cases referrals related to ML created and referred by the FIU to the law enforcement/intelligence authorities						
14.1	Including on NPOs						
15	Number of case referrals/additional case referrals related to FT created and referred by the FIU to the law enforcement/intelligence authorities						
15.1	Including on NPOs						
16	Amount of money in case referrals/additional cases referrals related to FT created and referred by the FIU to the law enforcement/intelligence authorities						
16.1	Including on NPOs						
17	Number of case referrals/additional case referrals related to the commission of the action identified by the CCU that does not pertain to ML created and referred by the FIU to the law enforcement/ intelligence authorities						
18	Amount of money in case referrals/additional case referrals related to the commission of the action identified by the CCU that does not pertain to ML created and referred by the FIU to the law enforcement/ intelligence authorities						
19	Number of case referrals and additional case referrals related to the suspension of financial transaction by the FIU						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
20	Amount of money in case referrals and additional case referrals related to the suspension of financial transaction by the FIU						
21	Number of financial transaction participants in case referrals/additional case referrals referred by the FIU to the law enforcement/intelligence authorities in the context of regions*						
22	Amount of financial transaction in case referrals/additional case referrals referred by the fIU to the law enforcement/intelligence authorities in the context of regions*						
23	Number of financial transactions included to case referrals/additional case referrals including by the signs of financial monitoring:						
23.1	Compulsory monitoring						
23.2	Internal monitoring						
23.3	Compulsory and internal monitoring						
24	Number of risky financial transactions in case referrals/additional case referrals referred by the FIU to the law enforcement authorities by signs of risk including:						
24.1	avoiding of financial monitoring procedures						
24.2	ML/FT suspicions						
24.3	Intricate financial transactions						
24.4	Regular cash transactions						
24.5	Financial assistance						
24.6	Others						
25	Number of case referrals/additional case referrals created by the FIU itself (on its own initiative)						
26	Number of case referrals/additional case referrals created by the FIU in response to the request of the law enforcement authority						
27	Number of STRs received by the FIU from the state authorities including those related to:						
27.1	ML						
27.2	FT						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
28	Number of financial transactions with the sign “terrorism” processed by the FIU						
29	Number of decisions on the suspension of financial transaction taked by the FIU including those related to:						
29.1	ML						
29.2	FT						
30	Amount of money suspended by the FIU including: Сума коштів, зупинених ДСФМУ, у тому числі:						
30.1	in connection with ML suspicion						
30.2	in connection with FT suspicion						
31	Number of dossiers on high risky transactions maintained by the FIU						
32	Number of financial transactions used in dossiers						
33	Amount of financial transactions used in dossiers						
34	Number of criminal proceedings iniotiated under case referrals or which use case referrals in the context of law enforcement/intelligence authorities including:*						
34.1	for ML						
34.2	for FT						
34.3	Under other Articles of the CCU (in the context of the relevant Articles of the CCU)						
35	Number of case referrals following the results of verification of which criminal proceedings was closed/initiation of criminal proceedings was refused including in the context of the law enforcement authorities*						
36	Number of criminal proceedings initiated under case referrals or in which case referrals are used referred to the court (at the stage of judicial proceeding) including:						
36.1	for ML						
36.2	for FT						
36.3	Under other Articles of the CCU (in the context of the relevant Articles of the CCU)						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
37	Number of criminal proceedings considered by the court with the indictment including:						
37.1	for ML						
37.2	for FT						
37.3	Under other Articles of the CCU (in the context of the relevant Articles of the CCU)						
38	Number of criminal proceedings considered by the court with an acquittal, including:						
38.1	for ML						
38.2	for FT						
38.3	Under other Articles of the CCU (in the context of the relevant Articles of the CCU)						
39	Total amount of the arrested/seized property (money) under criminal proceedings initiated and which used case referrals/additional case referrals						
40	Number of persons with regard to whom the court considered criminal proceedings in connection with case refferals/additional case referrals provided						
41	Amount of the proceeds (money or other property) legalized, obtained from crime established by the court decision						
42	Amount of money (property) (seized/voluntary reimbursed during the pre-trial investigation) established by the court and subjects to transferring to the state budget under the court verdict						
FIU's cooperation with the State Fiscal Service							
43	Total number of reports on the import of cash funds received by the FIU from the SFS						
44	Amount of money of transactions in reports on the import of cash funds received by the FIU from the SFS						
45	Total number of reports on the identified cases of non-declaration or incorrect declaration when importing cash funds received by the FIU from the SFS						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
46	Amount of money of transactions in reports on the identified cases of non-declaration or incorrect declaration when importing cash funds received by the FIU from the SFS						
47	Amount of information on crossborder cash transactions received by the FIU from the SFS (which belong to currency or negotiable bearer documents)						
FIU's access to data bases							
48	Number of data bases or information warehouses related to criminal justice, law enforcement activity and intelligence to which the FIU has an access (direct or indirect)						
49	Number of the official administrative registers, data bases or information warehouse to which the FIU has an access (direct or indirect)						
50	Number of the official administrative registers, data bases or information warehouse which pertain financial sector to which the FIU has an access (direct or indirect)						
Interagency cooperation							
51	Number of meetings held by the FIU with other competent AML/CFT authorities						
52	Number of Memoranda on cooperation or other acts on cooperation concluded by the FIU with competent authorities						
FIU's cooperation with foreign FIUs							
53	Number of the AML/CFT (information) requests sent by the FIU to foreign FIUs of them:						
53.1	Number of the requests responded						
53.2	Number of the requests rejected						
53.3	Number of the requests being considered						
54	Number of AML/CFT (information) requests received by the FIU from foreign FIUs of them:						
54.1	Number of the requests responded						
54.2	Number of the requests rejected						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
54.3	Number of the requests being considered						
55	Number of the requests sent by the FIU to foreign FIUs in the context of countries*						
56	Number of the responses received by the FIU from foreign FIUs in the context of countries*						
57	Number of the AML/CFT (information) requests additionally sent by the FIU to foreign FIUs						
58	Number of responses additionally recived by the FIU from foreign FIUs						
59	Number of AML/CFT (information) requests additionally received by the FIU from foreign FIUs						
60	Number of responses addittionaly sent by the FIU to the foreign FIUs requests						
61	Average number of days spent by foreign FIUs for preparing response to the request						
62	Average number of days for preparing response to the incoming request from foreign FIUs						
63	Total number of cases of sending by the FIU information materials to foreign FIU (initially)						
64	Number of cases of information provision within the information exchange from foreign FIUs (initially)						
FIUs international cooperation							
65	Number of international Memoranda concluded						
66	Number of international events in which the FIU representatives participated of them:						
66.1	Events held abroad						
66.2	Number of participants						
66.3	Events organized by the FIU in Ukraine						
66.4	Number of participants						
66.5	Events organized by other organizations in Ukraine						
66.6	Number of participants						

