Евразийская группа по противодействию легализации
преступных доходов
и финансированию терроризма

Eurasian Group on Combating Money Laundering
and Financing of Terrorism

BEST PRACTICES AND RECOMMENDED APPROACHES FOR SECTORAL MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

Introduction

This document was developed as part of the implementation of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) project and is a summary of experiences and best practices of supervisory authorities of the EAG Member States in conducting sectoral money laundering and terrorist financing (ML/TF) risk assessments.

The document is intended for use in the work of the EAG Member States' supervisors in conducting ML/TF risk assessments at the level of supervised sectors, and in using risk assessment results in applying the risk-based approach to supervision.

The document is the result of the joint work of the members of the Project Team consisting of representatives of supervisory authorities and financial intelligence units of the Republic of Belarus, the Republic of Kazakhstan, the People's Republic of China, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan, Turkmenistan, and the Republic of Uzbekistan. The Project Team was headed by a representative of the Federal Financial Monitoring Service of the Russian Federation.

The members of the Project Team are grateful to the EAG Member States for the materials, examples, questionnaires, responses to questionnaires and other papers used in the development of this document. The Project Team is also grateful to the Financial Action Task Force (FATF) Secretariat for its comments on the draft document.

Key dates of the Project

June 2021	The 34th EAG Plenary Meeting approved the Project Plan to improve RBA mechanisms in supervisory activities in the EAG Member States.
November 2021	The 35th Plenary Meeting approved the initiative of the Russian Federation to implement the Project, instructed to form a project team, develop a project plan, send questionnaires to the Member States and receive responses to collect information.
December 2021 - May 2022	A Project Team consisting of representatives from 7 Member States and the EAG Secretariat was formed. A representative of the Russian Federation (Federal Financial Monitoring Service) was appointed to lead the Group. A Project Plan was developed and approved, outlining the timeline for implementing the project and assigning roles to those involved. The practice of ML/TF risk assessment at the level of individual economic sectors in the FATF and FSRB member countries was studied. The Member States were sent a questionnaire on approaches, experiences and best practices in carrying out sectoral risk assessments. Responses from supervisors in seven countries were analyzed, and key conclusions were drawn about the approaches used to collect, analyze, process, and interpret information for threat analysis, vulnerability identification, and risk assessment.
June 2022	The 36th EAG Plenary Meeting heard a report on the interim results of the project
June 2022 - October 2022	Responsibilities for developing the draft were assigned and a list of sectors to be covered was determined. The structure of the draft based on the responses of the EAG Member States was agreed. The need to develop separate annexes to the Guidelines in the form of questionnaires for each of the sectors covered was agreed. It was decided to expand the list of issues covered by the Guidelines and to describe the criteria of inherent and residual risks used by supervisors to assess reporting entities, as well as ML/TF typologies (schemes) using the infrastructure of representatives of individual sectors. In this regard, it was proposed to submit the question of extending the Project until May 2023 to the EAG Plenary.
November 2022	The 37th EAG Plenary Meeting approved the extension of the Project until May 2023 and requested that its final results be reported to the 38th EAG Plenary Meeting.
December 2022 - May 2023	During the intersessional period, the Project Team held further meetings to discuss the split of tasks for the development of the sample questionnaires for the various sectors. The members of the Project Team have taken on the task of developing questionnaires for the banking sector, non-banking credit institutions, notaries and dealers in precious metals and stones.

	Subsequently, the team developed a Survey Questionnaire on the purpose of using the results of the SRA, which was disseminated to the EAG Member States for completion. The responses of the member states were summarised and used in the development of the final paper. Based on the materials collected and analysed, the Project Team developed a draft paper and submitted to the WGTA and the Plenary meeting for approval.
June 2023	The 38th Plenary Meeting approved the Project implementation results.

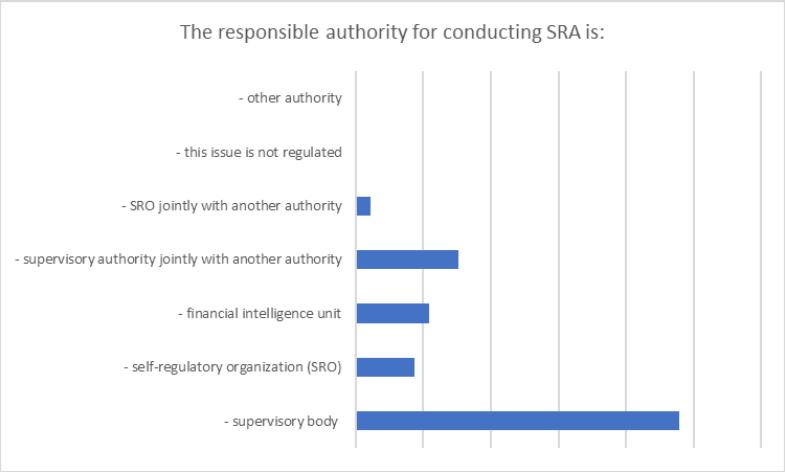
I. Best practices of preparing and conducting SRA

1. The Project Team developed a questionnaire on methodological approaches to sectoral ML/TF risk assessments, which aimed to summarize best practices of countries in developing universal methodologies for algorithmizing sectoral risk assessment (hereinafter – the SRA), collecting the information necessary for risk analysis and available to the competent authorities conducting the risk assessment, its subsequent analysis and interpretation of the results.

2. The questionnaire consisted of 5 main sections on preparatory work and description of the SRA context, approaches to threat assessment, approaches to vulnerability assessment, approaches to risk assessment, and examples of successful coordination of interagency efforts in conducting the SRA. The questionnaire was sent to the EAG Member States and responses were received and analyzed from 21 supervisory authorities.

Preparation and context

3. The responses to the questions on the sectoral risk assessment preparation and context showed that the SRA is usually carried out by a supervisor, either independently or jointly with another authority. In sectors where there is no supervisory authority, SRA is usually conducted by the financial intelligence unit.

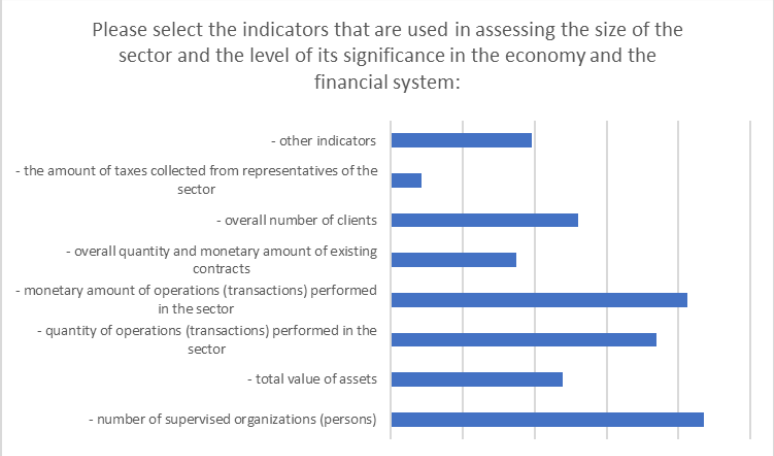


An SRA can be conducted at any time, either before or after a national risk assessment.

In most cases, the SRA is carried out by the supervisory authority itself, less often on the basis of a decision of the interagency coordinating body.

Before conducting an SRA, a fixed work plan should be approved. This work plan can be modified only to a limited extent.

4. At the same time, the analysis of responses to the preparation and context section of questions showed that to determine the importance of the sector it is necessary to use: the number of the sector entities, the volume of transactions in monetary and quantitative terms, the total value of assets and the total number of customers, other possible indicators (listed in the descending order of their importance).



To count the entities, it is proposed to count the permits/licenses issued and compare them with the number of entities actually operating, including information from other government authorities.

Financial assets should be included in the calculation of the sector's assets.

High-risk customers and non-residents should be counted separately.

5. When calculating the number of customers in the sector, the following customers are not taken into account: a) those who make one-off transactions; or b) those who have ceased business relationships; or c) those who have been inactive for more than two years at the time of conducting the SRA.

6. Examples of preparatory work or context study:

Example 1

In preparation of the SRA, the following will be identified:
- The activities required to conduct the SRA (establishment of a risk assessment working group and approval of its personal composition, approval of an action plan with identification of responsible persons and deadlines, etc.);
- Types, forms and methods of obtaining information for conducting the SRA (depending on the types of services provided and the entities providing them);
- Approaches to identifying persons involved in the SRA;
- Procedures for analyzing the information obtained to identify and assess risks.

Example 2

When organizing the work aimed at assessing the ML/TF risks in reporting entities, the Main Insurance Supervision Department, taking into account the specifics of the insurer (organization of the internal control system, market share, number of offices and branches, number of employees, distribution network, insurance portfolio structure, number of intermediaries, etc.), does not always apply common (standard) approaches to all insurance parties. The information for analysis and assessment of the insurer's compliance with AML/CFT legislation and the effectiveness of the internal control system is collected from various sources, including statistical tables and questionnaires developed by the Main Insurance Supervision Department and completed by insurance companies.

Example 3

In order to monitor compliance with AML/CFT legislation and the functioning of the internal control system at insurance companies in connection with the changed situation in the world due to the coronavirus infection and the increasing number of cases of illegal actions (global threats), insurers have conducted an internal assessment of ML/TF risks and vulnerabilities (including the impact of COVID-19), along with the assessment of insurance products implemented with the use of new technologies, as instructed by the Ministry of Finance in 2020. Based on the results of the internal risk assessment, the insurers have developed and approved action plans to mitigate these risks.

Example 4

The following indicators are used to estimate the size of the banking sector:
- Balances in customers' bank accounts;
- The structure of incoming and outgoing international transfers by country, the number and total amount of transfers;
- The volume of cash in circulation.

The following indicators are used to assess the size of the non-banking financial institutions sector:
- For leasing organizations – the volume of the leasing portfolio and the total price of contracts concluded by leasing organizations;
- For microfinance organizations – total assets, shareholders' equity, and liabilities;
- For forex companies – the authorized capital, the amount of margin funds, and the amount of the guarantee fund.

Example 5

There is clear agreement between the competent authorities and the FIU on the conduct of sectoral risk assessment of DNFBPs. The country's 2019 MER indicates a lack of effective preventive or supervisory measures with respect to DNFBPs. In order to address the deficiencies in the MER, identify and mitigate the ML/TF risks faced by DNFBPs, and apply risk-based supervision, the AML competent authority and relevant supervisory authorities have reached a consensus to initiate a risk assessment in the DNFBP sector.

In assessing risks in the DPMS sector, the AML competent authority and self-regulatory bodies first analyzed and determined that gold, diamonds, and precious stones comprise the majority of the precious metals and stones market. Therefore, the DPMS sector assessment focused on the mining, processing, retailing, and refining of these three types of metals and stones.

