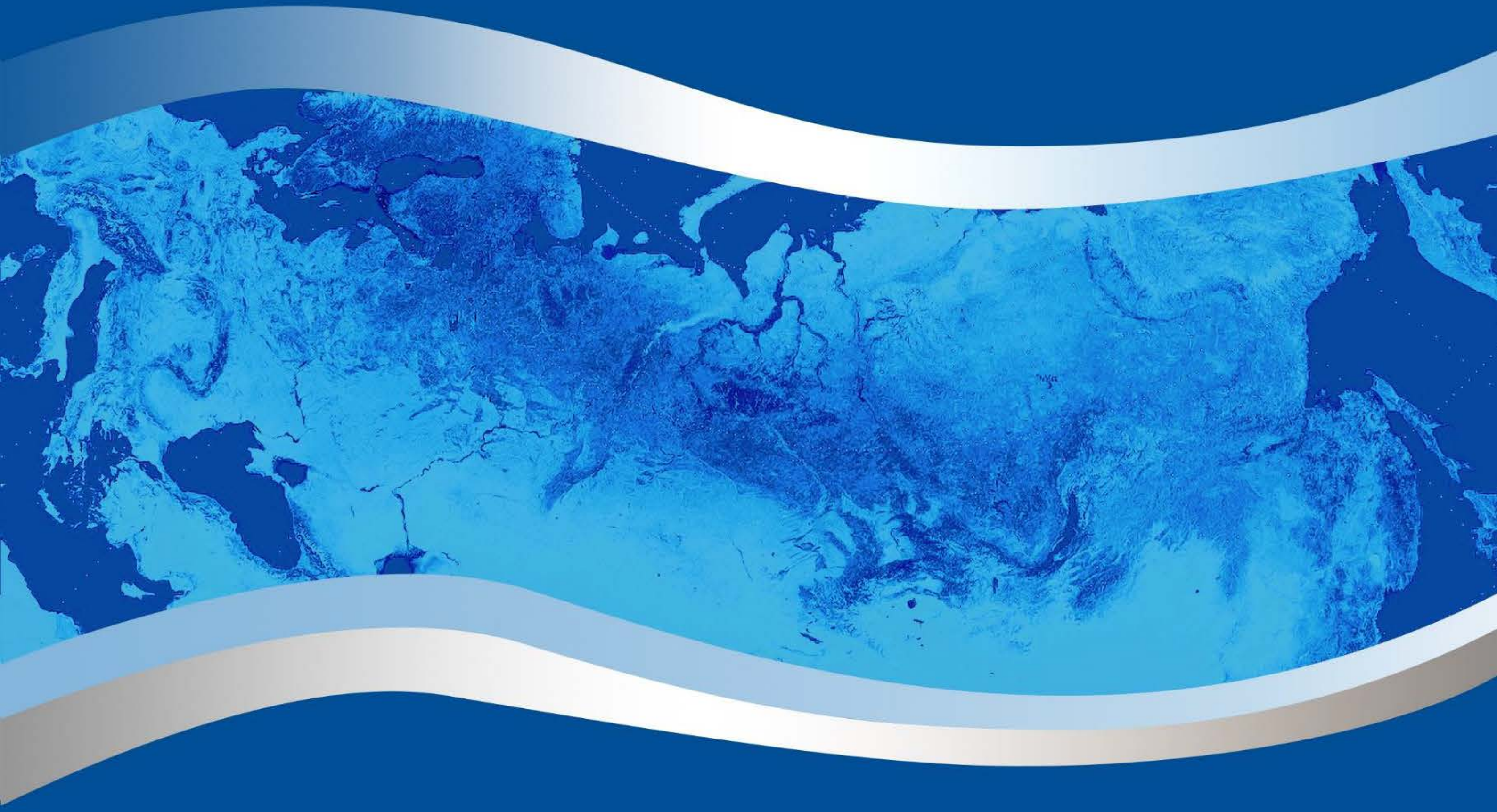
ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов и
финансированию терроризма

EURASIAN GROUP
on combating money laundering and financing of
terrorism



METHODOLOGY

OF THE EURASIAN REGION ML/TF RISK ASSESSMENT

EURASIAN REGION ML/TF RISK ASSESSMENT METHODOLOGY

According to FATF Recommendation 1, states should identify, assess, and understand the money laundering (ML) and terrorist financing risks (TF), and should take measures to prevent and mitigate ML/TF that are commensurate with the risks identified.