No.	INDICATOR	2013	2014	2015	2016	2017	2018
66.7	Events organized by the FIU jointly with other organization in Ukraine						
66.8	Number of participants						
66.9	Business meetings with foreign delegations, groups, foreign citizens in the FIU						
66.10	Number of participants						
67	Number of events on providing expert assistance to FIUs and AML/CFT competent authorities of other countries						
Research and training activity in the area of financial momnitoring							
68	Number of trainings for the REs						
69	Number of workshops for the REs						
70	Number of listeners in the context of the RE						
71	Number of trainings for the SFMEs						
72	Number of listeners in the context of the SFMEs*						
73	Number of trainings for law enforcement authorities, judges and other authorities						
74	Number of listeners of trainings for law enforcement authorities, judges and other authorities						

ANNEX 3. DATA COLLECTION TEMPLATE THAT FULFILLS EACH SFME BASED ON ITS SECTOR (SUPERVISED BY THEM TYPES OF REPORTING ENTITIES)

#	INDICATOR	2013	2014	2015	2016	2017	2018
FATF							
1. Situation in the financial sector and DNFBP sector							
1	Number of registered REs (in the context of REs)						
2	Assets amount of REs						
3	Total scope of client financial operations carried out by the REs during the reporting period						
2. Supervisory Activities							
4	Number of REs in each risk level (assigned by the state financial monitoring entity (SFME) in accordance with internal procedures)						
5	Number of on-site AML/CFT audits by REs carried out by the correspondent SFME						
6	Number of off-site AML/CFT audits by REs						
7	Total number of identified violations of legislation in the AML/CFT area by REs						
8	Number of normative requirements violation by REs regarding the responsibilities for ML/FT risk assessment						
9	Number of normative requirements violation by REs regarding the use of reinforced measures in high risk situations						
10	Number of identified violations by REs regarding the failure to provide/untimely provision of information on financial transactions in which the bank denied the client or on the refusal to establish business relations to the specially authorized authority						

#	INDICATOR	2013	2014	2015	2016	2017	2018
11	Number of detected violations of the requirements of the legislation and requirements of regulatory acts by the REs, regarding: PEPs (national and foreign) FT targeted financial sanctions high risk countries identified by the FATF						
12	Number of detected violations of regulatory requirements relating to suspicious transaction reports and other reporting obligations						
13	Number of detected violations regarding the failure to take measures to prevent the information disclosure and non-compliance with the order of documents/information storage on financial monitoring issues by the REs						
14	Number of inspections during which violations of regulatory requirements were detected, related to: non-compliance of the internal banking documents on financial monitoring with the requirements of the legislation failure to/non-observance of the timing of events to ensure the training of a responsible employee and professional development						
15	Number of detected REs violations regarding failure to apply the impact, sanctions of the National Bank and/or requirements of the National Bank to eliminate violations of legislation by the bank.						
16	Number of measures of methodological, technical and other assistance provided by the REs to the supervisory authorities in the AML/CFT area.						
17	Number of clarifications provided by the supervisory authorities on the implementation of legislation in the AML/CFT area						
18	Number of other documents related to ML/FT risks						
19	Number of outreach measures for REs on AML/CFT issues						