Example 6

In 2019, the Central Bank, together with the FIU and reporting entities, conducted an assessment in the banking sector and in the sector of non-banking financial institutions. In particular, a methodology was developed that includes the identification, analysis and assessment of ML/TF risks based on risk factors (types of customers, types of activities, products and services, distribution channels, specifics of geographic reach, etc.).

The first stage of the SRA focused on identifying the necessary information. To this end, the Central Bank conducted a series of consultations with a wide range of stakeholders, including representatives of reporting entities. This was followed by the development of a set of tables containing a wide range of quantitative indicators and a questionnaire for the qualitative assessment of the functioning of the AML/CFT system.

Example 7

As part of the 2019 SRA, a set of statistical tables were prepared to provide general information on the state of the banking sector and the supervisory activities of the Central Bank, containing the following information:
- Number of banks;
- Size of banks' assets;
- Number of customers, their activities and volume of transactions;
- List of products and services, number of customers and volume of transactions conducted by them;
- Statistical data on the distribution channels of products and services;
- Volume of international transactions by country;
- Volume of cash in circulation;
- Volume of international money transfers;
- Volume of transactions with high-risk customers;
- Number of on-site inspections, violations and deficiencies found, actions taken by the Central Bank in response.

Example 8

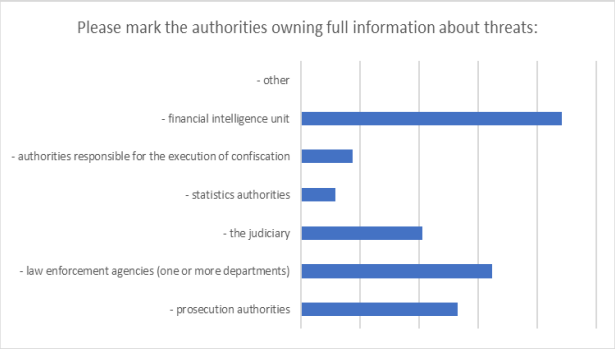
General (contextual) information is used to determine the scope of ML/TF risks in the financial market. ML/TF risks are considered to be derived from the following factors: threats, vulnerabilities, and consequences. The process of risk identification consists in forming an opinion about the potential threats, vulnerabilities and the likelihood of their combination in the conduct of transactions on the financial market, the occurrence of consequences.

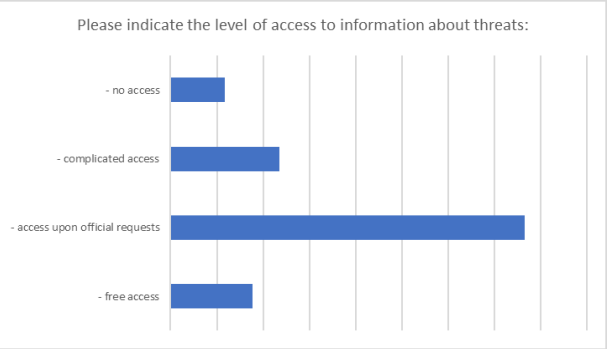
Based on the likelihood of occurrence, ML/TF risks in financial market transactions are categorized as high, medium and low. The level of risk is determined by: comparing the identified vulnerabilities with the actual volume of transactions to determine the likelihood of such transactions or services being used for ML/TF purposes; comparing the identified vulnerabilities with the level of threat posed by ML/TF offences; identifying ML/TF vulnerabilities in the conduct of financial market transactions.

Threat assessment

7. In terms of threat assessment, a special role is assigned to financial intelligence units, which supervisors believe should serve as a central point for collecting, summarizing and providing information on crimes, criminals and criminal proceeds that pose a threat to the sector. As an alternative, it is proposed to contact law enforcement, prosecutorial agencies or judiciary directly.

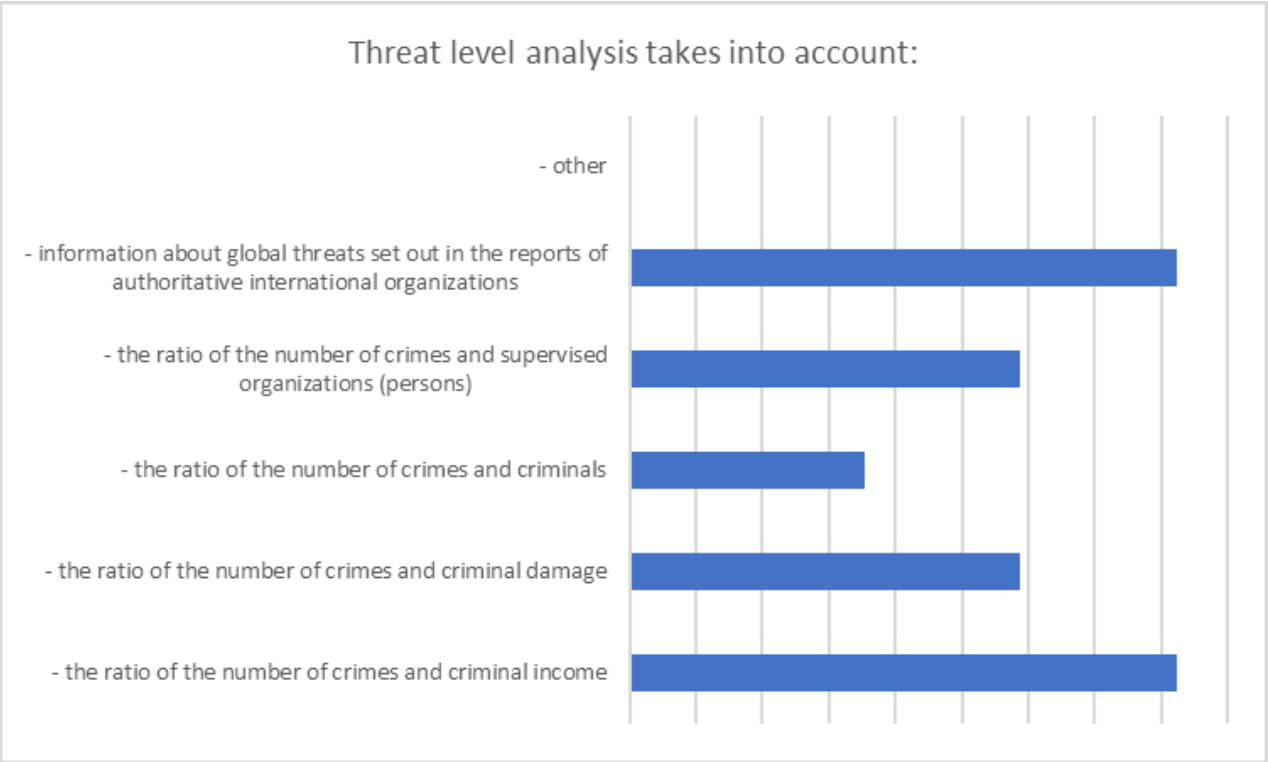
8. It should be taken into account that there is little or no free access to threat information. This information can be obtained through a formal request, but this information may be difficult or impossible to access.





9. The threat analysis may be carried out either by the authority that initiated the SRA itself or by a competent authority that has information about threats. The threat analysis should pay more attention to the frequency and volume of ML and TF.

10. In assessing the threat level of offenders involved in ML, consideration is given to those directly associated with the sector, as well as those who commit crimes as part of a group of individuals. In assessing the threat level of offenders involved in TF, consideration is given to those on terrorist or



extremist watch lists, as well as those who use sector services for TF or provide resources to third parties for TF purposes.

11. Threat level analysis requires an examination of the relationship between the number of crimes and criminal proceeds. It also requires an examination of global threat data as reported by reputable international organizations. To a lesser extent, the ratio of crime to the sector entities is considered.

The frequency of crimes committed and the damage caused can be used to assess the threat level of laundered money.

Criminal income and the value of confiscated property are less frequently taken into account.

12. Examples of threat assessment:

Example 1

Information on quantitative indicators of the ML/TF threat (statistical data from law enforcement agencies, prosecutors, customs and tax authorities, etc.).

Information on qualitative indicators of the ML/TF threat (investigative information, reports of government authorities, publications of international organizations such as FATF, IMF, World Bank, etc.).

Open sources of information, media, publications of non-profit organizations, etc.

Example 2

In assessing sectoral risks, the country follows the applicable recommendations of the FATF's Guidance on national ML/TF risk assessment and draws on the experience of the World Bank's risk assessment tools. The SRA will include both quantitative and qualitative analysis.

Threat assessments typically involve the collection and analysis of information and data, such as ML cases, predicate offence cases, and suspicious transaction reports. In processing this information, agencies typically conduct quantitative analysis of statistical trends in geographic patterns, the size and types of predicate offenses, the distribution channels for ML cases, and the volume of STRs involved.

In addition to quantitative data, relevant qualitative information, such as intelligence, expert opinion, private sector input, and reliable reports from relevant industry organizations, is used to better target the threat assessment.

Example 3

In the context of the 2020 SRA in the banking sector, the identification of threats for the sectoral assessment was carried out according to the following procedure:

1. Assessment of the scale and nature of socially dangerous acts preceding ML/TF:
   - Identification of the main types of socially dangerous acts preceding ML;
   - Collection of data on the scale and nature of terrorist activity within the country, in the region and in neighboring countries.

2. Identification of tools, methods and techniques used to conceal or disguise the illegal origin of proceeds or TF (typologies):
   - Identification of ML and TF methods and techniques;
   - Identification of the characteristics of the person carrying out ML or TF;
   - Determining the location of legalized proceeds or sources of TF;
   - Determining the time of ML and its duration;
   - Examples of ML and TF typologies.

Based on the results of the information study, a list of external and internal threats was compiled.

The external threats were identified as those threats, which are formed outside the AML/CFT system and it is impossible to counter them only by the efforts of the stakeholders of the national financial monitoring system.

For reference: External threats may be associated with any event in the financial market or in the economy, in particular:

- *The emergence of new financial products and services;*
- *The emergence of new financial institutions and/or intermediaries;*
- *The intensification of the activities of organized criminal groups;*
- *The commission of predicate or other offences;*
- *The implementation of illegal activities;*
- *An increase in the level of economic crime.*

Example 4

The 2019 SRA in the banking sector analyzed information received from law enforcement on ML-related predicate offences, with a particular focus on the banking products and services involved in these offences.

Global trends related to ML/TF in the banking sector were also examined, and interviews were conducted with experts in the sector to obtain their judgment on relevant issues in assessing threats to the sector.

Example 5

During risk analysis, the following information is requested from law enforcement agencies: ML/TF offences committed using products or services; predicate offences committed using products or services.