ML/TF risk assessments are key to effective AML/CFT efforts, since it is not possible to build a robust AML/CFT framework and take timely measures to manage and mitigate the identified risks without a deep and comprehensive understanding of the ML/TF risks by both government and reporting entities.

The results of regional (supranational) risk assessments may inform national risk assessments (NRA). In line with the FATF framework documents, national assessments should be informed by the assessment of the same risks in neighbouring states, including in order to identify cross-border risks. However, due to confidentiality, NRA reports may not be available to other member states. In such a situation, the results of a regional risk assessment may be used for national risk assessments in the member states.

As a result, the assessment of regional ML/TF risks and development of guidelines for their mitigation has been made one of the focus areas identified in the EAG Strategy 2019-2023[1], adopted by the EAG 30th Plenary (par. 2 of Section II of the Strategy).

This methodology sets out the framework for carrying out the assessment of risks inherent in the subregions specified herein, including EAG states, and for developing joint measures to mitigate such risks and increase the effectiveness of AML/CFT efforts.

Section I. General Provisions

Regional ML/TF risk assessment goals and objectives

The purposes of a regional risk assessment are to identify and assess the key ML/TF risks facing EAG states at the regional level, as well as to develop measures to mitigate them and assess the need for technical assistance and follow-up. A risk is defined as regional if it is of a cross-border nature or inherent (may occur in) in two or more EAG member states included in the assessed region (sub-region).

The objectives of a regional risk assessment are:

- to identify the main schemes used for ML, to raise and move terrorist funds to, within and outside the region (subregion), and to use these funds in the region (subregion);
- to assess the frequency of occurrence of the identified main schemes and the amount of assessed damage/criminal proceeds or funds allocated for TF;
- to understand the nature of threats and key vulnerabilities that negatively impact the level of ML/TF risks;
- to prioritize regional capacity-building measures in order to more effectively combat ML/TF.

Key terms

For the purposes of a regional risk assessment, the following terms and definitions are used in this methodology:

a. EAEU (Eurasian economic union) domestic market means an economic space without internal borders that provides for the free movement of goods, people, services and capital between

[1] https://eurasiangroup.org/files/uploads/files/other_docs/PLEN_(2019)_7_eng.pdf

Armenia, Belarus, Kazakhstan, Kyrgyzstan and Russia, pursuant to Article 28 of the Treaty on the Eurasian Economic Union, signed in Astana on May 29, 2014;

b. opportunity (in the context of the assessment of the effect of threats/vulnerabilities on the resulting risk) means the simplicity and accessibility of ML/TF schemes achieved through the absence or small number of obstacles and/or financial expenses;

c. EAG member states means Belarus, India, Kazakhstan, China, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan;

d. intent (in the context of the assessment of the effect of threats/vulnerabilities on the resulting risk) means the purpose or aim to exploit a scheme for ML/TF;

e. observable ML/TF schemes means ML/TF schemes whose existence is obvious due to the existence of recorded cases of their use, criminal prosecutions and/or convictions, e.g., use of shell companies for ML;

f. unobservable ML/TF schemes means ML/TF schemes whose existence is likely due to the availability of data from the relevant sources required to conduct risk assessments;

g. residual risk means the resulting level of risk for unobservable schemes which is acceptable in relation to the inherent risk after the adoption of risk mitigation measures. In the case of observable schemes, the risk is initially considered residual.

h. money laundering means the following acts committed intentionally:

   - The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such an activity to evade the legal consequences of that person's action;
   - The concealment or disguise of the true nature, source, location, disposition and movement of, as well as the rights to the property or its ownership if such property is known to constitute proceeds of crime;
   - The acquisition, possession or use of property in order to conceal or disguise its illegitimate source or assist any person involved in the commission of these acts, if at the time of its acquisition such property was known to constitute the proceeds of crime;
   - Complicity (masterminding, aiding, abetting, assisting or counselling, etc.) in the commission, preparation (including conspiracy) or attempt to commit any of the acts listed above.