#	INDICATOR	2013	2014	2015	2016	2017	2018
20	Number of applications for obtaining a license or registration of creditable financial institutions and established of non-financial institutions and professions: received processed approved rejected						
21	Annual number of violations of licensing or registration requirements of credit financial institutions and DNFBP						
22	Number of supervisory measures/measures to eliminate violations applied in relation to violations of licensing or registration requirements for new and existing credit financial institutions and DNFBP						
23	Number of REs inspections on compliance with the requirements in the area of prevention and counteraction to the financing of the proliferation of weapons of mass destruction regarding targeted financial sanctions in the area of financing the proliferation of weapons of mass destruction						
24	Number of NBU decisions on the prohibition on acquiring substantial participation in the bank						
25	Number of NBU decisions regarding the rejection to approve/ confirm the business reputation and professional suitability of bank executives						
26	Number of banks that were liquidated by the NBU decision						
27	Number of cases where a bank license was withdrawn due to non-compliance of the bank ownership structure with the NBU-established requirements for its transparency						
28	Measures of influence/sanctions applied to REs for violation of the AML/CFT legislation by REs:						

#	INDICATOR	2013	2014	2015	2016	2017	2018
29	Written requests Banks written warnings Number of fines Total amount of fines, UAH Temporary, until the violation has been addressed, suspension of a bank official Restriction, termination, or stopping of certain types of operations carried out by a bank Assigning a bank to a category of problem/insolvency Revocation of a bank license and bank liquidation/revocation of a non-bank financial institution license						
30	Total number of RE clients						
31	Total number of RE clients' accounts						
32	Balance on accounts Number of client operations in foreign affiliates and subsidiaries						
33	Amount of client operations (ths. UAH)						
34	Amount of client cash transactions						
3. International SFME cooperation (requests to foreign supervisory authorities)							
35	Number of AML/CFT requests submitted to foreign authorities of financial supervision, including:						
	number of satisfied requests						
	number of rejected requests						
	number of requests under consideration						
36	Number of AML/CFT requests received from foreign authorities of financial supervision, including:						
	number of satisfied requests						
	number of rejected requests						
	number of requests under consideration						
37	Number of cases when information was provided by foreign authorities of financial supervision in the framework of information exchange						

#	INDICATOR	2013	2014	2015	2016	2017	2018
38	Average time for providing a response to a request of foreign competent authorities regarding beneficial owners:						
	legal entities						
	legal formations						
39	Average time for providing a response by foreign competent authorities regarding beneficial owners:						
	legal entities						
	legal formations						
40	Number of satisfied requests submitted by foreign competent authorities regarding beneficial owners:						
	legal entities						
	legal formations						

ANNEX 4. DATA COLLECTION TEMPLATE BY THE LAW ENFORCEMENT AND INTELLIGENCE AUTHORITIES

#	INDICATOR	2013	2014	2015	2016	2017	2018
FATF							
Countering offenses related to ML and crimes preceding ML							
1	Number of registered ML criminal proceedings						
2	Number of closed ML criminal proceedings in the reporting period						
3	Number of ML criminal proceedings submitted to the court, including:						
3.1	with an indictment						
4	Number of individuals served a suspicion note for ML crimes						
5	Number of registered criminal proceedings in the context of predicate crimes*						
6	Number of closed criminal proceedings during the reporting period in the context of predicate crimes*						
7	Number of criminal proceedings submitted to the court in the context of predicate crimes, including:						
7.1	with an indictment						
8	Number of individuals served a suspicion note in the context of predicate crimes						
9	Established amount of financial damage from criminal activity						
10	Established amount of legalized funds and property for ML						
11	Withdrawn of funds and property for ML						
12	Seize of property for ML						
Countering terrorism and FT							
13	Number of criminal proceedings initiated for terrorism, including:						
13.1	under CCU Art. 258 (Terrorist attack)						

#	INDICATOR	2013	2014	2015	2016	2017	2018
13.2	under CCU Art. 258-1 (Involving in the committing of a terrorist attack)						
13.3	under CCU Art. 258-2 (Public calls for the committing of a terrorist attack)						
13.4	under CCU Art. 258-3 (Establishing of a terrorist group or terrorist organization)						
13.5	under CCU Art. 258-4 (Facilitating the Committing of a Terrorist Attack)						
14	Number of criminal cases initiated for terrorism financing (CCU Art. 258-5)						
15	Number of individuals who have been given suspects in criminal proceedings for terrorism, including:						
15.1	under CCU Art. 258 (Terrorist attack)						
15.2	under CCU Art. 258-1 (Involving in the committing of a terrorist attack)						
15.3	under CCU Art. 258-2 (Public calls for the committing of a terrorist attack)						
15.4	under CCU Art. 258-3 (Establishing of a terrorist group or terrorist organization)						
15.5	under CCU Art. 258-4 (Facilitating the Committing of a Terrorist Attack)						
16	Number of individuals who have been given suspects in criminal proceedings for TF						
17	Number of closed criminal proceedings for terrorism, including:						
17.1	under CCU Art. 258 (Terrorist attack)						
17.2	under CCU Art. 258-1 (Involving in the committing of a terrorist attack)						
17.3	under CCU Art. 258-2 (Public calls for the committing of a terrorist attack)						