Example 6

Information on money laundering threats should include: the type of predicate offence; a summary of the offence; the product or service used for money laundering; the amount of money laundering and seized/confiscated property.

Example 7

ML and predicate offence threat analysis can collect and use criminal statistics on cross-border crime to assess risks from foreign jurisdictions in relation to a particular sector.

Example 8

When identifying ML threats, special attention is attached to:

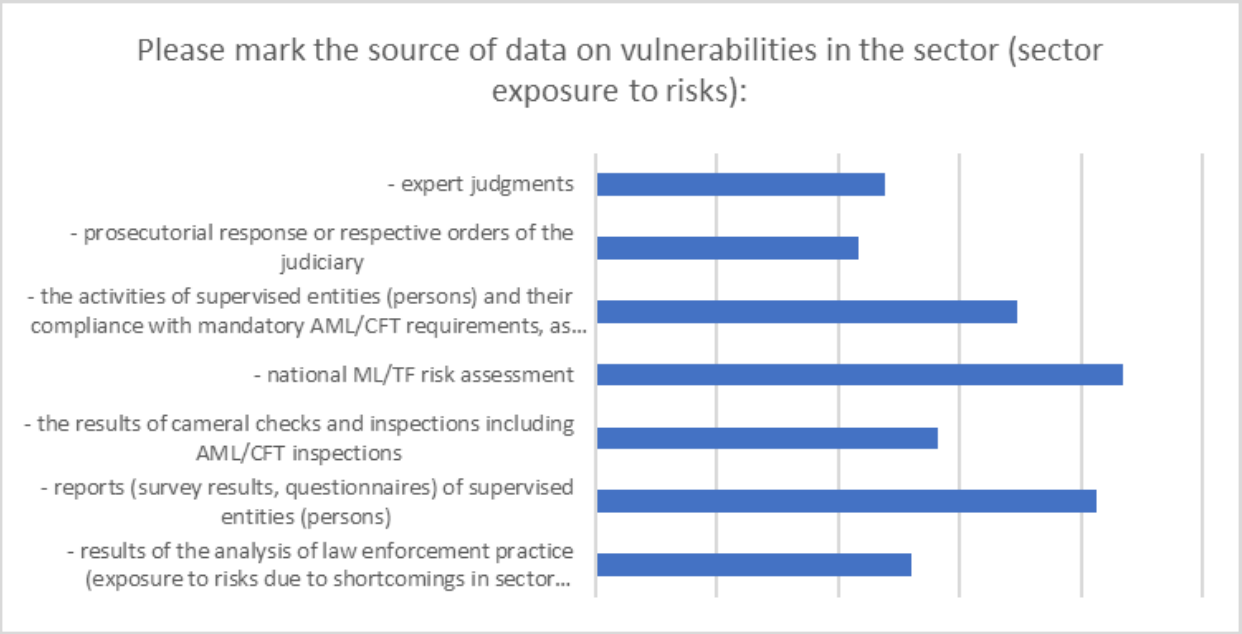
- the types of predicate offences being committed;
- the nature and scale of the relevant criminal activity in the country;
- the amount of proceeds of crime in the country;
- the cross-border flows of proceeds of crime;
- the amount of proceeds of crime committed abroad and laundered at home;
- the sources, locations and concentrations of criminal activity;
- the nature and extent of terrorist activities and terrorist groups in the country;
- available information on the nature and scope of terrorist activity and terrorist groups in neighbouring countries and regions.

In addition to the aforementioned factors, attention is attached to the existence of favourable conditions for the training of terrorists, formation of terrorist groups, commission of terrorist acts, and financing of terrorism.

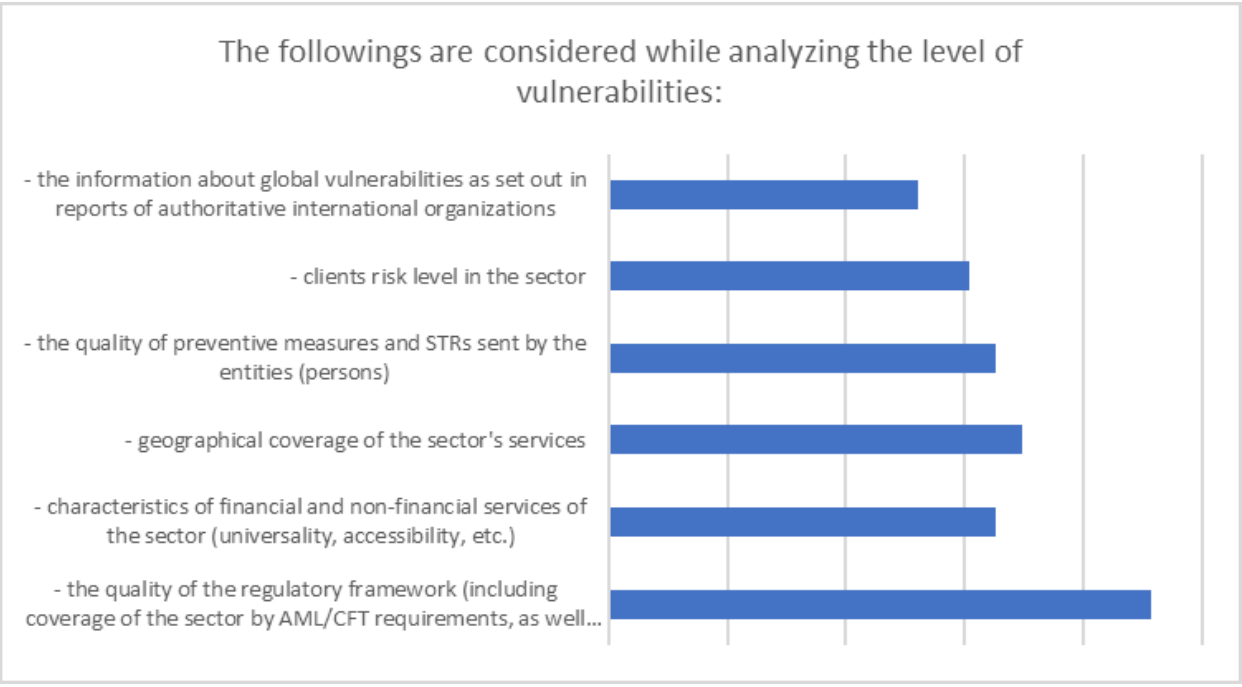
Vulnerability assessment

13. A wide range of data is used as a source of data on vulnerabilities in the sector, including the results of the NRA, the results of a questionnaire survey of the sector entities, their practical activity, the results of a study of law enforcement practices, the findings of desk audits and inspections, as well as orders of law enforcement agencies and special court rulings.

14. In cases of insufficient information, expert opinion is used.



15. The vulnerability level is most influenced by the quality of legislation governing the sector's activities and supervision, the quality of the sector's preventive measures, the geography and risks of customers, and the specifics of the sector's services. The smallest source of information on vulnerabilities can be information on global vulnerabilities in the reports of international organizations.



16. The analysis of the quality of preventive measures is based primarily on the study of the reports of the sector entities, the results of inspections and sanctions applied, information from law enforcement or judicial agencies. To some extent, the results of desk audits should be used.

17. Reports by international organizations will be used in conjunction with other sources of information on vulnerabilities. Such reports should play a complementary rather than a dominant role.

18. Examples of vulnerability assessments:

Example 1

The information for the analysis of information on vulnerabilities is obtained (collected) from various sources (complaints of natural and legal persons, court decisions, the Internet, information obtained within the framework of control (supervisory) functions, etc.), including reports of reputable international organizations and questionnaires developed by the Main Insurance Supervision Department and completed by insurance companies.

Example 2

Supervisors can develop a matrix to conduct a simplified risk assessment of less complex entities, such as auditors with low ML/TF risk exposure. Such matrices can be used to collect information on DNFBPs' activities and operations, products and services, customer characteristics, etc.

Example 3

The vulnerability of the sector is assessed using data from reports filed by reporting entities to the supervisor, which includes information on suspicious transaction reports submitted to the FIU.

Example 4

- Data on the freezing of assets and the blocking of transactions of persons involved in terrorist activities;
- Data on the number of actions taken by judicial and law enforcement agencies conducting criminal proceedings to impose restrictions on funds and other assets of customers of financial institutions;
- Information on the number of inspections conducted by the supervisor, violations and deficiencies found, and actions taken;
- Information on quantitative and qualitative indicators of the sector from scheduled reports, National Bank questionnaires, etc.;
- Information on types of products/services, customers, delivery channels, geographic factors, etc.

Example 5

When assessing risks of the DPMS sector based on its characteristics, the authorities analyze vulnerability in all sub-sectors: mining, processing, retailing and recycling. Similarly, when assessing risks in the real estate sector, vulnerability is also assessed in the following three types of real estate businesses: sales of newly constructed real estate, real estate brokerage, and real estate appraisal or expertise.

When assessing vulnerability, it is also important to analyze inherent risks from various perspectives, such as customer, geography, services provided, and the effectiveness of preventive measures. As a result of the joint analysis of inherent risks and preventive measures, the level of residual risks, including high-risk areas in the sector, can be determined.

Example 6

SRA in the banking sector (2020), in identifying the vulnerabilities associated with the use of different types of legal persons, explored the following questions through a survey:

- What types of legal persons account for the largest proportion among the customers;
- What types of corporate customers are high risk;
- Financial transactions of which types of corporate customers have raised ML/TF suspicions and information on which has been submitted to the FIU;
- What types of legal persons have been denied business relationships/transactions.

In order to identify and assess vulnerabilities, information received from law enforcement agencies on predicate offences for ML was analyzed, with a particular focus on the banking products and services involved in these offences.

Example 7

Information and data are requested from financial institutions in the following areas: general description of activities, including types of transactions, statistics on volume of transactions, etc.; information on circumstances affecting ML/TF risks; information on internal control measures.

Vulnerability information should describe the circumstances that occur or are likely to occur in transactions.

Example 8

Information for vulnerability analysis is obtained from a variety of sources.

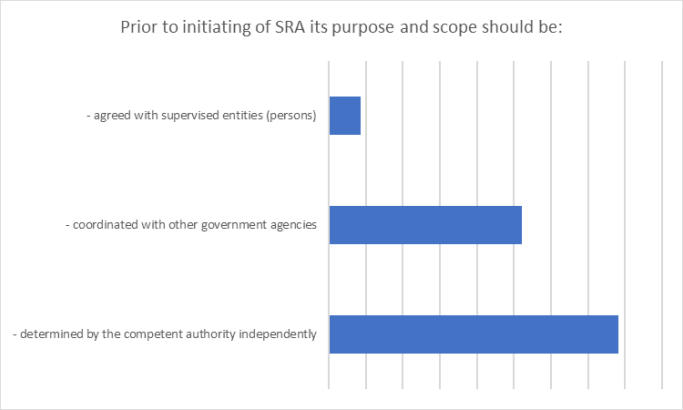
The general situation in the sector concerned, the volume of transactions, the presence/absence of internal control rules on the part of those carrying out financial transactions and their implementation in practice are investigated.