   ML shall be considered as such even if the acts resulting in the laundered proceeds were committed in the territory of another EAG member country or in the territory of a third country.

i. ML/TF risk assessment means a process conducted on the basis of a methodology agreed upon by participants in the assessment, which involves the identification, analysis and understanding of the ML/TF risks, and development of risk mitigation measures.

j. project team means a group comprising representatives of EAG member states and EAG Secretariat staff, which has been created to carry out a regional risk assessment;

k. Eurasian region means the territory within which the EAG member states are located;

l. subregion means the territory within which several EAG member states or part thereof are located, or an interstate body whose members include EAG member states that share common cultural, economic, political ties or borders;

m. risk of observable ML/TF schemes means the likelihood of implementation of observable ML/TF schemes;

n. risk of unobservable ML/TF schemes means the possibility of realization of a ML/TF threat due to vulnerability;

o. regional risk means the ML/TF risk characterized by common features which is typical for or may arise in two or more EAG member states as well as the risks of a cross-border nature;

p. sector means a set of representatives of professions or categories of entities (financial or non-financial) that can be misused for ML/TF. This term includes, at a minimum, financial institutions and designated non-financial businesses and professions (DNFBPs) as they are defined in the FATF Recommendations2.

q. terrorist financing means the provision or collection of funds, or the provision of financial services, with the intent to use them, or in the knowledge that they are to be used, in full or in part, to commit any terrorist offences, as well as in the knowledge that they are intended to be used to finance an organization, or to finance or otherwise provide for a person to commit at least one of these offences, or to provide for an organized group created to commit at least one of these offences;

r. threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their associates, their funds, as well as past, present and future ML/TF activities.

s. vulnerability means the factors that represent weaknesses in the AML/CFT regime or controls or certain features of a region (country). They may also include the characteristics and features of a particular sector, financial product or type of service that make them attractive for ML or TF purposes.

Scope of application of regional risk assessment results

Regional risk assessment results can be used by:

- International and regional organizations, in particular, in AML/CFT technical assistance programmes:
- EAG member states' government agencies to develop national AML/CFT policies, make informed decisions regarding the regulatory framework and allocate resources for the competent authorities;
- Law enforcement and investigative authorities, financial intelligence units, relevant border authorities for use in operational activities;
- Supervisors and self-regulatory organizations for use in regulatory activities;
- Financial institutions and DNFBPs for which a supra-national ML/TF risk assessment is the most important source of information for conducting their own risk assessments and fulfilling obligations informed by risk assessment findings;
- Non-profit organizations to mitigate the risks of their misuse for ML/TF purposes;
- AML/CFT assessors for use in the preparation of mutual evaluation reports;
- The public, science community, etc.

Grouping of risks in the regional risk assessment is not fundamental and essential for national risk assessment and mutual evaluations, but it may inform future cross-border cooperation in adopting regional risk mitigation measures, amending national legislation to mitigate regional risks, etc.

Section II. Splitting into Subregions for Risk Assessment Purposes

The ML/TF risks cannot be identical throughout Eurasian region. Therefore, a comprehensive risk-based approach should be used, which involves the splitting of Eurasian region into the following 4 subregions.

[2] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Subregion “Belarus and Russia (East European subregion)”

The East European subregion includes the following EAG member states: Belarus and Russia.

States from this sub-region have close economic ties with neighbouring MONEYVAL member states: Poland, Lithuania, Latvia and Estonia, Ukraine and Moldova.

Although TF risks are less common for these states, economic relations and the free movement of goods, work and services between individual states pose common ML risks.

“Eurasian Economic Union (EAEU)” subregion

The EAEU subregion includes the following EAG member states: Belarus, Kazakhstan, Kyrgyzstan, Russia as well as Armenia, which is a member of the CIS Council HoFIU.

EAEU states have a common customs regime characterized by the free movement of goods, work, services and capital.

“Central Asia and Russia” subregion

This subregion includes the following EAG member states: Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan.

States from this subregion may share ML/TF risks faced by neighbouring Asia-Pacific Group (APG) member states: Afghanistan, Mongolia as well as Iran, which is not an APG member.

“India and China” subregion

This subregion includes the following EAG member states: India and China.

States from this sub-region may share ML/TF risks faced by neighbouring Asia-Pacific Group (APG) member states: Bangladesh, Nepal, Pakistan and Sri Lanka.

Section III. Analysed Regional Risk Assessment Period

For each round of regional risk assessments, the analysed period is the three-year period preceding each round of assessments.