#	INDICATOR	2013	2014	2015	2016	2017	2018
17.4	under CCU Art. 258-3 (Establishing of a terrorist group or terrorist organization)						
17.5	under CCU Art. 258-4 (Facilitating the Committing of a Terrorist Attack)						
18	Number of closed criminal proceedings for TF (CCU Art. 258-5)						
19	Number of criminal cases for terrorism, where the criminal case was submitted to court with an indictment, including:						
19.1	under CCU Art. 258 (Terrorist attack)						
19.2	under CCU Art. 258-1 (Involving in the committing of a terrorist attack)						
19.3	under CCU Art. 258-2 (Public calls for the committing of a terrorist attack)						
19.4	under CCU Art. 258-3 (Establishing of a terrorist group or terrorist organization)						
19.5	under CCU Art. 258-4 (Facilitating the Committing of a Terrorist Attack)						
20	Number of criminal cases for TF (CCU Art. 258-5), where the criminal case was submitted to court with an indictment						
21	Number of criminal cases initiated only for TF						
22	Number of criminal cases initiated for TF and another CCU article						
23	Number of criminal cases under CCU Art. 258-5 in the context of TF tools						
24	Number of criminal cases under CCU Art. 258-5 in the context of international TF and domestic TF						
25	Value of assets seized or confiscated from terrorists or terrorist financing individuals						
26	Number of legal entities from which assets owned by terrorists or terrorist financing individuals, or otherwise related to TF or terrorism were seized or confiscated						

#	INDICATOR	2013	2014	2015	2016	2017	2018
27	Number of criminal cases for TF on individuals and legal entities on the terrorist list						
28	Number of criminal cases initiated under CCU Art. 332 (human smuggling across the state border)						
29	Number of closed criminal cases initiated under CCU Art. 332 (human smuggling across the state border)						
30	Number of criminal cases under CCU Art. 258-5, where the criminal case was submitted to court with an indictment (human smuggling across the state border)						
31	Number of criminal cases related to international terrorism						
32	Number of transit points for deployment of terrorist organizations detected by the law enforcement authorities						
33	Number of criminal cases for terrorism by international terrorist organizations						
34	Number of investigations/prosecutions against international terrorist organizations						
Countering proliferation of weapons of mass destruction							
35	Number of criminal cases initiated under CCU Art. 439 (Use of weapons of mass destruction)						
36	Number of criminal cases initiated under CCU Art. 440 (Development, production, purchasing, storage, transportation, distribution of weapons of mass destruction)						
37	Number of criminal cases under CCU Art. 439 (Use of weapons of mass destruction) submitted to court with an indictment						
38	Number of criminal cases under CCU Art. 440 (Development, production, purchasing, storage, transportation, distribution of weapons of mass destruction) submitted to court with an indictment						
39	Number of NPOs involved in criminal cases under CCU Art. 439 (Use of weapons of mass destruction)						

#	INDICATOR	2013	2014	2015	2016	2017	2018
40	Number of NPOs involved in criminal cases under CCU Art. 440 (Development, production, purchasing, storage, transportation, distribution of weapons of mass destruction)						
41	Number of legal entities involved in criminal cases under CCU Art. 439 (Use of weapons of mass destruction)						
42	Number of legal entities involved in criminal cases under CCU Art. 440 (Development, production, purchasing, storage, transportation, distribution of weapons of mass destruction)						
43	Number of stopped/blocked shipments of goods related to persons who were served a suspicion note under CCU Art. 439 and CCU Art. 440						
44	Number of criminal cases initiated under CCU Art. 440 for illegal shipment of goods to high-risk jurisdictions, including:						
44.1	chemicals						
44.2	weapons						
44.3	other (please indicate)						
Use of NPOs in the terrorism and TF crimes							
45	Number of inspections of NPOs on TF issues						
46	Number of sanctions and other corrective measures imposed on NPOs in TF countering						
47	Number of outreach measures (including supervisory documents) in the NPO sector in relation to measures and trends in TF countering						
48	Number of NPOs that pursue their activities in the conflict zones						
49	Number of NPOs that pursue cross-border financial transactions						
50	Number of NPOs on the list of terrorist organizations						
51	Number of criminal cases initiated under CCU Art. 258 – 258-5 on the use of NPOs by terrorists						