In identifying vulnerabilities, special attention is also paid to:

- the existence of financial transactions involving cash;
- types of customers;
- presence of high-risk customers;
- conducting business and customer base in high-risk geographic areas (states and territories that do not comply with FATF Recommendations, offshore zones, states with high terrorist activity);
- compliance with the requirements of regulations relating to clients;
- the presence of non-resident clients;
- implementing customer due diligence;
- ongoing due diligence, including monitoring of transactions;
- identification of beneficial owners;
- implementation of STR referral measures;
- existence of internal controls;
- blocking of financial transactions;
- freezing of funds;
- data retention;
- AML/CFT skills development.

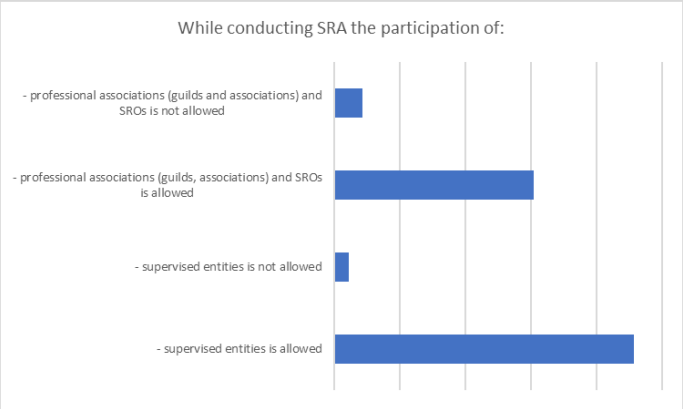
ML/TF risk assessment

19. Prior to conducting an SRA, its purpose and scope are generally determined by the government authority or SRB initiating the assessment and coordinated with other government authorities, if appropriate.



In determining the scope of the SRA, the context of the sector and its share in the total volume of the country's financial market are taken into account.

20. The participation of the sector entities in the SRA is mandatory. In addition, professional associations of the sector entities should be allowed to participate in the SRA.

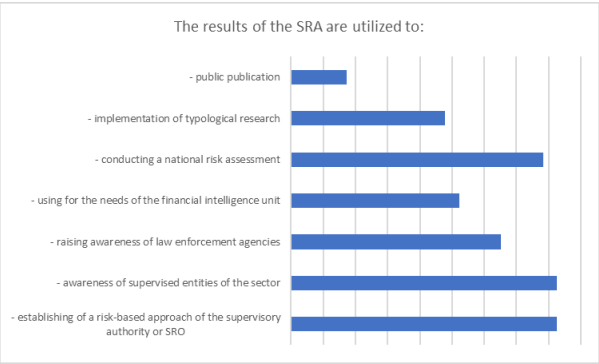


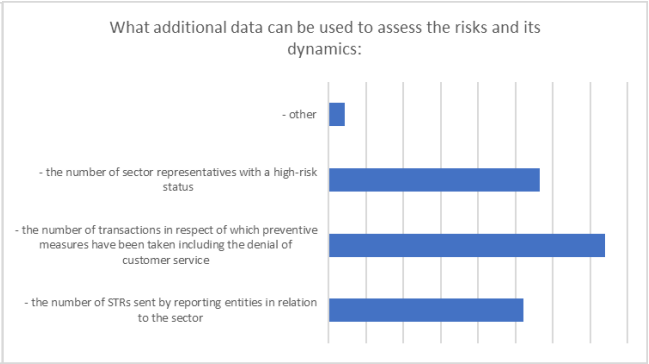
The SRA necessarily take into account the results of the NRA and the reports of entities on existing risks. As mentioned above, supervisory materials and reports from international organizations are also used.

A vulnerability assessment is used to determine the likelihood and consequence levels of a threat materialization.

21. Additional data should be used in the SRA process, including information on preventive measures taken up to and including refusal to conduct transactions, the volume of STRs reported by the sector and the number of high-risk entities in the sector.

22. The results of risk assessments are generally used for a variety of purposes, including: updating the NRA, applying risk-based supervision, raising awareness among the sector entities and law enforcement agencies, as well as for the needs of the FIU and conducting typologies studies.





23. The decision to publish the results of the SRA will be made independently on a case-by-case basis.

24. Examples of ML/TF risk assessment:

Example 1

Regular or ad hoc requests by DNFBPs (auditors) to reporting entities aimed at obtaining quantitative and qualitative data and information from them on key ML/TF risk indicators (e.g., lines of business, business segments, types of customers) and general information about the entities and the nature and scope of their activities.

Example 2

The use of regularly updated questionnaires on DNFBPs' ML/TF risk management controls, existing management systems, changes and additions to relevant policies and procedures, reliability of controls, etc., will allow supervisors to form an early view of the adequacy of the controls implemented by DNFBPs to mitigate ML/TF risks and to plan targeted supervisory activities.

The level of risk (low, medium, high) is determined based on the developed matrix by comparing the threat and vulnerability levels. The threat and vulnerability levels are determined by experts based on the analysis of all available information.

Example 3

The following are used to assess risk:
- Suspicious transaction reports;
- Reports on inspections of reporting entities, information on actions taken, etc.
- Information received from other government authorities (law enforcement agencies, tax authorities, prosecutors, etc.)

Example 4

In assessing sectoral risk, the country used the second generation of the World Bank's NRA toolkit to separately assess the threat and vulnerability levels. The threat and vulnerability levels were then mapped into a two-dimensional risk matrix to reflect the overall level of sectoral ML/TF risks.

Example 5

As part of the 2020 SRA in the banking sector, when determining the level of sectoral ML risk, the Central Bank has examined the following characteristics of the sector:
• Completeness and effectiveness of legal regulation of the sector with respect to ML;
• General review of the ML-related criminal situation in the sector;
• Status of compliance of reporting entities with legal requirements in the field of preventing and combating ML;
• Effectiveness of regulation and supervision of entities in terms of ML;
• Model ML schemes involving the sector entities.

Example 6

As part of the 2020 SRA in the banking sector, STRs were examined in terms of customer types, products/services, distribution channels and geographical characteristics.

When analyzing the information provided by financial institutions to identify and assess the level of vulnerability, attention is paid to the presence of: transactions in the activities of financial institutions that are sensitive (vulnerable) to misuse for ML/TF purposes; circumstances that increase ML/TF risks; weaknesses in the organization of internal controls.

The information gathered is analyzed and an opinion is formed on the nature and likelihood of ML/TF risks in the financial market, based on the high-risk conditions, the state of internal controls, and existing threats.

25. Interagency cooperation among the government authorities, as well as interaction with self-regulatory bodies existing in the sector, is important to the effective implementation of the SRA.

26. Examples of interagency coordination:

Agencies	Purpose of coordination	Format	Brief description
Judicial authority	Implementation of the FATF Recommendations	Interaction with the FIU	Establishing a transparent beneficial ownership identification mechanism
FIU	Implementation of the FATF Recommendations	Regular publication of typologies	Information on predicate offence typologies enables effective assessment of sectoral ML/TF risk level by matching threat level to vulnerability level
FIU	Implementation of the FATF Recommendations	Feedback from reporting entities	Existence of a feedback loop with persons engaged in financial transactions, based on the results of the examination of the information provided and special reports (STRs)
Financial regulators	Unified approach to risk assessment in the financial sector	Meetings with representatives of agencies, meetings with the private sector representatives	As a result of joint activities, unified approaches to the methodology of risk assessment of financial institutions have been developed, sectoral risk assessment reports have been reviewed and approved
Interagency AML/CFT Commission or FIU, law enforcement agencies and supervisory authorities	Timely exchange of information for SRA purposes	Providision of information to interested ministries and agencies	Law enforcement agencies prepared a threat report, which is provided to the supervisory authorities for use in the SRA
Judicial authorities	Identification of ML/TF threats to NPOs	Interagency Group	1. Risk identification working groups are held every three months; 2. A working group is established to identify threats and risks
Supervisor and FIU	Data exchange	Regular reporting by reporting entities	Generation of data on vulnerabilities and risks of reporting entities
The AML competent authority and SRB	Sectoral risk assessment	Joint discussions and interviews, formal consultations and information sharing	In assessing ML risk of the DPMS sector, the AML competent authority and SRBs jointly developed private sector questionnaires and conducted interviews to understand the scope, patterns, internal controls, and relevant information about the sector
Working Group on preparation of the country for ME and NRA	Preparation for ME and NRA	Online and in-person meetings	Preparation of the country for the second round of mutual evaluation and national risk assessment

II. Recommended approaches to conducting the SRA

General provisions

27. The following recommended approaches are based on the study of relevant FATF guidances, examples of best practices of the EAG Member States' supervisory authorities and are intended for use in conducting sectoral risk assessments in the EAG Member States.

28. The recommended approaches are not mandatory, but are intended to assist supervisors in selecting principles and approaches for conducting sectoral ML/TF risk assessments.

29. Sector risk assessment (SRA) means a set of activities related to the collection, consolidation, and analysis of quantitative and qualitative information to determine the likelihood that ML/TF threats will be materialized through sector vulnerabilities with consequences in the form of ML or TF.

Preparation for conducting the SRA and its frequency

30. The frequency with which SRAs are conducted is to be determined by the supervisor. The reasons for conducting an SRA may include:

- The need to update the information on ML/TF risks in the sector gathered as a result of the previous SRA;

- Significant changes in the volume of transactions, quantitative and qualitative composition of the sector;

- The identification of new ML/TF typologies and patterns in the sector or global reports by international organizations.

31. The SRA can be carried out either before or after the national risk assessment. In general, an SRA precedes a national risk assessment (NRA), with the NRA taking into account the results of the SRA. However, conducting an SRA after the NRA can have a positive impact on supervisors' understanding of ML/TF risks in the supervised sectors.

32. The SRA should be conducted among reporting entities engaged in similar types of activities. It is acceptable to group reporting entities by type of activity (e.g., financial or non-financial, credit or payment services, etc.) for SRA purposes if these sectors have a small separate volume of transactions or if the SRA is aimed at assessing the risks associated with a particular type of financial or non-financial activity.

33. The SRA is conducted by a government authority and/or self-regulatory body that exercises supervisory functions in the sector, either independently or jointly with the FIU.

34. The decision to start an SRA should be taken by its initiator. At the same time, where the SRA is carried out before the NRA, it is advisable for the decision to start the SRA to be taken by the coordinating interagency body, where such a body exists, to enable agreement to be reached on the timing, objectives and scope of the SRA in all the sectors under assessment.