Section IV. Data Sources Used in Regional Risk Assessments

The following open source information is used in the regional risk assessments:

- Reports and information of international organizations;
- Information of international conferences and coordinating bodies;
- Information contained in national risk assessment reports;
- Information contained in mutual evaluation reports;
- Available data on TF threat assessment;
- Data on ML/TF offences.

In addition, the findings of surveys of the following public authorities and the private sector as well as EAG observers are used:

a. Law enforcement and prosecution authorities (including, as appropriate, the police, customs/border authorities and criminal investigation agencies):

   - information on specific investigations in specific assessed areas;
   - assistance in assessing the amount of criminal proceeds on the basis of information on predicate offences available to them;
   - relevant statistics on ML/TF investigations, prosecutions and convictions, as well as statistics on seized, confiscated, recovered and shared assets, and (international) requests for legal assistance;

- information on criminal schemes obtained in the course of investigations;
- information on new trends and risks identified during the investigation;
- information on vulnerabilities associated with deficiencies of legislative, interagency, organizational and other nature.

b. Intelligence agencies and/or other security services:

- information relating to terrorism and its financing, in particular information on threats;
- information on vulnerabilities associated with deficiencies of legislative, interagency, organizational and other nature.

c. Financial intelligence units:

- information regarding ML/TF threats, vulnerabilities, trends and schemes, including emerging, based on suspicious transaction reports, other information and ongoing strategic analysis;
- case studies/examples that do not contain classified information, summarized data to identify trends in the use of specific types of financial instruments and or transactions;
- reporting entities' reporting statistics.

d. Regulatory and supervisory bodies (including, for example, self-regulatory bodies and FIUs with such powers):

- information on vulnerabilities associated with the types of products, transactions (including cross-border) and clients possibly linked to ML/TF identified on the basis of field and desk audits and remote monitoring. Thus, they have the opportunity to express their views on the adequacy of measures taken by supervisors to mitigate the specific risk;

e. Representatives of the private sector (financial institutions and DNFBPs):

- information about the size and structure of sectors, their customers, as well as the features and characteristics of certain products and services, which may be useful for determining the level of risk they represent and help in identifying vulnerabilities.

f. International and foreign partners, and FATF-style regional bodies (FSRBs):

- information on risks, in particular the plan for carrying out work in other parts of the region, aimed at identifying and understanding risks.

This list is not exhaustive.

Data sources used in the assessment should be reliable and objective. Information is collected from various sources to ensure the reliability of the assessment results. Data obtained from questionable sources should be critically evaluated, taking into account the context of accompanying data and other information identified as reliable.

Section V. Information gathering field visits

Information gathering field visits are carried out to facilitate the collection of comprehensive data required for an objective and reliable assessment. The information gathering field visits include interviews with AML/CFT system stakeholders. The information gathering field visits will conduct on a purely voluntary basis.

The sequencing of information gathering filed visits depends on the inclusion of EAG member states in one or more subregions. The information gathering field visits to states included in only one subregion should be carried out first. This will allow project team departing for states included in several subregions to have certain information on them.

The information gathering field visits should ideally be divided into three groups:

- Group 1: Tajikistan, Turkmenistan and Uzbekistan.

- Group 2: India, Kazakhstan and Kyrgyzstan.
- Group 3: Belarus, China and Russia.

The information gathering field visits are carried out by the project team members (experts) consisted of 3 (three) representatives.

Section VI. Regional Risk Assessment Methodology

A regional risk assessment is expected to reveal ML/TF schemes that may pose ML/TF risks at the level of the Eurasian sub-region as a whole and individual sub-regions in particular.

Regional risks are conventionally divided into two categories: observable and unobservable.

As per the FATF standards, the purpose of a risk assessment is to identify, assess and understand these risks.

To determine the level of risk of observable ML/TF schemes, project team compare the frequency of their occurrence and the amount of assessed damage/criminal proceeds or funds allocated for TF.

The determination of the resulting regional risk of the observable ML/TF schemes (mechanisms) is set out in paragraphs 45-48 of this Methodology.

It is also possible to use expert opinion at this stage of risk assessment.

It is worth noting that the level of regional risks may not match the level of risks identified at the national level for objective reasons: each country takes different measures to mitigate the risks identified. That is, a high regional risk does not automatically translate into a high level of national risk. Where the regional risk is high for one country, for another it may be low or medium.