#	INDICATOR	2013	2014	2015	2016	2017	2018
52	Number of NPOs involved in criminal cases under CCU Art. 258-5						
53	Amount of arrested/seized/confiscated funds under CCU Art. 258-5 by NPOs						
Information access of law enforcement authorities							
54	Number of databases or information storages related with criminal justice, law enforcement and intelligence activities that law enforcement authorities and other competent authorities have access to.						
55	Number of official administrative registers, databases or information storages accessed by law enforcement and other competent authorities						
56	Number of registries, databases or information storages related to the financial sector to which law enforcement and other competent authorities have access						
Cross-border transfer of assets							
57	Annual volume of currency and securities falsely declared or undeclared, or concealed, or moved abroad						
58	Number of identified undeclared movements						
59	Additional sanctions imposed on offenders						
60	Number of customs declarations received						
61	Scope of information received by the competent authorities on cross-border cash transactions (currency, securities)						
62	Number of initiated criminal cases based on information on undeclared transfer of assets across the border						
63	Number of criminal cases transferred to court based on information on undeclared transfer of assets across the border						
64	Number of illegal border-crossing offenses						
65	Amount of confiscated undeclared cash on court orders						

#	INDICATOR	2013	2014	2015	2016	2017	2018
66	Number of reports from the State Border Guard Service on illegal transfers of currency, precious metals						
67	Information provided by the State Fiscal Service to the SFMS on undeclared transfer of assets across the border:						
67.1	number of reports						
67.2	number of individuals involved						
67.3	amount of currency values						
67.4	precious metals						
67.5	precious natural stones						
67.6	Other						
68	Amount of undeclared cash at the Ukrainian borders						
International cooperation in the area of AML/CFT and financing of proliferation of weapons of mass destruction (MLA and extradition requests)							
MLA (mutual legal assistance) requests							
69	Number of MLA requests received, including:						
69.1	number of responded MLA requests						
69.2	number of rejected MLA requests						
69.3	number of MLA requests being considered						
70	Number of received MLA requests (including MLA requests related to asset identification, freezing/seizure) including:						
70.1	number of responded MLA requests						
70.2	number of rejected MLA requests						
70.3	number of MLA requests being considered						
71	Number of received requests regarding the execution of confiscation and distribution and recovery of assets decisions:						
71.1	number of responded MLA requests						
71.2	number of rejected MLA requests						
71.3	number of MLA requests being considered						

#	INDICATOR	2013	2014	2015	2016	2017	2018
72	Number of submitted requests submitted regarding the execution of confiscation and distribution and recovery of assets decisions:						
72.1	number of responded MLA requests						
72.2	number of rejected MLA requests						
72.3	number of MLA requests being considered						
73	Average processing time for an MLA request						
74	Average time for processing a request related to the execution of confiscation and distribution and recovery of assets decisions						
75	Average time for processing an incoming extradition request (from the moment of receiving to the moment of informing on the review results)						
76	Number of investigations conducted by foreign competent authorities or jointly with foreign competent authorities, including joint investigation groups						
77	Average response time to an MLA request submitted:						
77.1	committing certain procedural actions (interrogation, serving of documents, receiving information/documents, etc.)						
77.2	asset identification, freezing, arrest						
78	Average time for receiving a response to a responded request related to the execution of confiscation and distribution and recovery of assets decisions						
79	Number of foreign (incoming) MLA requests (including on asset identification / freezing / arrest / confiscation / distribution and recovery) in total, specifically in relation to:						
79.1	ML						
79.2	TF						
79.3	corruption						
79.4	drugs						

#	INDICATOR	2013	2014	2015	2016	2017	2018
79.5	tax evasion						
79.6	organized crime						
79.7	other						
80	Number of foreign (incoming) MLA requests related to asset confiscation						
81	Total number of foreign requests for assets arrest						
82	Total value of arrested assets on the basis of foreign requests						
83	Total number of foreign requests for asset confiscation						
84	Total value of confiscated assets on the basis of foreign requests						
85	Total value of assets returned to the requesting country after final confiscation						
86	Number of outgoing requests for MLA from Ukrainian instituions based on the type of assistance requested, including:						
86.1	obtaining documentary evidence/information						
86.2	serving of documents						
86.3	interrogating a witness (including through videoconferencing)						
86.4	arrest of assets						
86.5	confiscation of assets						
86.6	distribution and recovery of assets						
87	Number of outgoing requests for MLA from Ukrainian instituions based on the type of crime:						
87.1	ML						
87.2	TF						
87.3	corruption						
87.4	drugs						
87.5	tax evasion						
87.6	organized crime						
Extradition requests							
88	Number of extradition requests in the AML/TF area, including:						

#	INDICATOR	2013	2014	2015	2016	2017	2018
88.1	received requests						
88.2	submitted requests						
88.3	requests being considered						
88.4	responded requests						
88.5	rejected requests						
89	Total number of received extradition requests, including:						
89.1	responded requests						
89.2	rejected requests						
89.3	requests being considered						
90	Total number of individuals for which extradition requests were received						
91	Total number of individuals extradited from Ukraine						
92	Total number of submitted extradition requests, including:						
92.1	responded requests						
92.2	rejected requests						
92.3	requests being considered						
93	Total number of individuals for which extradition requests were submitted:						
93.1	responded requests						
93.2	rejected requests						
93.3	requests being considered						
94	Total number of individuals extradited to the jurisdictions from which the request was received						
95	Average response time for the extradition request						
96	Three countries to which the largest number of extradition requests were submitted						
97	Number of MLA requests received on asset identification, freezing, arrest, including:						
97.1	number of responded MLA requests						
97.2	number of rejected MLA requests						