35. It is advisable to develop and approve a methodology for conducting an SRA before it starts. The methodology should include approaches to data collection and analysis, and the formulation and publication of conclusions on risk levels. It is recommended that the SRA methodology be coordinated with the FIU or an interagency coordinating body.

36. In addition to the decision to start the SRA and approval of the methodology, an SRA work plan must be developed and approved, which should include:

- SRA objectives and timelines;

- The list of information sources to be analyzed and the procedure for analyzing them;

- Description of the resources involved in the SRA;

- Tools and procedures for interacting with reporting entities, the FIU, other government authorities, and SRBs;

- The format of expected SRA results, objectives and procedures for their use.

SRA objectives and timeline

37. The objectives of the SRA may include:

- Determining the causes and conditions of ML/TF risk exposure of reporting entities required to apply AML/CFT measures, including the reporting of suspicious transactions to the FIU;

- Determining the dynamics of the ML/TF risk level in the sector as a whole, as well as in its individual segments (types of activities of reporting entities);

- Updating the AML/CFT risk assessment model developed by supervisors for the purpose of planning supervisory activities;

- Prioritizing supervisory activities and effectively allocating resources for desk and on-site inspections, including their frequency and depth;

- Determining the level of attention to be given to relevant activities and reporting entities, and identifying risks that require priority attention;

- Developing measures to mitigate ML/TF risks in the sector;

- Assessing the effectiveness of measures taken to mitigate ML/TF risks in the sector, based on the results of the national ML/TF risk assessment and the previous sectoral ML/TF risk assessment;

- Raising awareness among reporting entities of ML/TF typologies available in the sector;

- Preparation of a national risk assessment.

38. The timeline of the SRA depends on its purpose and is determined by the initiating body or the coordinating interagency body. The latter is preferable from the point of view of planning to conduct SRAs in several sectors at the same time and subsequently use their results to conduct NRA.

Recommended information sources for conducting an SRA, interacting with the sector entities, FIU and other government authorities

39. Prior to launching an SRA, the initiating authority should establish a preliminary list of data required for the analysis, identify sources, and assess the level of availability of such data.

40. Internal sources of information available to the supervisory authority may include the following:

- Results of remote monitoring, control (supervision) activities in the field of AML/CFT, including preventive and control measures, carried out in relation to the sector entities;

- Generalized data of questionnaire survey of representatives of supervised sectors, professional organizations (associations, guilds), as well as specialists of the supervisory authority. Sample forms of questionnaires by sectors are provided in the Chapter III;

- Complaints from citizens, requests from the FIU, law enforcement agencies, tax authorities, prosecution agencies, other government authorities and foreign partners received by the supervisory authority.

41. External sources of information to which supervisors may have access, either as part of the FIU's feedback or upon request, include:

- The results of financial investigations involving the sector entities (their counterparties, customers);

- Identified typologies and schemes of ML and TF used in the sector (with the participation of the sector infrastructure);

- The results of the analysis of law enforcement practice;

- Official statistical data;

- Results of analytical studies conducted by rating, information and analytical agencies, international organizations;

- Media reviews;

- Information from reference and information systems.

42. When conducting an SRA, it is advisable to cover as many reporting entities as possible. In sectors with a large or unknown number of entities, it is recommended to cover the number of entities that will provide confidence that the results obtained are correlated with the sector as a whole.

43. Channels of communication with the sector entities should be identified before conducting an SRA. The most effective channels may be questionnaire surveys (*highest coverage, probability of unreliability*), meetings (*high coverage, lower efficiency*), interviews (*low coverage, high reliability*), publications on the website (*high availability, probability of untimely communication*), official correspondence (*moderate availability, timely communication*), etc. The effectiveness of communication will significantly increase the involvement of the territorial branches of the supervisory authority or SRBs.

Description of the sector and its structure

44. The purpose of this stage is to determine the main data characterizing the sector in the context of the risk assessment, including:

- the number of entities in the sector, as determined by the number of licenses issued (permits, registrations, records, notifications, etc.), adjusted for the number of entities actually operating;

- the total value of assets (*for financial sectors*) or the volume of transactions conducted in quantitative and monetary terms (*for non-financial sectors*), where possible;

- the total number of customers in the sector[1];

- the specifics of the sector's organization (*regulation and supervision, institutional characteristics, availability of sectoral AML/CFT legislation, quality of preventive internal controls, etc.*);

- Assessment of the sector's share in the financial market structure (for financial sectors) or the sector's share in the total volume of non-financial services[2] (for non-financial sectors);

- The importance of the sector and its individual segments in the national AML/CFT system.

45. An important element of the description of the sector is the analysis of the specifics of regulation, the existence of special requirements for licensing, including mechanisms to exclude criminals and their accomplices from beneficial ownership and control of the activities of the sector entities.

46. Structuring the sector involves determining the quantitative composition of its segments. To structure the sector, the criteria most relevant to risk assessment (size, type of activity, form of ownership, geographic reach, etc.) are identified.

47. This stage also determines the dynamics of the indicators that are universally used to assess the risk exposure of sectors or their individual segments:

- the proportion of cash settlements;

- the proportion of cross-border transactions, including those with high-risk jurisdictions[3];

[1] It is advisable to exclude from the number of customers those who make one-off transactions, those who have been inactive for more than two years, or those who have ceased business relationships at the time of the SRA.
[2] Refers to non-financial services falling within the definition of DNFBPs as set forth in the FATF Glossary.
[3] High-Risk Jurisdictions subject to a Call for Action

- the proportion of transactions with politically exposed persons, other high-risk customers and non-residents;

- the proportion of entities in the sector or their customers that have the indicators of shell companies.

48. Information received by the FIU can be used to assess the dynamics of the indicators characterizing the scope of activity and risk exposure of the sector. For example, the volume and number of transactions subject to mandatory control, expert assessment of the current state and trends in the development of the sector (type of activity), information received from representatives of the sector during a questionnaire survey, etc.

Assessment of the threat level in the sector

49. In the context of the SRA, threat refers to the level of criminalization of the sector, the characteristics of the conditions and environment in which predicate offences are committed and criminal proceeds are generated, the criminals and criminal groups that use sector entities to commit ML/TF offences, and the scale or volume of criminal activity in the sector.

50. The threat assessment is an analysis of the number and methods of ML/TF offences committed by the sector entities, the characteristics of those convicted of committing them, and the amount of criminal proceeds generated.

51. The source of data on threats is aggregated information from the FIU, law enforcement agencies and special government authorities, customs or tax authorities, prosecutor's offices and courts. At the stage of preparation of the SRA it is necessary to identify the government authority that will be the source of information on threats and plan the procedure for obtaining such information (using connections to common databases, direct requests or requests through other government authorities, etc.).

52. Collection of the threat level data includes the following activities:

a) Generating and analyzing quantitative and qualitative data on criminal cases of ML/TF offences (*by type of offence*) committed using sector infrastructure, including:

- the dynamics of the number of criminal cases and the number of persons prosecuted (by year). Comparing the data for the sector with the overall aggregated data can give an idea of the level of criminalization of the sector;
- court sentences that have entered into force for ML offences and other economic crimes;
- court sentences that have entered into force for TF offences;
- requests from law enforcement agencies, tax authorities, prosecutor's offices, the FIU, other government authorities and foreign partners;
- appeals from citizens, information from the mass media containing information about the possible commission of crimes using the infrastructure of the sector entities;
- findings of financial investigations and analytical reports on the results of control (supervisory) activities;

b) Selection of anonymized criminal case studies, which will allow to demonstrate the algorithm of actions of criminals, schemes of committing crimes;

c) Formation and analysis of the results of the questionnaire survey of the sector representatives on the level of threats in the sector (assessment of the level of criminalization and its dynamics, etc.).

53. In assessing the level of threat posed by the laundered proceeds, the frequency of the offences committed and the amount of criminal proceeds generated should be taken into account. In the absence of information on the amount of criminal proceeds, criminal damage may be taken into account. However, this approach is likely to distort the result, as criminal proceeds and criminal damage may differ significantly.

54. When assessing the level of threat posed by criminals, those directly linked to the infrastructure of the sector or involved in criminal groups should be considered. Particular attention should be paid to those on sanctions lists.

55. In cases of insufficient information or lack of access to threat intelligence, threat intelligence reported by reputable international organizations may be used. It should be noted that the use of global threat intelligence may distort the SRA results and reduce the effectiveness of risk mitigation measures in the sector.

56. The assessment of the level of threat is carried out by experts on the basis of data on threats in the sector, based on the results of the previous risk assessment, as well as the results of the analysis of the above-mentioned statistical data and contextual information.

57. The number of threat levels is chosen by the body conducting the SRA, and it is recommended that at least three threat levels (low, medium, high) be used. In the case of large variations in the initial data analyzed, intermediate threat levels (moderately high, moderately low, etc.) may be used.

Vulnerability level assessment (sector exposure to ML and TF risks)

58. The concept of "vulnerability" in the context of ML/TF risk assessment includes deficiencies in legislation or weaknesses in the application of internal controls by reporting entities, including those resulting from gaps in supervisory activities, which may lead to the materialization of the ML/TF threat. Vulnerabilities are categorized as internal and external to the sector entities.

59. External vulnerabilities include factors that determine the sector's exposure to risks due to:

- imperfect legislation (*lack of mandatory AML/CFT requirements, including the exclusion of persons with unexpunged or unspent convictions for economic crimes from beneficial ownership and control of the organization, etc.*);

- poor supervision (*deficiencies in the application of the risk-based approach, insufficient resources for AML/CFT supervision, low number of supervisory activities and preventive measures, etc.*), low level of AML/CFT coverage of the sector;

- lack of mechanisms to monitor compliance with AML/CFT requirements in financial groups (*consolidated supervision, internal audit, etc.*).

60. Internal vulnerabilities include factors that determine the sector's exposure to risk due to:

- inadequate compliance with AML/CFT legislation (*in terms of implementation of internal controls, risk assessment, interaction with the FIU, including suspicious transaction reporting, etc.*);

- insufficient awareness among the sector entities of ML/TF risks, typologies and indicators of suspicious transactions, as well as ineffective application of risk mitigation measures and identification of suspicious transactions;

- the specificities of the type of activity, universality, availability and accessibility of the financial services provided by the sector entities, which make them attractive for ML or TF purposes.

61. When the level of vulnerability is high, criminals incur relatively low costs in using the sector's infrastructure for ML/TF purposes and/or the sector provides a higher level of latency for ML/TF offences.