For the understanding of the ML/TF risks, project team will consider the measures taken by each country of the subregion to mitigate the identified risks. To this end, assessors determine the nature of threats as well as the sufficiency and effectiveness of the protective measures taken in the states of the assessed subregion to mitigate the consequences of the existing schemes and achieve the expected level of risk.

To determine the level of risk of unobservable ML/TF schemes, project team assess the level of threats and vulnerabilities. In this case, they assess the intentions and capabilities of criminals to use emerging ML/TF schemes, the availability of protective measures and their effectiveness.

The determination of the resulting regional risk of the unobservable ML/TF schemes (mechanisms) is set out in paragraphs 60-62 of this Methodology.

Section VII. Regional Risk Assessment Procedure

Regional risk assessment rounds

The ML/TF risk assessment in the Eurasian region is carried out in two rounds:

- The first round includes the assessment of observable ML/TF schemes.
- The second round includes the assessment of unobservable ML/TF schemes.

The initial phases of the first and second rounds of the regional risk assessment and their features

The use of two rounds of a regional risk assessment is necessitated by the presence of significant differences in the initial phases of their implementation.

Initial phases of the first round regional risk assessment (assessment of observable schemes)	*Initial phases of the second round regional risk assessment (assessment of unobservable schemes)*

- identification of regional risks (schemes); - assessment of regional risks (assessment of the frequency of scheme occurrence and the amount of criminal proceeds or funds allocated for TF); - understanding the regional risks (determining the nature of threats and vulnerabilities).	- identification of regional risks (schemes); - assessment of the ML/TF threats; - assessment of vulnerabilities in sectors; - assessment of the resulting level of the regional risk.

The first round of the regional risk assessment includes the assessment of observable ML/TF schemes

Identification of regional risk

The first phase involves the identification of all ML/TF risks inherent in the subregion for their subsequent assessment during the next phase of the risk assessment process.

Risk identification consists in compiling a list of known ML/TF schemes. To this end, project team use EAG typological and mutual evaluation reports, states' opinions and reports of other FSRBs to prepare a form containing all known schemes as well as a questionnaire for submission to the EAG members and observers. In the said form, ML/TF schemes are listed according to the predicate offences established in the FATF standards.

The risk identification phase should not include the assessment of their level, since this will be the goal of the next phase.

Assessment of the level of regional risks

After identifying known risks (schemes described in STRs, FIU analytics, criminal investigations and court decisions), assessors should determine the extent and frequency of each risk relative to other risks.

The risks identified during the first phase are classified based on the frequency of their occurrence and the amount of criminal proceeds or funds allocated for TF.

Levels of the regional risk are determined by initially calculating the average of the frequency of the scheme and the amount of proceeds of crime (damages incurred) for each risk within a sub-region. However, when the same scheme is used within the same country for ML for several types of predicate crimes, the average value of each of the indicators for the country is first calculated.

The risk indicators are then mapped onto a coordinate system, where "x" is the frequency of occurrence of the scheme and "y" is the amount of criminal proceeds (damage caused) received or funds used for terrorist financing. The resulting level of the regional risk in absolute number is defined as the distance from the beginning of coordinates to the point formed by the intersection of values of indicators, according to the formula R= $\sqrt{x^2 + y^2}$**, and affects the distribution of risks into the following groups:** regional risks requiring significant attention and enhanced risk mitigation measures (from 2 to 3 points inclusive); regional risks requiring on-going monitoring and enhanced risk mitigation measures (from 1 to 2 points inclusive); regional risks requiring standard risk mitigation measures (from 0 to 1 points inclusive), no risk (0 point).

Understanding the identified regional risks (determining the nature of threats and vulnerabilities)

When analysing the ML/TF risks, it is extremely important to have a common understanding of why ML and TF cases exist. Therefore, the main goal of this phase is to analyse the identified risks in order to understand sectors' vulnerabilities that affect the frequency of such schemes.

This phase consists of the following elements:

- Assessment of threats (predicate offences and criminals);
- Identification of vulnerable products/services featured in each scheme;
- Analysis of the legislative framework and the effectiveness of its implementation (are legislative measures being implemented by the private sector, supervisor and law enforcement);
- Organizational factors affecting the nature and level of vulnerability, including the existence and effective use of powers by the competent authorities (does the FIU have sufficient resources and authority to identify and analyse ML/TF schemes; do LEAs have sufficient resources and authority to investigate and prosecute ML/TF; do supervisors have the power to audit reporting entities and impose sanctions, etc.);
- The existence of international and interagency information exchange, including concluded international agreements and memoranda that enable competent authorities to exchange documents and information to identify ML/TF schemes and their analysis.

The second round of the regional risk assessment includes the assessment of unobservable ML/TF schemes

Identification of regional risk

For the purpose of a regional assessment, risk identification consists in compiling a list of likely ML/TF schemes.

Despite the fact that the identification of risks will largely involve the analysis of the known schemes, it is also important to consider new or emerging threats for the counteraction of which, presumably, there are no comprehensive protective measures.

The risk identification phase should not include the assessment of their level (substantial or non-substantial), since this will be the goal of the next phase.

Assessment of the effect of the threat level on the resulting regional risk level

The threat level for unobservable schemes is assessed by determining the intent and opportunities to use this scheme. The intent to use a specific ML/TF scheme depends on its attractiveness and awareness of the correspondent AML/CFT measures. The intent is assessed by identifying previous attempts to use a given scheme.

When evaluating the “opportunity” element, assessors should assess the level of simplicity of using a given ML/TF scheme (required technical knowledge and support), as well as its availability. The criteria for assessing the effect of the threat level on the resulting risk are given in Annex 1.

Assessment of the effect of the vulnerability level on the resulting regional risk level

The third phase consists in assessing the vulnerability level (low, medium or high) for each scenario (ML/TF process in comparison with the sectors in which it may occur).

For each scenario, a vulnerability assessment will mainly consist in identifying the availability of protective measures and their effectiveness. The more effective control and protective measures are, the lower level of vulnerability and, by extension, the risk.

A vulnerability assessment will be carried out in the context of activity areas/sectors (which are subject to AML/CFT requirements) in which ML and TF schemes may be used. Particular attention should also be paid to other criteria, such as the effectiveness of information sharing between FIUs, cooperation with other agencies tasked with combating ML, and the effectiveness of international cooperation, including between supervisors.

The criteria for assessing the effect of the vulnerability level on the resulting risk are given in Annex 2.

Assessment of the resulting regional risk level

Based on the results of the second (threat assessment) and third (vulnerability assessment) phases, the level of each risk identified during the first phase (ML/TF scheme) is determined based on the sum of the estimated threat and vulnerability levels.

The resulting risk level is determined by comparing the threat with vulnerability. It is assumed that the vulnerability level increases the attractiveness and, therefore, the intent of criminals/terrorists to use a specific method, thus affecting the threat level. Consequently, vulnerability has a greater potential for determining the level of risk, hence the greater weight given to the vulnerability level in determining the resulting risk level.

The resulting level of regional risk, which affects the distribution of risks into the following groups, is determined using the arithmetic mean based on the aggregate of identified threats and vulnerabilities: regional risks requiring significant attention and enhanced risk mitigation measures (from 2 to 3 points inclusive); regional risks requiring on-going monitoring and enhanced risk mitigation measures (from 1 to 2 points inclusive); regional risks requiring standard risk mitigation measures (from 0 to 1 points inclusive), no risk (0 point).

Subsequent (identical) phases of the regional risk assessment for observable and unobservable schemes

Report preparation and adoption

A regional risk assessment report should, at a minimum, contain a description of the following:

- The most common ML schemes;
- Sectors of financial institutions and DNFBPs most vulnerable to ML/TF;
- ML/TF risks occurring within, or with the involvement of, the sectors of financial institutions and DNFBPs.

The EAG Secretariat will provide a report to the EAG member states to assist them in identifying, understanding, managing and mitigating the ML/TF risks, as well as to improve other stakeholders' understanding of these risks, and will forward recommendations for the elimination of the identified risks prepared during the assessment.

The reports are given a status of publicity in accordance with the Guidelines on conducting EAG typologies projects (WGTYP (2017) 2 rev.4).

Development of risk management measures (risk mitigation measures)

During this phase, analysis findings are used identify priority risk mitigation areas, taking into account the goals identified at the beginning of the assessment process. Such priority areas can help develop a risk mitigation strategy.

To this end, an Action Plan will be developed to mitigate the identified regional risks.

This phase also includes an assessment of states' need for technical assistance required to implement the developed measures (e.g., financial assistance, development of IT solutions). This information should be taken into account when drawing up technical assistance plans.

Subsequent updating of risk assessment results

The project team uses the results of the regional assessment and other available data to formulate in the report proposals for the subsequent phases of the regional risk assessment in order to update the level of existing or determine the level of emerging threats, typically once in three years.

The follow-up monitoring is conducted to ensure a comprehensive analysis of the ML/TF risks and implementation of the relevant prevention measures. This is necessary to track progress in mitigating the identified risks and to update the risk profile.

A repeat assessment, in the absence of significant circumstances, is carried out by collecting information (questionnaires) and aims to evaluate the implementation of the project team's recommendations for the application of risk mitigation measures, as well as to assess the risks after the implementation of these measures.

Whenever necessary, the methodology can be amended to reflect the experience gained during various rounds and phases of the regional risk assessment.

Annex 1

Threat assessment criteria:

Low	– criminals may have general, non-specific intentions to use this scheme for ML/TF purposes; – this scheme is difficult to access, and / or may entail higher costs than other schemes; – this scheme is not considered attractive and / or safe; – there are some indicators suggesting that criminals have the necessary capabilities to use this scheme; – compared to other scheme, criminals require planning, knowledge and / or technical experience to use this scheme; – organized criminal groups and money launderers/terrorist financiers rarely use this method.
Medium	– criminals use this scheme for ML/TF purposes; – this scheme is accessible and financially feasible; – this scheme is considered quite attractive and / or relatively safe; – criminals have the necessary capabilities to use this scheme; – criminal require moderate planning, knowledge and / or technical experience to use this scheme; – organized criminal groups and money launderers/terrorist financiers periodically use this method.
High	– criminals repeatedly use this scheme for ML/TF purposes; – this scheme is widely accessible, can be used through a variety of means and / or at a relatively low cost; – this scheme is considered attractive and / or safe; – criminals are known to possess the necessary capabilities to use this scheme; – this scheme is relatively easy to use, requiring little planning, knowledge and / or technical experience compared to other schemes; – organized criminal groups and money launderers/terrorist financiers frequently use this scheme.

Annex 2

Vulnerability assessment criteria:

Low	Dissuasive and enforcement measures in place in the reviewed sector/field of activity enable effective prevention of ML/TF. The sector hints at the existence of an organizational structure that has some deficiencies and weaknesses, but its susceptibility to ML/TF risks is low. Assessment criteria examples SUSCEPTIBILITY TO RISKS: - there are no or a small number of products, services or transactions that facilitate the execution of very fast or anonymous transactions; mainly secure and / or controlled supply channels are used; a relatively large number of executed transactions; a relatively low number of cash transactions; good management of new technologies and / or new payment methods; - a small number of customers posing a higher risk; good opportunities for managing customer relations with legal entities or trusts;

	- there are a number of business relationships and clients located in regions rated as high risk; a relatively high volume of cross-border transactions. AWARENESS OF VULNERABILITIES INFORMED BY RISKS: - there is a certain level of awareness of the ML/TF risks inherent in the sector (evidence, measures taken, training, resource allocation). The sector takes advantage of the organizational structure, which, however, has some deficiencies and weaknesses; - the competent authorities provide, in a relatively sufficient volume, the results of ML/TF risk assessments related to the sector under review, and law enforcement agencies are well placed to counter the ML/TF risks (ML/TF cases are monitored, and there exists a probability of their detection, which leads to some investigations, prosecutions and convictions) - the FIU has the capacity to identify and analyse risks in certain areas, which ensures a high rate of STR submissions, particularly through the use of special indicators. LEGAL FRAMEWORK AND ENFORCEMENT MEASURES: - the existing legal framework covers the main elements of the risks inherent in the sector under review; - there are some deficiencies in the implementation of enforcement measures provided by law by sector participants. There are reliable CDD/identification mechanisms, which, however, do not ensure a systematic compliance with the procedures for establishing (identification) and verifying the identity (verification) of clients, their representatives, beneficiaries and beneficial owners. Reporting entities exercise to some extent internal controls (e.g., risk management, record keeping and training). Reporting entities submit a small number of STRs to FIUs; - domestic and international information sharing between the agencies tasked with AML, particularly between FIUs and supervisors, is not sufficient.
Medium	Dissuasive and enforcement measures in place in the sector/area of activity under review prevent the misuse of services by criminals/terrorists only to a limited extent. The sector hints at the existence of an organizational structure that has some deficiencies and weaknesses, and/or at serious ML/TF risk. Assessment criteria examples SUSCEPTIBILITY TO RISKS: - there are a significant number of products, services or transactions that facilitate the execution of very fast or anonymous transactions; a small number of secure and / or controlled supply channels are used; a significant number of executed transactions; a significant number of cash transactions; poor management of new technologies and / or new payment methods; - a significant number of customers posing a higher risk; limited opportunities for managing customer relations with legal entities or trusts; - there are a large number of business relationships and clients located in regions rated as high risk; a significant volume of cross-border transactions. AWARENESS OF VULNERABILITIES INFORMED BY RISKS: - awareness of the ML/TF risks inherent in the sector (evidence, measures taken, training, resource allocation) is limited. The sector takes advantage of the organizational structure; - the provision by the competent authorities of ML/TF risk assessment results related to the sector under review is limited, and law enforcement agencies' capacity to counter the ML/TF risks is limited (a limited number ML/TF cases are monitored, and there is a low probability of their detection, resulting in a limited number of investigations, prosecutions and convictions); - FIUs have the ability to identify and analyse risks only in limited circumstances, resulting in a limited collection of STR-related intelligence. LEGAL FRAMEWORK AND ENFORCEMENT MEASURES:

	- the existing legal framework does not cover the most significant elements of the risks inherent in the sector under review; - there are significant deficiencies in the implementation of enforcement measures provided by law by sector participants. There are a small number of reliable CDD/identification mechanisms, which do not ensure effective compliance with the procedures for establishing (identification) and verifying the identity (verification) of clients, their representatives, beneficiaries and beneficial owners. There are very significant deficiencies in the implementation of internal controls (e.g., risk management, record keeping and training) by reporting entities. Reporting entities submit a very small number of STRs to FIUs; - domestic and international information sharing between the agencies tasked with AML, particularly between FIUs and supervisors, is very limited.
High	Enforcement measures and mechanisms in the sector/area of activity under review are absent, very limited or they do not function as expected. The sector hints at the existence of an organizational structure that has major deficiencies and weaknesses, and/or at high ML/TF risk. Assessment criteria examples SUSCEPTIBILITY TO RISKS: - there are a large number of products, services or transactions that facilitate the execution of very fast or anonymous transactions; no secure and / or controlled supply channels are used; a large number of executed transactions; large number of cash transactions; no management of new technologies and / or new payment methods; - a large number of customers posing a higher risk; no opportunities for managing customer relations with legal entities or trusts; - business relationships and clients located in regions rated as high risk; a large volume of cross-border transactions. AWARENESS OF VULNERABILITIES INFORMED BY RISKS: - the reviewed sector does not demonstrate awareness of the ML/TF risks inherent in the sector (evidence, measures taken, training, resource allocation); the sector lacks an adequate organizational structure to manage and mitigate the ML/TF risks; - the competent authorities do not provide ML/TF risk assessment results related to the sector under review, and law enforcement agencies are not able to counter the ML/TF risks (the identification of such cases is very difficult, with only a small number of identified cases, or there are no financial or other indicators of suspicious activity; the number of investigations, trials and convictions is extremely low); - the FIU is able to identify and analyse risks in very limited circumstances, or completely lacks such ability regardless of the circumstances. LEGAL FRAMEWORK AND ENFORCEMENT MEASURES: - the existing legal framework does not cover the risks inherent in the sector under review; - there are major deficiencies in the implementation of enforcement measures in the sector by sector participants; there are no reliable CDD/identification mechanisms, and the required procedure for establishing (identifying) and verifying the identity (verification) of clients, their representatives, beneficiaries and beneficial owners is not followed; application of internal controls by reporting entities is inadequate (e.g., risk management, record-keeping, training); reporting entities do not report suspicious transactions to financial intelligence units; - domestic and international information sharing between the agencies tasked with AML, particularly between FIUs and supervisors, is absent or does not allow the exchange of information.

www.eurasiangroup.org