#	INDICATOR	2013	2014	2015	2016	2017	2018
97.3	number of MLA requests being considered						
98	Number of MLA requests submitted on asset identification, freezing, arrest, including:						
98.1	number of responded MLA requests						
98.2	number of rejected MLA requests						
98.3	number of MLA requests being considered						
Sanctions pursuant to the UN Security Council Resolutions							
99	Total value of frozen assets or property pursuant to targeted financial sanctions against individuals and legal entities included on the lists pursuant to the UN Security Council Resolutions on combating TF and proliferation of weapons of mass destruction						
100	Total value of funds or other assets covered by targeted financial sanctions against individuals and legal entities included on the lists pursuant to the UN Security Council Resolutions on combating TF and proliferation of weapons of mass destruction						
101	Average time spent on freezing assets or property within a country, based on targeted financial sanctions after adding of an individual associated with such assets or property to the list pursuant to the UN Security Council Resolutions on combating TF and proliferation of weapons of mass destruction						
102	Average time spent on selecting individuals for imposition of internal financial sanctions after adding them to the list pursuant to the UN Security Council Resolutions on combating TF and proliferation of weapons of mass destruction						
103	Number of investigations related to violation of targeted financial sanctions on individuals and legal entities included on the lists pursuant to the UN Security Council Resolutions on combating TF and proliferation of weapons of mass destruction						
104	Number of individuals, in relation to which accounts targeted financial sanctions were imposed by the UN Security Council or other organizations						

#	INDICATOR	2013	2014	2015	2016	2017	2018
105	Number of individuals and legal entities included on the national lists whose assets were frozen on other grounds (compared to those included on the list pursuant to the UN Security Council Resolutions 1267)						
106	Number of accounts and aggregate amount of cash and/or assets covered by targeted financial sanctions pursuant to the UN Security Council Resolutions (in the context of resolutions)						
107	Value of assets frozen pursuant to targeted financial sanctions by the UN Security Council or other organizations						
108	Average time spent on freezing assets after adding to the lists pursuant to the UN Security Council Resolutions and/or international documents						
109	Number of international requests related to the UN Security Council Resolutions:						
109.1	received						
109.2	submitted by the country						
110	Number of persons added by the country to the list pursuant to the UN Security Council Resolution 1373						
111	Number of financial transactions refused due to targeted financial sanctions						
112	Number of persons or organizations added to the lists by mistake, information on which reporting entities transferred to the state authorities (e.g., individuals with identical or similar surnames)						
113	Average time for adding an individual/legal entity to the sanction list after dicission of the UN Security Council						
Joint protocols signed							
114	Number of concluded interagency agreements						
115	Number of concluded bilateral agreements						
116	Number of concluded multilateral agreements						
117	Number of signed memoranda on cooperation						

ANNEX 5. DATA COLLECTION TEMPLATE ON THE JUDICIAL SYSTEM

#	INDICATOR	2013	2014	2015	2016	2017	2018
FATF							
Judicial review of criminal cases related to ML							
1	The number of criminal proceedings concerning crimes committed against ML, received in court during the reporting period of all, of which the pre-trial investigation was conducted:						
1.1	by the investigators of PGOU						
1.2	by the investigators of NPU (internal affairs)						
1.3	by the investigators of SSU						
1.4	by the detectives of NABU						
2	The number of criminal proceedings concerning crimes committed by ML, considered by courts in the reporting period, total, of them:						
2.1	with a sentence						
2.2	with the closure of proceedings in a case						
2.3	with a return to an additional (pre-trial) investigation						
3	The number of individuals in respect of which the courts reviewed criminal proceedings for crimes against ML, all of them:						
3.1	convicted						
3.2	justified						
3.3	on which criminal proceedings are closed						
4	The number of persons against whom the court decision on confiscation of funds and property was made following the results of the criminal proceedings concerning the crimes committed against ML						
5	The amount of legalized proceeds (funds, property) established by a court decision						
6	The number of court sentences related to ML by division of type cases:						
6.1	self-laundering						
6.2	laundering by third persons						

#	INDICATOR	2013	2014	2015	2016	2017	2018
6.3	autonomous ML						
6.4	ML with the predicate foreign crime						
7	Type of convicted persons in court sentences related to ML:						
7.1	leader of state company						
7.2	leader of another company						
7.3	prosecutor						
7.4	judge						
7.5	former or current high-ranking official						
6	Number of court sentences on ML in the context of predicate crimes *						
7	Number of ML criminal cases which led to a decision on prosecution for a predicate crime (without CCU Art. 209)						
8	Number of court decisions according to which the grounds for dropping the charges on ML were:						
8.1	not enough evidence						
8.2	sent on additional (pre-trial) investigation						
8.3	Convictions on ML are absorbed by sentences for predicate crimes						
9	Number of accusatory acts of the court for predicate crimes in the context of articles of the CCU*						
10	Number of individuals sentenced for predicate crimes in the context of articles of the CCU*						
11	Number of individuals which are the subject to a sanction for ML fines						
12	The average amount of fines applied to individuals convicted for VC						
13	The number of individuals convicted under Art. 209 CCU to imprisonment (except for probational sentences and suspended sentences)						
14	Average imprisonment term (in months >0) for individuals convicted on ML (except for probational sentences and suspended sentences)						
Judicial review of criminal cases related to TF							