62. External vulnerabilities can be analyzed by assessing the technical compliance of the industry's AML/CFT legislation with international standards, assessing the quality of measures taken to mitigate ML/TF risks identified in previously conducted SRAs, and examining the quality and scope of AML/CFT supervision of reporting entities, including consolidated supervision.

63. The following information is used to assess the level of compliance with mandatory requirements by the sector entities:

a) the results of questioning the sector entities (indicators of practical AML/CFT activities, information on the client base, information on the products and services offered, including the channels through which they are provided, the existence of indicators of high-risk operations, etc.). Sample questionnaires are provided in Chapter III;

b) analysis of the quality of the implementation of internal controls, the availability of sufficient resources to meet AML/CFT requirements, the level of automation of business processes, and the interaction with the supervisor, the FIU, other government authorities, and the sector entities;

c) dynamics of the number and share of entities with a low risk of non-compliance with the requirements of AML/CFT legislation;

d) information characterizing the level of the sector's involvement in suspicious transactions, the dynamics of the volume of suspicious transactions involving representatives of the sector, the number of participants in such transactions;

e) the dynamics of refusals to conduct transactions or establish business relationships;

f) the results of supervisory actions, including:

- the proportion of inspections that identify violations, including serious violations of AML/CFT legislation;
- a list of the most frequently detected violations of AML/CFT legislation;
- the proportion of repeated inspections with detected violations;
- the dynamics of the number and proportion of entities that have evaded the elimination of violations;
- the dynamics of the number and proportion of entities that evaded the payment of fines;
- inspections leading to the imposition of administrative sanctions in the form of warnings;
- information on rulings, orders, warnings from law enforcement and judicial agencies, customer complaints against the sector entities received by the supervisor.

g) Statistics on the use of the sector's products or services to commit the most typical ML/TF offences.

64. The assessment of the level of vulnerability is carried out by experts on the basis of data on the level of vulnerability in the sector, based on the results of the previous risk assessment, as well as the results of the analysis of the above-mentioned statistical data and contextual information.

65. In the case of insufficient information, expert opinion of persons directly involved in the supervisory activities of the sector entities with the participation of specialists of reporting entities may be used.

66. Where there is insufficient understanding of the actual vulnerabilities of the sector, it is possible to use the information on typical inherent vulnerabilities provided in the relevant FATF Guidances on the application of the risk-based approach to supervision (Annex). It should be noted that this information should be complementary rather than predominant.

67. The assessment of vulnerability levels may be based on the scope, depth and significance of the identified deficiency in legislation, internal controls or supervisory activities. The number of vulnerability levels is selected by the body conducting the SRA, and it is recommended that vulnerabilities be assessed in at least three levels (low, medium, high). Intermediate levels of vulnerability (moderately high, moderately low, etc.) may be used if there is a wide variation in the baseline data to be analyzed.

68. The result of this stage is the identification of the main vulnerabilities that characterize the sector and its individual segments, as well as the measures (supervisory, legislative, organizational, etc.) to address them.

Assessment of likelihood

69. Matching threats and vulnerabilities provides an idea of likelihood as the potential probability of ML/TF risk events occurring.

70. A likelihood assessment is an optional component of an SRA, but can provide a clearer picture of the level of ML/TF risk and help to appropriately prioritize mitigation measures.

71. The level of likelihood can be assessed by comparing the number of ML/TF offences (threats) committed using the identified sector vulnerability to the total number of ML/TF offences in the sector.

72. In the absence of sufficient information for such a comparison, it is possible to use expert opinions to assess the materialization of certain threats through specific sectoral vulnerabilities.

73. The number of likelihood levels generally depends on the number of threat and vulnerability levels selected.

Assessment of consequences

74. Consequences refer to the impact or damage that may be caused by the materialization of ML/TF risks and include the effects of criminal activity on financial systems and institutions, on the population, on specific groups of people, on the business environment, on national or international interests, and on the reputation and attractiveness of a country's financial sector and economy as a whole.

75. A measure of the amount of damage done to the national economy as a result of ML/TF offences using the infrastructure of the sector can be used to assess the consequences.

76. In view of the difficulties associated with the formation of statistical and other data necessary for determining or assessing the consequences of ML/TF, it is permissible to limit the formation of conclusions to an expert opinion, taking into account, inter alia, the results of the questionnaire survey of representatives of the supervised sector. Taking into account the negative nature of ML/TF, it is permissible to apply a consistently "high" level of consequences when conducting an SRA.

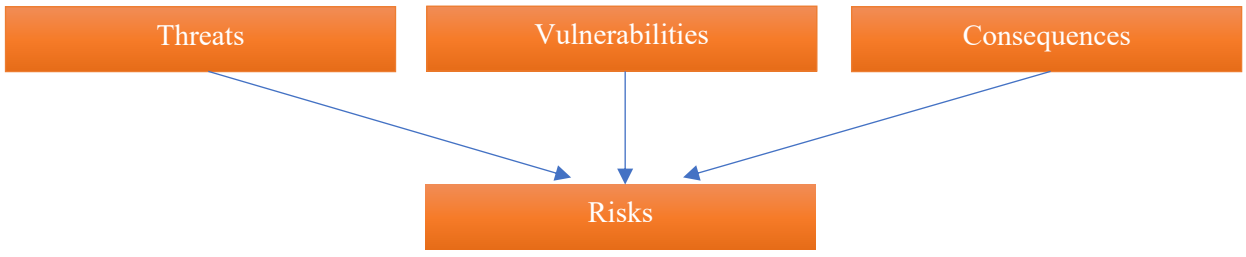
77. The assessment of the level of consequences is carried out by experts on the basis of data on the significance of consequences in the sector, based on the results of the previous risk assessment, as well as the results of the analysis of the above-mentioned statistical data and contextual information.

Sectoral ML/TF risk assessment

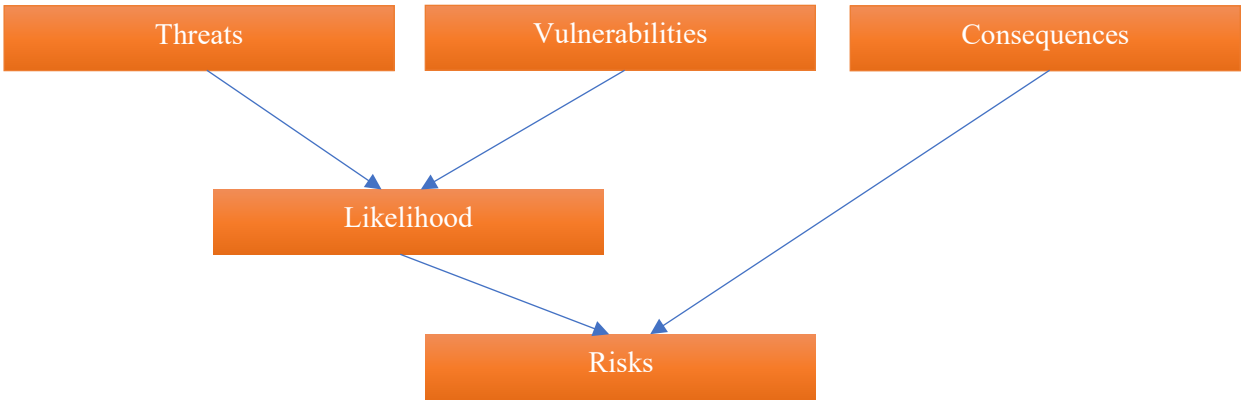
78. For the purposes of the SRA, ML/TF risks can be divided into inherent and residual risks. Inherent risks refer to the degree to which a threat is materialized through sector vulnerabilities that lead to consequences.

79. The level of inherent ML/TF risk is assessed by comparing:

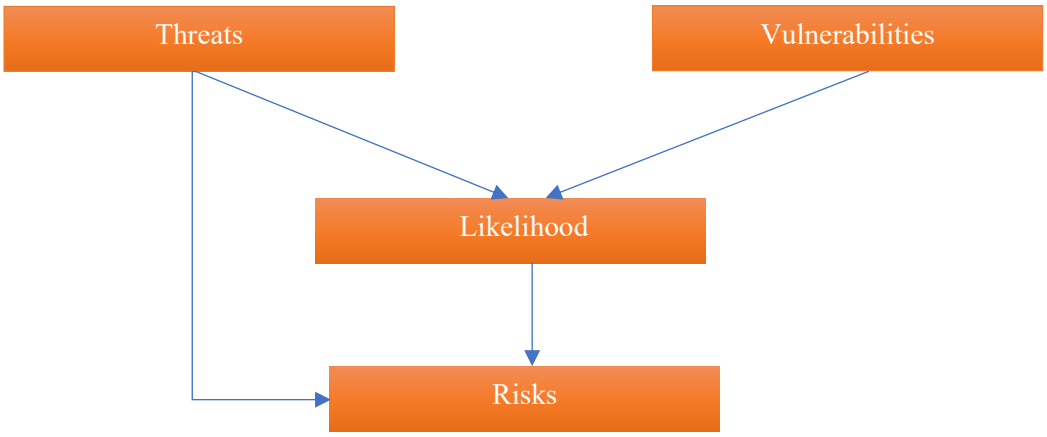
a) Threats, vulnerabilities and consequences, where consequences are assessed and where likelihoods are not (Model 1)



b) Likelihoods and consequences – in the case of assessing likelihoods and consequences (Model 2)



c) Threats and consequences – in the case of assessing likelihoods and applying a consistently "high" level of consequences (Model 3)



80. The assessment of inherent ML/TF risks should take into account the results of previous SRAs and NRAs, as well as reports from reporting entities on identified risks.

81. Residual risk is the level of inherent risk after the application of preventive measures aimed at reducing it. Residual risk is calculated on the basis of the difference between the materialization of threats before and after the application of preventive measures, if such statistics are available. In the absence of such statistics, the residual risk can be calculated on the basis of expert opinion.

82. Residual risk can be estimated by comparing the level of inherent risk with the level of effectiveness of available mitigation tools. For instance, residual risk is high when the inherent risk is deemed high and the mitigating tools are considered to be ineffective or insufficient.

Formalization and approval of the results of the sectoral risk assessment

83. Prior to formal approval, it is recommended that the results of the SRA be discussed with the FIU, representatives of professional organizations (associations, guilds, etc.), and specialists from other supervisory authorities in the field of AML/CFT.

84. Preliminary discussion of the SRA results may also take the form of consultative meetings with the private sector representatives. In this case, the results of the meetings should be taken into account in the preparation of the final report on the SRA results.

85. The results of the assessment of the dynamics and level of threats, vulnerabilities, likelihoods, consequences and risks of transactions (financial operations) for the purposes of ML/TF in the activity area of reporting entities, as well as the recommended measures to mitigate these risks, shall be formalized in the form of a report on the SRA results, which may include the following sections:

I. General characteristics of the sector.

II. Characteristics of threats.

III. Characteristics of vulnerabilities.

IV. Characteristics of likelihoods/consequences.

V. Comparative assessment of ML/TF risk level in the sector, current ML/TF typologies and schemes.

VI. Recommended risk mitigation measures in the sector.

86. The SRA report is recommended to include ML and TF typologies (schemes), which are implemented using the products and services of the sector. For clarity, the typologies are visualized, equipped with a brief description of the profile of participants, operational and behavioral indicators characterizing the typology (scheme).

87. The construction of a matrix of risks (both inherent and residual) is left to the discretion of the body conducting the SRA. However, it is recommended that the results of the SRA be presented in a visualized form that clearly shows the type and level of ML/TF risks in the sector. Such an approach will make it much easier for reporting entities to understand the risks.

Risk matrix - sample 1

Threats \ Consequences	Low	Medium	High	Medium	Low	Vulnerabilities
Low						Low
Medium						Medium
High						High

Risk matrix - sample 2

Likelihoods \ Consequences	Low	Medium	High
Low			
Medium			
High			

Risk matrix - sample 3

Threats \ Likelihoods	Low	Medium	High
Low			
Medium			
High			

88. Based on the results of the risk assessment, a list of recommended measures to mitigate risks in the sector should be prepared with a possible timetable for their implementation, including:

- proposals for improving legislation;

- proposals for adjusting the organization (planning) and implementation of supervisory activities, improving the application of the risk-based approach to supervision, etc.;

- measures to improve the internal control systems of reporting entities, including the implementation of CDD measures, monitoring of business relationships, including enhanced monitoring, data analysis and storage, reporting of suspicious transactions, application of targeted financial sanctions, etc.;

- measures to strengthen interagency cooperation with the FIU, law enforcement agencies, and special government authorities, as well as international cooperation with foreign supervisors;

- measures to conduct AML/CFT/CPF training of the staff of the supervisory authority and reporting entities.

89. The results of the SRA may be reviewed and approved both at the supervisory authority level and at the level of the interagency AML/CFT/CPF coordinating body. As a general rule, the SRA report is approved by the body that made the decision to conduct the SRA.

90. Supervisors should always communicate the SRA results to reporting entities. For this purpose, it is recommended to use official websites or pages of supervisors in social networks, as well as to hold explanatory and training activities or events of a supervisory nature.

Using SRA results

91. The SRA results are used according to the objectives set at the time of the decision to conduct the SRA. Most commonly, the SRA report is used to revise the supervisory strategy, improve risk-based supervision, and raise awareness among the sector entities and law enforcement agencies.

92. The principles of a risk-based approach to supervision are recommended to be set out in a document, which, at a minimum, should contain:

1) criteria for assigning risk levels to reporting entities based on the structure of the client base (*in terms of riskiness*), types and geographic coverage of services (products) and channels of service provision (e.g., remote provision of a service or provision of a service without proper customer due diligence);

2) procedures for conducting documentary audits of supervised entities for compliance with AML/CFT/CPF requirements, including, but not limited to, reporting pro-forms; the way of their collection; data analysis and use of the results of the analysis; structure, number, functions and responsibilities as well as qualification requirements for persons responsible for documentary audits;

3) The procedure for designating and conducting AML/CFT/CPF inspections of reporting entities, including the general procedure for designating on-site inspections (*e.g. inspection plan, order, etc.*); the procedure for selecting entities for inspection based on the risk level determined by the criteria and results of documentary inspections; the depth of inspection (*e.g. period, types of services, types of customers, geographic coverage areas, etc.*); the structure, number, functions and responsibilities and the qualifications for those responsible.

4) The basis and procedure for applying various types of corrective measures or sanctions when violations of AML/CFT/CPF requirements are identified, including the criteria for sending written notices to rectify the violation; holding meetings with the entity's management; applying financial sanctions; sending documents to the authorities to apply administrative penalties; as well as submitting documents to law enforcement authorities to consider initiating criminal proceedings.

93. Other uses of the SRA results could be to update the national risk assessment or to conduct joint typologies research with the competent financial intelligence units.

III. Sample questionnaires for collecting information for ML/TF risk assessment

Sample questionnaire to assess the functioning of the AML/CFT system in banks

1. Do the bank's legal acts (policies, rules, procedures, regulations, instructions, decisions, orders, methods, job descriptions and others) fully incorporate the regulatory requirements and relevant recommendations of the National Bank in the field of AML/CFT (specify the name, date of adoption and numbers of the main (up to 5) valid documents)?

2. Who is the official responsible for the implementation of the internal control rules (specify position and legal act conferring authority)?

3. Provide the name of a special AML/CFT unit, its regular and actual staffing.

4. Whether the Head of the special unit is subordinated to the Head (Deputy Head) of the bank or to an official responsible for internal control in the bank and is accountable to the Board of Directors (Supervisory Board) (specify the legal act of the bank and the subordination)?

5. Whether timely notification of the supervision about the appointment of the head of a special unit, his/her deputy (persons replacing them) is ensured?

6. Which of the following functions does the special AML/CFT unit perform:

6.1. development of internal control rules;

6.2. development of procedures to manage the risks associated with money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction;

6.3. submitting to the Head of the Bank or his authorized deputy proposals on improvement and increase of effectiveness of the internal control system in the Bank;

6.4. coordination of organization of the internal control system in the Bank;

6.5. participation in the process of introduction of new banking products and services;

6.6. advising the Bank's officers on issues arising during the implementation of the Bank's internal control rules, including customer identification, preparation of reports and completing special forms;

6.7. organizing and participating in AML/CFT/CPF training of the Bank's officers;

6.8. organizing knowledge tests and participating in briefings of responsible officials of the Bank's structural divisions included in the organizational structure of the Bank's internal control system in the AML/CFT/CPF sphere;

6.9. preparing and submitting to the Bank's Board of Directors (Supervisory Board), at least once a year, a report on the results of the implementation of the Bank's internal control rules and on the recommended measures to improve the internal control system;

6.10. conducting a self-assessment of the Bank's involvement in suspicious transactions related to the receipt and/or legalization of proceeds of crime, financing of terrorist activities, proliferation or financing of proliferation of weapons of mass destruction;

6.11. other functions (please specify)

7. In your opinion, are there any barriers that prevent a special AML/CFT unit from fully performing the required functions (if so, please list them)

8. Describe the frequency and procedure for informing the bank's management bodies, including the Board of Directors (Supervisory Board), about the results of the implementation of AML/CFT procedures (provide indicators of the adequacy of the system for identifying criteria and indicators of suspicious financial transactions:

8.1. ratio of the number of special forms submitted to the number of reports prepared (%);

8.2. ratio of the number of special forms not submitted to the number of special forms submitted (%).

9. How many bank officers receive training (internship) on AML/CFT issues (specify the number of officers who received training and their share (%) in the total number of officers involved in operational activities)? Describe the methods of the training (internship).

10. Describe the customer identification process and its specifics (specify: the name of the electronic customer database; whether the risk score method is used; the source of the data used to identify PEPs; the data used to verify the identification data (database); whether the activities of the customer who systematically conducts suspicious financial transactions are investigated).

11. Describe the procedure for identifying persons involved in terrorist activities.

12. Whether identification agents are used to identify customers (if so, specify the customer groups and products, the number and names of identification agents)?

13. Describe how the interbank identification system is used (specify the number of customers whose identification data are obtained from the interbank identification system (broken down by customer group - natural persons, individual entrepreneurs, legal persons)).

14. Specify the number of automated/partially automated criteria for detecting and identifying suspicious financial transactions.

15. Can you confirm that you have no relationship with shell banks (a bank that has no physical presence and is not affiliated with a regulated bank that has a physical presence)?

16. Are the retention periods for records related to customer identification and account transactions observed? Specify the norms of the bank's legal act establishing them.

17. Specify the number of internal AML/CFT audits conducted, and briefly describe their findings and measures taken.

18. Do you have a policy to protect bank officers by implementing enhanced internal controls for customers who systematically engage in suspicious financial transactions? If you have such a policy, please specify its main provisions.

19. Are there any cases of dismissal of officials for violations of AML/CFT legislation? If so, please specify the number of officials dismissed.

20. What vulnerabilities do you see in the identification of the parties to a financial transaction? Do ML/TF risks increase due to the abolition of the sale of foreign currency with a passport; the possible introduction of a threshold to identify the e-wallet owner?

Sample questionnaire to assess the functioning of AML/CFT system
in non-banking financial institutions

1. Do the institution's legal acts (policies, rules, procedures, regulations, instructions, decisions, orders, methods, job descriptions and others) fully incorporate the legal requirements and relevant recommendations of the National Bank in the field of AML/CFT (specify the name, date of adoption and numbers of the main (up to 5) valid documents)?

2. Who is the official responsible for the implementation of the internal control rules (specify position and legal act conferring authority)?

3. Provide the name of a special AML/CFT unit, its regular and actual staffing and/or the number of responsible officials.

4. How many employees of the institution receive training (internship) on AML/CFT issues (specify the number of employees who received training and their share (%) in the total number of employees involved in operations). Describe the methods of training (internship).

5. Describe the customer identification process and its specifics (the source of the data used to identify PEPs; the data used to verify the identification data; the use of the list of persons involved in terrorist activity; whether the activities of the customer who systematically conducts suspicious financial transactions are investigated).

6. Describe the process for identifying and entering into agreements with politically exposed persons.

7. Describe the process for identifying persons involved in terrorist activities.

8. Are identification agents used for customer identification (if so, specify the customer groups, the number and names of identification agents)?

9. Specify the number of internal AML/CFT inspections, and briefly describe the results and actions taken.

10. Does the institution have facts of dismissal of officials based on the results of revealed violations in the field of AML/CFT (if any, specify the number of such persons)?

11. Specify the share (in %) of high-risk customers by group (natural persons, individual entrepreneurs, legal persons).

12. Are the retention periods for documents related to customer identification and customer transactions observed? Specify the norms of the local legal act of the institution that establish them.

13. Do you have a policy or measures in place to protect employees who exercise enhanced internal controls with respect to customers who systematically engage in suspicious financial transactions (brief description, if any)?

Sample questionnaire for the collection of information for the assessment of ML/TF risks, perceptions and practices among notaries

I. General questions

1. Are you familiar with the requirements of international standards that require risk assessment? Which of the FATF Recommendations specify these requirements (provide numbers)?

2. Has a risk assessment been conducted (or is one being conducted):
- in the country?
- in the sector?

3. What legal acts (specify the norms) establish the liability of persons guilty of violating AML/CFT/CPF legislation?

4. Who, in your opinion, should be the coordinator/organizer of the risk assessment of notaries (FIU, supervisory authorities, other (please specify))?