#	INDICATOR	2013	2014	2015	2016	2017	2018
15	The number of criminal proceedings on crimes against the FT, considered by the courts in the reporting period, total, of them:						
15.1	with a sentence						
15.2	with the closure of the proceedings						
15.3	with returning on additional (pre-trial) investigation						
16	The number of persons in respect of which the courts reviewed criminal proceedings for crimes against the TF, all of them:						
16.1	convicted						
16.2	justified						
16.3	on which criminal proceedings are closed						
17	The number of persons against whom a court decision on confiscation of funds and property has been taken as a result of consideration of criminal proceedings concerning TF crimes						
18	Number of convicted individuals on TF crimes, including:						
18.1	convicted to imprisonment						
18.2	fined						
18.3	other punishments						
19	Number of court sentences for TF crimes by regions*						
20	The average term of imprisonment for a TF crime						
21	Number of court sentences only for TF						
22	Number of court sentences on TF and other Art. of CCU						
23	Number of court sentences on TF by international TF and TF inside country						
24	Number of convicted individuals under art. 258-5 CCU in terms of categories:						
24.1	Number of individuals convicted to imprisonment						
24.2	Number of individuals convicted to imposition of a fine						
24.3	Number of individuals convicted to other types of punishment						
Using NPOs for TF crimes							
25	Number of convictions under CCU Art. 258 – 258-5 on the use of NPOs by terrorists						
26	Number of convicted persons under CCU Art. 258 – 258-5 on the use of NPOs by terrorists						
27	Number of sentences under Art. 258-5 CCU (TF) and NPOs						

#	INDICATOR	2013	2014	2015	2016	2017	2018
28	Number of convicted persons under Art. 258-5 (TF) and NPOs						
Judicial review of criminal cases related to financing of proliferation of weapons of mass destruction							
29	Number of court sentences under Art. 439 CCU (use of weapons of mass destruction)						
30	Number of court sentences under Art. 400 CCU (development, production, acquisition, storage, transportation, sale of weapons of mass destruction)						
31	Number of sanctions imposed according to the conviction of Art. 439 CCU:						
31.1	concerning individuals						
31.2	concerning legal persons						
32	Number of sanctions imposed according to the conviction under Art. 440 CCU on the proliferation of weapons of mass destruction:						
32.1	concerning individuals						
32.2	concerning legal entities						
Arrest, confiscation, freezing of assets							
33	Number of court decisions on confiscation (special confiscation)						
34	Amount of confiscated property						
35	Number of confiscation decisions of equivalent value						
36	Number of court sentences with the use of confiscation as an additional punishment						
37	Number of persons against whom a decision was made to confiscate money and property						
38	Number of cases of confiscation of assets without court verdict / by court verdict						
39	The number of individuals whose assets were confiscated without a court judgment/by a court judgment						
40	The annual value of the proceeds of crime divided by foreign jurisdictions returned to the owner-country or returned to the victim						
41	Number of court decisions on confiscation in relation to illegal enrichment and abuse of authority						
42	The number of criminal proceedings against which a decision was made to freeze criminal assets						

#	INDICATOR	2013	2014	2015	2016	2017	2018
43	Cost of seized or frozen criminal assets						
44	Number of seized assets and property at the stage of additional (pre-trial) investigation						
45	The amount of criminal proceeds arrested during an additional (pre-trial) investigation						
46	The number of criminal proceedings in which law enforcement authorities arrested/seized property						
47	Total amount of property arrested/seized by law enforcement authorities						
48	Arrests on assets received as a result of committing predicate criminal offenses, which are placed in banks, other financial institutions in Ukraine and (or) abroad						
49	Number of frozen assets and property at the stage of additional (pre-trial) investigation						
50	Number of cases concerning identification and finding of assets						
51	Number of freezing assets						
52	Number of individuals whose assets have been frozen						
53	The cost of frozen assets						

ANNEX 6. EXCERPTS FROM UKRAINIAN RECOMMENDATIONS ACCORDING TO EXPERTS' CONCLUSIONS

Results of the first National Risk Assessment in the AML/CFT area (2016)

According to the results of the conducted first National Risk Assessment in AML/CFT area in Ukraine, the Government of Ukraine adopted a number of mandatory measures that should be taken by state authorities in order to minimize the identified risks, in particular:

- information exchange with the competent authorities of foreign states and international organizations with the aim to establish ML methods, schemes and mechanism, and documenting offenses in the foreign economic area;
- establishment of close cooperation between the NABU and the SFMS in the context of information exchange and the implementation of an effective cooperation mechanism;
- implementation of measures for cashless settlements development;
- bill drafting to implement the provisions of EU Directive 2015/849 of the European Parliament and Council on prevention of money-laundering and combating terrorism and EU Regulation No 2015/847 of the European Parliament and Council on information accompanying fund transfers and their accompaniment to the Verkhovna Rada of Ukraine before adoption;
- implementation of measures aimed at increasing cooperation effectiveness of law enforcement authorities on combating organized crime area, in particular in the area of cooperation with newly created (including anti-corruption) law enforcement authorities;
- taking effective measures to detect and eliminate FT channels;
- creation of an effective feedback system between the law enforcement authorities and the SFMS regarding the results of law enforcement consideration of the case referrals by ensuring the control and accounting of the state of consideration case referrals and ensuring the timely relevant information exchange;
- drafting of the Law of Ukraine "On Realtor Activity" and its accompaniment in the Verkhovna Rada of Ukraine before adoption;
- conducting a sectoral risk assessment of using non-profit organizations for ML/FT and financing of proliferation of weapons of mass destruction.

Results of the MONEYVAL 5th round of mutual evaluation of Ukraine in the AML/CFT area by Committee of Experts of the Council of Europe (2018)

Key recommendations to Ukraine defined by Report on the results of the MONEYVAL 5th Round of Mutual Evaluation of Ukraine by the Committee of the Council of Europe:

- deepening risk understanding in certain areas (for example, cross-border risks, risks caused by non-profit organizations and legal entities sector);
- legal enforcement focused on combating ML related to corruption;
- directing national coordination and policy formation mechanisms to minimize the risks caused by fictitious enterprises, the shadow economy and cash use;
- updated IT system of the SFMS, increasing the staff number for adequately increasing workload;
- use of confiscation consistently in all generating income cases;
- bringing the legislation regarding the implementation of FT targeted financial

sanctions system in accordance with international standards;
- implementation by non-banking institutions and DNFBP preventive measures taking into account the risk-based approach;
- implementation by the majority of supervision authorities improvements of the performance of their supervisory functions in the financial monitoring area;
- ensuring the reliability and relevance of information on beneficial ownership in the United State Register;
- ensuring the effective provision of mutual legal assistance.

Results of the 4th round of Ukraine's evaluation of corruption prevention among people's deputies, judges and prosecutors by GRECO experts (2017)

Key recommendation for Ukraine:
- taking necessary measures to prevent circumvention of limitations by people's deputies to carry out business activity;
- implementing at the legislative level performance assessments of prosecutors official duties in prosecutor's offices on the basis of established objective criterias;
- increasing the effectiveness of disciplinary proceedings against misdemeanors of prosecutors by increasing the limitation period and ensuring the possibility for the relevant prosecutor's authorities and heads to initiate disciplinary proceedings;
- development of measures, in particular, regulatory for strengthening the independence and impartiality of the National Agency on Corruption Prevention;
- ensuring the unrestricted access for National Agency on Corruption Prevention to all declarations received by the National Agency on Corruption Prevention and within the framework of criminal proceedings opened on the basis of such declarations to all national and regional databases necessary for the declarations evaluation;
- taking measures to reduce the external pressure and the impact of corruption on judges.

LIST OF ABBREVIATIONS

ADHWG	–	Ad Hoc Working Group
AML/CFT	–	preventing and countering legalization (laundering) of proceeds of crime and financing of terrorism
CCU	–	Criminal Code of Ukraine
CDD	–	Client Due Diligence
CJS	–	Criminal justice system
CMU	–	Cabinet of Ministers of Ukraine
DNFBP	–	Designated Non-Financial Businesses or Professions
EGMLTF	–	Expert Group on ML and TF
ESA	–	European Supervisory Authorities
EU	–	European Union
FATF	–	Financial Action Task Force
FIU	–	Financial Intelligence Unit
FSRB	–	FATF-Style Regional Bodies
GDP	–	Gross Domestic Product
IMF	–	International Monetary Fund
Law	–	Law of Ukraine "On Preventing and Countering Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of Proliferation of Weapons of Mass Destruction" (of 14.10.2014, No. 1702-VII)
LEA	–	Law Enforcement Agencies
ML	–	Legalization (laundering) of proceeds of crime
ML/TF	–	Legalization (laundering) of proceeds of crime and terrorist financing
MLA	–	Mutual Legal Assistance
MONEYVAL	–	Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MS	–	Member State
NBU	–	National Bank of Ukraine
NGO	–	Non-Governmental Organizations
NPO	–	Non-Profit Organizations
NRA	–	National Risk Assessment
OSCE	–	Organization for Security and Cooperation in Europe
POC **RE**	– _	Proceeds of crime Reporting Entity
RBA	–	Risk-Based Approach
SFME	–	State Financial Monitoring Entities
SFMSU	–	State Financial Monitoring Service of Ukraine
SNRA	–	Supranational Risk Ass
SRB	–	Self-Regulatory Bodies
STR	–	Suspicious transaction report
TF	–	Terrorist Financing
UBO	–	Ultimate beneficial owner
UN Security Council	–	United Nations Security Council