II. International risks

5. Who approves the list of countries (territories) that do not comply with the FATF Recommendations and do not participate in international AML/CFT/CPF cooperation (hereinafter - the FATF's list of non-compliant countries)?

6. What government authority website has a list of countries that do not comply with the FATF Recommendations?

7. Is there an obligation to take action against customers from countries on the FATF's list of non-compliant countries:
- Yes
- No
- Cannot say

What acts establish this obligation:

- Legislative acts
- Acts of the FIU, supervisory or regulatory authorities
- Internal control rules
- Other (please specify).

Have you ever had to take action against customers who are on the FATF's list of non-compliant countries?

8. What is the approach to defining offshore jurisdictions (offshore zones) (e.g., countries and territories with preferential tax treatment and/or no disclosure or reporting, other (please specify))? Are there any lists of offshore jurisdictions in the country? Are you familiar with the contents of such lists? Who publishes them? Do you have access to such lists?

9. What measures can be applied to customers from offshore jurisdictions?

10. Who compiles the list of persons classified as domestic and foreign PEPs, officials of public international organizations? Where is the list published?

11. Specify the most common ML and TF indicators:

12. Has AML/CFT/CPF training been provided to notaries? If so, when? Have you participated in such events? If so, when?

14. In your opinion, what measures could mitigate the risks?

III. Implementation of internal control rules by notaries and application of RBA in notaries' activities. Degree of ML risk perception.

15. Does the country have general requirements for internal control rules?

Does the country have requirements for internal control rules that take into account the specificities of notaries' activities?

16. Who sets the internal control rules?

17. What is the date of your approval of the internal control rules (taking into account changes in legislation)?

18. Who is responsible for implementing the internal control rules?

19. When does a notary carry out internal controls?

20. How often do you analyze the implementation of internal controls?

21. When do you identify a party to a financial transaction?

22. Do you use a risk-based approach to internal controls?

23. What risk factors that increase risk are provided for in the internal control rules?

What risk factors that mitigate risk are provided for in the internal control rules?

24. What internal controls are included in the internal control rules?

25. According to the internal control rules, what are the extended internal controls?

26. How many suspicious transaction reports have been prepared and submitted to the FIU (by year, in the last 5 years)?

27. What scale of risk is established by the internal control rules?

28. What measures are taken when dealing with high-risk customers?

29. Is the notary obliged to identify the beneficial owners?

What acts require the identification of beneficial owners:
- Legislative acts
- Acts of the FIU, supervisory or regulatory authorities
- Internal control rules
- Other (please specify).

30. What sources of information are used to verify beneficial ownership information:
- Government databases
- Commercial databases
- Own databases (using information from mass media, Internet)
- Other (please specify).

31. What risk factors affecting the level of risk are set forth in the internal control rules (both high and low)?

32. Under what conditions is a financial transaction subject to special monitoring?

33. Are the criteria and indicators of suspicious financial transactions subject to special monitoring defined, taking into account the activities of notaries?

What acts establish such criteria and indicators:
- Legislative acts
- Acts of the FIU, supervisory or regulatory authorities, internal control rules
- Other (please specify)?

What criteria and indicators do you use in practice to identify suspicious financial transactions that require special monitoring?

34. How is data recorded to identify parties to financial transactions?

35. What are the timelines for updating information on customers and their representatives, as required by the internal control rules?

36. What is the procedure for documenting financial transactions subject to special control?
What acts regulate such a procedure:
- Legislative acts
- Acts of the FIU, supervisory or regulatory authorities
- Internal control rules
- Other documents (please specify)

37. Presence of non-resident customers (specify the number broken down by year):
- Legal persons
- Individual entrepreneurs
- Natural persons.

38. Specify the number of customers from regions of concern (countries with high levels of corruption, terrorism, and other threats, broken down by year)?

39. What is the liability for violation of AML/CFT/CPF legislation (specify the norms)?

40. What are the retention periods for the information and documents (copies thereof) received as a result of the identification of customers, their representatives, as well as those received and prepared during the application of the enhanced internal controls?

Risks of crimes preceding money laundering

41. In your opinion, which criminal risks are most likely to arise from the use of notarial services.

Rank them in order of risk reduction.

Sector-specific money laundering risks

42. In which sectors of the economy do you think the ML risks associated with the use of notarial services are most likely to occur? Rank them in order of risk reduction.

IV. Terrorist financing risks

43. What website provides a list of entities and individuals involved in terrorist activities?

44. Who provides access to the list of entities and individuals involved in terrorist activities:

45. Does the country have an obligation to freeze the funds of persons on the list of entities and individuals involved in terrorist activities or to block a financial transaction if a designated person is a party to or beneficiary of such a financial transaction?

Have there been any instances of such action in your practice?

46. In what cases are you obliged to suspend a financial transaction? Have there been any cases in your practice where such a measure has been applied?

47. What, in your opinion, are the most characteristic indicators of the transactions possibly related to TF in performing notarial acts:

48. Do internal control rules require increased attention to customers and transactions related to the non-profit sector (charitable institutions, foundations, and others)?

49. Is the concept of extremism defined in the country's national legislation?

Do internal control procedures cover the identification of persons and transactions with indicators of links to extremist financing?

V. Coordination and cooperation

50. In your opinion, is the availability of information on ML/TF sufficient? What are the main sources of information on ML/TF activities?

51. What is your source of information on best practices, including international, in terms of typologies, practices?

52. What forms of interaction with government authorities do you use and find most effective?

53. In what areas do you believe the AML/CFT/CPF system needs further improvement to increase its effectiveness?

Sample questionnaire for precious metals and stones sector

Overview of sector and entity development: This section aims to understand overall development of the sector and the development status of the entity.

1. Your entity’s main product and business type:
   - precious metals such as gold.
   - precious stones
   - gems
   - Others (please note the name of the main product)

2. Your entity’s annual main business revenue:
   - 5 million dollars (included) and below
   - 5 million to 50million dollars (included)
   - 50 million to 100 million dollars (included)
   - 100 million dollars to 1 billion dollars (included)
   - above 1 billion dollars

3. Whether your entity’s main business is regulated by competent authority, whether a special establishment or operation license is required for your entity to carry out business?

4. Does your entity establish foreign subsidiaries or branches?

5. Whether there are relevant AML/CFT laws and regulations for your sector?

6. Whether AML/CFT self-regulatory mechanism is established in your sector?

7. Does your entity have an internal control mechanism for AML and CFT?

8. Does your entity organize propaganda and training on AML and CFT?

Customer's ML/TF risk profile: This section aims to identify customer's ML/TF risk profile of the entity. Customers are classified as suppliers and buyers.

9.The number of your entity's annual supplier customers:

- 10 (included) and below
- 10-20 (included)
- 20-50 (included)
- above 50

10. The proportion of foreign supplier customers purchase amount to your entity's total purchase amount:

- 10% (included) and below
- 10%-25% (included)
- 25%-50% (included)
- 50%-75% (included)
- above 75%
- not involved

11. The proportion of purchase amount involving high risk countries/jurisdictions to your entity's total purchase amount?

- 1% (included) and below
- 1%-5% (included)
- 5%-10% (included)
- above 10%
- not involved

12. The proportion of supplier's total cash transaction amount to your entity's total purchase amount:

- 10% (included) and below
- 10%-25% (included)
- 25%-50% (included)
- 50%-75% (included)
- above 75%
- not involved

13. Does your entity introduce membership for retail customers, and the number of member customers:

- 100 thousand(included) and below
- 100 thousand to 500 thousand (included)
- 500 thousand to 1 million (included)
- 1million to 5million (included)
- above 5 million
- does not introduce membership

14. The proportion of foreign buyer customers' transaction amount to your entity's total sales transaction amount:

- 20% (included) and below
- 20%-40% (included)

- 40%-60% (included)
- 60%-80% (included)
- above 80%
- not involved

15. The proportion of buyer customers' transaction amount involving high risk countries/jurisdictions to your entity's total sales transaction amount:

- 1% (included) and below
- 1%-5% (included)
- 5%-10% (included)
- above 10%
- not involved

16. The proportion of buyer customers' cash transaction amount to your entity's total sales transaction amount:

- 10% (included) and below
- 10%-25% (included)
- 25%-50% (included)
- 50%-75% (included)
- above 75%
- not involved

17. Does your entity have customers/customers' beneficial owners who are politically exposed persons?

18. Does your entity undertake customer due diligence measures when carrying out cash transactions above USD/EUR15,000 and preserve relevant customer identification and transaction information?

19. Does your entity establish a business system or anti-money laundering system, which is capable of registering and inquiring customer's identification and transaction information, and monitoring customers' suspicious transaction?

Product/business/channel ML/TF risk profile: This section aims to identify the ML/TF risk profile of supervised entities' product, business and service channels

20. Does your entity carry out repurchase business of precious metals and stones?

21. Your entity's annual repurchase transaction amount of precious metals and stones?

- 500 thousand dollars(included) and below
- 500 thousand dollars to 1 million dollars (included)
- 1 million dollars to 5 million dollars (included)
- above 5 million dollars

22. When carrying out repurchase business, does your entity identify the reasonableness of the precious metals / stones source and take appropriate risk identification and control measures?

23. Does your entity carry out the business in a non face-to-face manner such as online?

24. Your entity's total sales transaction amount through non face-to-face manner:

- 500 thousand dollars (included) and below
- 500 thousand dollars to 1 million dollars (included)
- 1 million dollars to 5 million dollars (included)
- above 5 million dollars

25. Does your entity have appropriate risk identification and control measures in place when dealing with non-face-to-face business?

Annex

FATF Guidances on applying the risk-based approach to supervision

Risk-based Approach Guidance for the Real Estate Sector	Risk-based Approach Guidance for the Real Estate Sector
Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers	Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers
Guidance on Risk-Based Supervision	Guidance on Risk-Based Supervision
FATF Guidance for a Risk-Based Approach for the Accounting Profession	FATF Guidance for a Risk-Based Approach for the Accounting Profession
Guidance for a Risk-Based Approach Guidance for Legal Professionals	Guidance for a Risk-Based Approach Guidance for Legal Professionals
FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers	FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers
Risk-based Approach Guidance for the Securities Sector	Risk-based Approach Guidance for the Securities Sector
Guidance for a Risk-Based Approach: Life Insurance Sector	Guidance for a Risk-Based Approach: Life Insurance Sector
Guidance for a Risk-Based Approach for Money or Value Transfer Services	Guidance for a Risk-Based Approach for Money or Value Transfer Services
Risk-Based Approach for the Banking Sector	Risk-Based Approach for the Banking Sector
Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services	Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services
FATF Guidance on the Risk-Based Approach for Casinos	FATF Guidance on the Risk-Based Approach for Casinos
FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones	FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones