Published on (https://www.bnm.md)

Expand Hide

05.05.2011

Recommendations on banks' risk-based approach actions taking in relation to their customers in the context of prevention and combating money laundering and terrorist financing, approved by the DCA of the NBM no.96 of May 5, 2011

Published in the Official Monitor of the Republic of Moldova no.83-85/527 of May 20, 2011

Council of Administration
of the National Bank of Moldova

Decision no.96
of May 5, 2011

On the approval of the Recommendations on banks' risk-based approach actions taking in relation to their customers in the context of prevention and combating money laundering and terrorist financing

In accordance with the art. 2 and 5 item d) of the Law no.548-XIII of July 21, 1995 on the National Bank of Moldova (Official Monitor of the Republic of Moldova, no. 56-57/624 of October 12, 1995), with all subsequent amendments and completions, art. 23 and 40 of the Law on Financial Institutions no. 550-XIII of July 21, 1995 (Official Monitor of the Republic of Moldova, no. 1 / 2 of January 1, 1996), with all subsequent amendments and completions, art. 10 paragraph (2) of Law no. 190-XVI of July 26, 2007 on prevention and combating money laundering and terrorist financing (Official Monitor of the Republic of Moldova, no. 141-145/597 of September 7, 2007), with all subsequent amendments and completions, Council of Administration of the National Bank of Moldova

HAS Decided:

1. To approve Recommendations on banks' risk-based approach actions taking in relation to their customers in the context of prevention and combating money laundering and terrorist financing (see attached).
2. The banks, in the process of development and implementation of their own programs in the domain of prevention and combating money laundering and terrorist financing, will take into considerations the provisions of the Recommendations mentioned at the paragraph 1 of the present decision.

Chairman
of the Council of administration
of the NATIONAL BANK OF MOLDOVA

DORIN DRĂGUŢANU

RECOMMENDATIONS
on bank's risk-based approach actions taking in relation to their customers in the context of prevention and combating money laundering and terrorist financing

I. General provisions

1. The Recommendations on banks' risk-based approach actions taking in relation to their customers in the context of prevention and combating money laundering and terrorist financing (hereinafter the Recommendations) has the purpose to methodologically guide banks in developing internally effective mechanism for identification and assessment of the risks associated with customers, their activity and transactions (operations) for preventing and combating money laundering and terrorist financing.

2. The Recommendations has as an object to:
a) describe the main objectives of the risk based approach to customers;
b) establish the criteria and the risk assessment process of money laundering and terrorist financing concerned with customer's activity, implement the system managing risks related to money laundering and terrorist financing;
c) implement the risk based approach to customers;
d) describe the peculiarities of the internal control procedures related to risk based approach to customers.

3. The Recommendations are developed taking into account the FATF 40+9 Recommendations, FATF Guidance on the risk-based approach to combating money laundering and terrorist financing, Wolfsberg statement guidance on a risk based approach for managing money laundering risks and other relevant international documents.

4. The terms and notions of "bank's customer", "image risk", "country risk", "operational risk", "information security", "information system", "transaction" used in these Recommendations have the significance of those given in the Regulation on Internal Control Systems within Banks, approved by Decision of the Council of Administration of the National Bank of Moldova, minutes no. 96 of April 30, 2010. At the same time, for the purpose of the Recommendations the following terms and notions shall be used:
risk-based approach to customers – the process used by the bank to identify its customers and assess the potential risks of money laundering and terrorist financing that they can generate;
international organizations – United Nations, Council of Europe, FATF, Basel and other organizations recognized by the international community;
complex and unusual transactions - transactions carried out through a single operation or several operations during the month that are not specific to the customer's ordinary activity and/or are not common to its type of the activity;
legal risk – possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can adversely affect the operations or situation of the bank;
concentration risk – is the risk related to the following:
a) on the assets side of the bank's balance sheet – is manifested by the lack of an information system to identify credit concentrations (exposures) and prudential limits established in order to restrict bank's exposures to single borrowers or groups of inter-related borrowers;
b) on the bank's liabilities side – is manifested by the early withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity resulting from inadequate analysis of deposits concentration, characteristics of their depositors, as well as non-maintenance of a close relationship by liabilities managers with large depositors;
information technologies risks – risk of registering cases of money laundering and terrorist financing or risk of favoring appearance of such activities as a result of some vulnerabilities within the bank's informational systems.

II. The objectives of risk based approach to customers

5. The bank undertakes adequate measures to identify, assess and minimize the risks associated with customers in order to prevent its use or implication in another way in money laundering and terrorist financing transactions.

6. Risk based approach to customers contributes to the identification of the risks that need additional measures and control, and to concentrate resources where the highest risks exists. As consequences, a risk based approach to customers in the context to prevention and combating money laundering and terrorist

financing has as the main objective to ensure that the undertaken adequate measures are in order to minimize the risk involved.

7. A reasonable interpretation of the concept of risk-based approach to customer must contain the means by which the bank identifies the criteria for assessing the risk of money laundering and terrorist financing.

8. The process of risk based approach to customers implemented by the bank should offer an efficient mechanism for identification of the potential risks of money laundering and terrorist financing, associated with customers and their transactions (operations), and which could allow the bank to concentrate to the highest risk of money laundering and terrorist financing, that a customer, or its activity or transaction can impose. Thus, the risk based approach is a method of the identification of suspicious activities and/or transactions (operations).

III. Setting criteria and the process of the assessment of the risks of money laundering and terrorist financing

9. The peculiarity of the risk-based approach process to customers, implemented by the bank, depends on the principles of setting the business relation by the bank with its customers and how the operations are conducted. In this context, the internal policies and procedures should determine the way in which the bank manages and minimizes the money laundering and terrorist financing risks, and especially the image risk, operational, legal, concentration and information technologies risks.

10. In order to implement a reasonably risk based approach to customers it is recommended the bank to identify the criteria to assess the potential risk of money laundering and terrorist financing. The identification of the risks of money laundering and terrorist financing, either to customers or categories of customers and their transactions (operations), will allow the bank to establish and implement proportionate measures and controls to minimize these risks.

11. The risk assessment should be performed at the moment of establishing the business relation. At the same time, for some customers, a complete profile of risk may become evident only when conducting transactions (operations) via the bank account. In this regard, monitoring of customer transactions (operations) is a fundamental component of risk-based approach to customers.

12. The bank also needs to adjust the risk assessment of a particular customer based on information received from a competent public authority.

13. The money laundering and terrorist financing risks can be measured using various categories. Establishment of the risks categories has as a purpose the implementation by the bank of the risk management strategies in order to carry out adequate and proportionate supervision and control on customers regarding the potential cases of money laundering and terrorist financing. In this regard, the most commonly used risk criteria are: country (geographic) risk, customer risk and products or services risk.

14. When assessing the risks of money laundering and terrorist financing, depending on the current development conditions in each bank, the bank individually determine the categories of risk weights to be used (individually or in combination). These risk categories should include at least country (geographical) risk, customer risk and products or services risk.

15. Country (geographical) risk refers to countries with a high risk of money laundering and terrorist financing. Countries that impose a high risk are the following:
a) countries, identified by competent authorities, where illegal manufacture of drugs may occur;
b) countries, identified by competent authorities, which represent an increased risk caused by high levels of crime and corruption;
c) countries and / or off-shore areas, identified by competent authorities;
d) countries, identified by competent authorities, which do not have legal norms against money laundering

and terrorist financing, or have inadequate legal norms in this regard;
e) countries, identified by competent authorities, which finance, provide support for terrorist activities and allow terrorist organizations to operate on their territory;
f) countries subject to sanctions, embargoes and other measures by international organizations.

16. The bank in order to assess the customer's risk, relying on its own criteria, shall determine whether a relationship with a particular customer impose a high risk of money laundering and terrorist financing. Categories of customers whose activities and transactions (operations) may indicate high risks are:
a) customers who are late or do not present the necessary documents for identification, or if the documents are doubtful (invalid), the activity of the customers are complex and unusual;
b) customers practicing their activity and/or transactions (operations) in an unusual circumstances:

- the purpose and nature of business relationship is unclear, and the transactions are complex and unusual;
- making frequent funds transfers between economic agents and / or individuals from different regions without a clear economic purpose;

c) customers whose founders structure is complex and does not permit to clearly identify the beneficial owner or customers whose beneficial owners are residents of countries / areas listed in item 15;
d) customers practicing their activity in the countries listed in item 15 or who have their headquarters/ residence in these countries, or customers having business relations with economic agents who have headquarters in these countries;
e) customers whose activity involves working intensively with cash or its equivalent:

- exchange offices, hotels, non-bank providers of payment services through special devices ("cash-in"), wholesale and retail dealers of products and goods, including agricultural products, institutions with the right to provide services related to exchange of postal money orders by post or telegraph or transfer of goods, other economic agents that facilitate the exchange or transfer of money and goods;
- casinos (including internet casinos), institutions organizing and conducting lotteries or gambling;
- economic agents the activity of which normally do not generate much cash, but in certain transactions may generate substantial amounts of funds in cash;

f) charity organizations (philanthropy) or other not for profit organizations the activity of which are not subject to monitoring or supervision, as well as those involved in activities of collection and distribution of funds and goods for philanthropy, religious, cultural, studying, social or other similar purposes, or for carrying out of other "charity activities";
g) customers whose activity suppose acting on behalf of another person and at the same time perform complex and unusual transactions, such as:

- real estate agents, when carry out real estate buying or selling transactions (operations) on behalf of their clients;
- professional participants in the security market;
- lawyers, notaries and other persons which practice independent professional activities and accountants, when prepare or perform transactions (operations) on behalf of their clients related to the following: buying or selling of real estates; funds management; debts or other clients' assets management; management of the banking accounts or other securities; organizing the subscriptions for setting up or administration of economic agents; setting up, administration or managing of legal persons or arrangements (such as, investment funds) and buying or selling of legal persons;
- persons providing investment or fiduciary assistance when are preparing or concluding the transactions for their clients and that act: as a director or secretary, a partner of a commercial society or other similar position in relation with other legal persons, or provide assistance for other person to act in such position; in order to provide an office, business address or other residency, correspondence or other addresses for the commercial society, whichever other person or legal arrangement linked together; as a shareholder with management right for other person (or provide assistance to other person to act in this position);

h) customers – insurance and reinsurance companies engaged in complex and unusual transactions;
i) customers – politically exposed persons;
j) customers – resident of free enterprise zones engaged in complex and unusual transactions;
k) customers which activity is related to sport domain (for instance, sports clubs, sports associations, etc.).

17. When assessing the risks of products or services it is recommended to identify the potential risks generated by bank's offered products and services. The bank pay high attention to risks associated with new or innovative products and services or to services provided specifically for supply of the products. In determining high risk associated with products or services the bank should consider the following:
a) services or products identified by the international organizations, as services or products that pose high risk, such as international correspondent banking services with payments to persons that are not customers (acting as intermediary bank);
b) services that involve trade in precious metals or precious stones, trading and delivery of banknotes and coins, bills, other financial instruments in bearer form;
c) transactions (operations) performed to finance international trading, such as letters of credit, bills of exchange, etc.;
d) assets storage or management services;
e) operations with foreign financial instruments;
f) services that allow to keep anonymity or can readily cross international borders, such as internet banking, national / international electronic transfers, etc;
g) other services or products that may impose high risks of money laundering and terrorist financing.

IV. Sources of information for money laundering and terrorist financing risk assessment

18. In order to perform an adequate assessment of the bank's risks and vulnerabilities of money laundering and terrorist financing it is recommended to use different sources of information, such as national, international, public, private, etc.

19. The bank assesses the risks relying on their own experience on different indicators that characterize the customers and the likelihood of the appearance of those risks associated (customer's characteristics, types of transactions (operations), the countries of interest, etc.). These customer's activity indicators are used to create automat control systems as part of methodology and appropriate reporting procedures.

20. The bank establishes the purpose that shall be achieved during the assessment of the money laundering and terrorist financing risks and used resources, as well as the information available for achieving the goal. At national level can be used statistical data on various indices that show some negative trends (for instance, crime rate), depending on different characteristics (such as geographical area, age, etc.), other information, relevant reports, including those posted on websites of public authorities and other legal persons.

V. Control of customers with high risk

21. When, based on the risk based approach analysis performed by the bank, are identified customers that impose a high risk, the bank applies the necessary measures and control to mitigate the potential money laundering and terrorist financing risks associated with these customers. These measures and controls shall include, but without limitation thereto:
a) enhanced measures when applying "know your customer" rule, according to the normative acts in the respective domain;
b) measures to approve the business relationship or perform transactions (operations);
c) monitoring of activities and transactions (operations);
d) permanent control and frequent review of business relationship.

VI. Implementation of risk-based approach to customers

22. In order to identify, timely assess and mitigate the money laundering and terrorist financing risks it is necessary sufficient to allocate the necessary resources based on the risk profile. Taking into consideration that the risks assessment imposes substantial allocation of bank's resources (staff, time, equipment, information, etc.), the process of allocation of necessary resources is recommended to be fulfilled in order of priority, determined by the bank's activities and transactions (operations) or those of the customer, considered vulnerable to money laundering and terrorist financing.

23. The assessment of money laundering and terrorist financing risks should determine bank to implement at least the following:
a) establish "know your customer" rules;
b) continue monitoring the business relationship with customers and of customer's activities and transactions (operations);
c) reporting of suspicious activities or transactions (operations);
d) on going personnel training.

24. "Know your customer" rules are intended to form an adequate understanding about the real identity of each customer, nature of business relationship and intended transactions (operations) with the bank.

25. "Know your customer" rules shall comprise the following:
a) identification and verification of the identity of each customer in a reasonable time;
b) taking adequate risk-based measures to identify and verify the identity of the beneficial owner;
c) obtaining additional information in order to know the customer's activity, including the purpose and nature of business relationship, as well as its intended transactions (operations).

26. The bank adequately assesses the risks imposed by the customer depending on existing risk factors. To this regard, it is recommended the bank to develop sets of identification measures with varying degrees of complexity, depending on the customer's risk profile:
a) customer's standard identification measures, that applies to all the customers;
b) customer's reduced standard identification measures, where the risk is low (such as, operations in favor of public authorities);
c) customer's enhanced identification measures which activity, ownership structure, type and volume of transactions (operations), etc. determines a high level of money laundering and terrorist financing risk.

27. The degree and nature of continue monitoring of customer's business relationship and transactions (operations) are determined taking into account the bank's size and money laundering and terrorist financing risks that it faces. The monitoring can be carried out both manual and automated, or a combination thereof.

28. In the process of implementation of the risk-based approach to customers, the bank shall take into consideration the fact that not all customer's activities and transactions (operations), accounts or customers should be monitoring in the same way. The specific of monitoring will depend on the specificity of each customer, its product or service, customer's headquarters (residence) and the place of performing its transactions (operations).

29. The monitoring system within risk-based approach should allow the bank to establish certain thresholds below which customer's transactions (operations) or activities will not be monitored. The defined situations or thresholds used for this purpose should be regularly revised to determine how adequate they are established according to the level of risks. The monitoring results should be documented.

30. The bank periodically assesses (at least annually) its system identifying of suspicious activities and transactions (operations).

31. In the process of collecting and submitting (reporting) the information to the competent authority the

bank will ensure an adequate level of security of submitted information and will respect the provisions of the legislation in force.

32. In order to ensure successful identification and control of money laundering and terrorist financing risks the bank carries out a continuous base the training of its personnel.

33. The training of the personnel should ensure their awareness regarding the requirements of the legislation on prevention and combating money laundering and terrorist financing, their skills in identification of money laundering and terrorist financing risks, role and the possible involvement of each employee in the process of prevention and combating money laundering and terrorist financing according to their level of responsibility and duties. The bank individually establishes the periodicity, type and the way trainings should take place.

34. Taking into consideration that money laundering and terrorist financing methods are not static phenomena, the bank will take into account the trend (dynamics) of these phenomena and will periodically perform the review (update) of the risk based approach to customers. Within this scope it is recommended to use the same quantitative and qualitative indicators to compare the changes in time, as well as the way risk assessment was performed in order to determine the methodological deficiencies or the lack of relevant sources of information.

VII. The internal control peculiarities

35. Risk based approach to customer's system must be a part of the bank's internal control system.

36. Bank's management is responsible to ensure that the bank has an effective internal control structure, which ensures the compliance with the relevant legislation in force, including monitoring and reporting suspicious activities and transactions (operations).

37. The internal control procedures should contain at least measures on identification, risks assessment, on establishing and utilization of special instruments in order to mitigate the risks and vulnerabilities identified, implementation of informational systems to monitor the risks (collect, analyze and data updating) according to customer's risk profile, documentation and reporting of suspicious activities and transactions (operations) and those reliable for reporting according to the legislation.

38. The nature and extent of internal controls will depend on several factors, such as: bank's specific, volume and complex activities; diversity of the bank's operations, including geographical diversity; customer's profile, product specific and banking service and the activity within the bank framework; distribution channels used by the customers, volume and size of their transactions (operations); the level of risk associated with each area of the bank activity.

VIII. Risk assessment

39. The risk assessment forms the basis of a bank's risk-based approach. It should enable the bank to understand how, and to what extent, it is vulnerable to money laundering and terrorist financing. It will often result in a stylized categorization of risk, which will help banks determine the level of resources necessary to mitigate the risk of money laundering and terrorist financing. It should always be properly documented, maintained and communicated to relevant personnel within the bank.

40. A bank's risk assessment need not be complex, but should be commensurate with the nature and size of the bank's business. For smaller or less complex banks, (for example where the bank's customers fall into similar categories and/or where the range of products and services the bank offers are very limited), a simple risk assessment might suffice. Conversely, where the bank's products and services are more complex, where there are multiple subsidiaries or branches, offering a wide variety of products, and/or their

customer base is more diverse, a more sophisticated risk assessment process will be required.

41. In identifying and assessing the money laundering and terrorist financing risk to which they are exposed, banks should consider a range of factors which may include:
a) The nature, scale, diversity and complexity of their business;
b) Their target markets;
c) The number of customers already identified as high risk;
d) The countries and off-shore areas in which the bank is exposed to, either through its own activities or the activities of customers, especially, those listed in item 15, notifications from the National Bank of Moldova and the Office for Prevention and Fight Against Money Laundering, FATF lists, European Council Decisions and other international organizations;
e) The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies on third parties to conduct Customer Due Diligence and the use of technology;
f) The internal audit and regulatory findings;
g) The volume and size of its transactions, considering the usual activity of the bank and the profile of its customers;

42. For a qualitative risk assessment, besides taking into account the above factors , banks should complement that information with information obtained from relevant internal and external sources, such as heads of business, relationship managers, national risk assessments, lists issued by international organizations and national governments, mutual evaluation in the field of prevention and combating money laundering and terrorist financing and follow-up reports by FATF or associated assessment bodies as well as typologies.

43. The efficiency of prevention and combating of money laundering and terrorist financing implies the determination of bank's customer risk level, thus, in this context, the risk-based approach represents setting of implemented systems and control measures that meet their particular risk of money laundering and terrorist financing. Therefore, for clients' risk assessment, the bank can use the qualitative method presented in Table no.1, taking into account the characteristic risk factors, such as country, type of activity, products and services, volume and frequency of money cash flows. This method involves granting points from a determined scale, as an answer to a question or subject that reflects the associated risk specific to the customer, and the total sum of the accumulated points determines the risk associated to the customer.

Table no.1: Customer risk assessment

	Questions/Subjects	Point	Remarks
1.	Nature of customer's activity (Is the customer the owner of any high risk Business?)		1 2 3 4 5 Low – 1; moderate– 2 - 4; high - 5.
2.	Country of residency of the customer or the beneficial owner (Is the customer residing in a high risk Country?)		1 2 3 4 5 Low – 1; moderate – 2 - 4; high - 5.
3.	Type of the customer, registration mode, ownership structure of the customer.		1 2 3 4 5 Low – 1; moderate – 2 - 4; high - 5.
4.	Account opening mode or business relation initiating mode		1 5 1. Face to face 5. Remotely – Internet/e-mail/others or by power of attorney

5.	Operations/transaction making methods		1 5 1. Ordinary – presence at banks office 5. Unordinary – use of correspondent institutions/ payments through electronic means, including internet/e-banking
6.	Deposit of cash during a month		1 2 3 4 5 a) individual 1. MDL 1 – 10,000 2. MDL10,001 – 50,000 3. MDL 50,001 – 100,000 4. MDL 100,001 -250,000 5. MDL 250,001 b) legal entity 1. MDL 1 — 50,000 2. MDL 50,001 — 100,000 3. MDL 100,001 — 250,000 4. 250,001-500,000 5. >500,001
7.	Wire transactions during a month		1 2 3 4 5 a) individual 1. MDL 1- 50,000 2. MDL 50,001- 100,000 3. MDL 100,001 – 300,000 4. MDL 300,001 – 500,000 5. MDL 500,001 b) legal entity 1. MDL 1- 300,000 2. MDL 300,001- 700,000 3. MDL 700,001 – 1,500,000 4. MDL 1,500,001 –3,000,000 5. >MDL 3,000,001
	Transaction profile during a		1 3 5

8.	Transaction profile during a month/quarter/semester/year (Is the customer's activity highly intensive?)		1 3 5 no combination yes
9.	Special KYC questions Is the initial deposit/expected transaction profile in line with the customer profile/ source of funds and source of wealth? etc.		0 18 If satisfactory, the coefficient is – 0; If not satisfactory, the coefficient is-18 and additional the bank should apply measures KYC measures and inform the responsible administrator, if necessary.
	Total points		0-15 = low risk; 16-29= moderate risk; 30-58 = high risk

44. To understand the main threats to which it can be exposed, the bank should proper identify, assess and manage the actual and/or potential risks. Thus, an efficient analysis of bank's activity, through activity's geographical area, number and type of customers and risks lead to a better understanding of constraints and threats involved. As a result, there are undertaken measures and established controls and procedures to minimize the negative influences over bank's activity.

45. The first step of the risk assessment process is the identification of specific products, services, customers, entities and geographical regions which represents a money laundering risk for the bank. The attempts to perform illegal activities through a bank, including those related to money laundering and terrorist financing, can also appear from sources outside the banking system. Thus, quantitative method for risk assessment in the field of money laundering and terrorist financing in a bank, in this case, may be efficiently used. By determining the weight of some products, services, customers, activities etc. in a bank can be established the risk level in the field of money laundering and terrorist financing, at a certain date. A matrix of risk assessment through the described method is presented in Table no.2.

Table no.2: Risk assessment in banks

	Low	Moderate	High
1.	Stable, known customer base, with a business relationship longer than 3 years.	Customers with unstable and changing business relationship with the bank, lasting between 1 to 3 years.	New customers with a business relationship with the bank less than 1 year.
2.	Resident customers.	New resident customers with a business relationship with the bank less than 1 year.	Non-resident customers.
3.	Customers, bank knows the beneficial owner.	Customers, bank knows the founder, but not the beneficial owner.	Customers, bank does not know the beneficial owner or has some suspicions that those are nominal owners.
4.	Customers, who do not use electronic products and services or e-banking (such as, wire transfers, payment of public services or account opening through internet).	Customers, who use electronic services and e-banking, but perform operations rarely.	Customers, who use electronic services and e-banking and perform permanent operations.
	Customers, who perform a limited	Customers, who perform a moderate	Customers, who perform a

5.	Customers, who perform a limited number and volume of cash transactions (<MDL 50 thousands per month).	Customers, who perform a moderate number and volume of cash transactions (>MDL 50 thousands per month and < MDL 500 thousands per month).	Customers, who perform a high number and volume of cash transactions (>MDL 500 thousands per month).
6.	Customers, who perform a limited number and volume of wire transactions (<MDL 500 thousands per month).	Customers, who perform a moderate number and volume of wire transactions (>MDL 50 thousands per month and <MDL 1 million per month).	Customers, who perform a high number and volume of cash transactions (> MDL 1 million per month).
7.	Customers without high risk	Customers without high risk, but with a business relationship with the bank less than 1 year.	High risk customers (customers resident in off-shore areas, PEPs, non-resident customers, etc.).
8.	Customers without high risk activity	Customers without high risk activity, but with a business relationship with the bank less than 1 year.	Customers with high risk activity (customers performing transfers in off-shore areas or other high risk jurisdictions, customers who do not provide confirmative documents, etc.).
9.	The bank has correspondent relationship with resident institutions. The relationship lasts longer than 5 years.	The bank has correspondent relationship with resident institutions. The relationship lasts less than 5 years.	The bank does not have correspondent relationship with resident institutions
10.	Customer, whom bank does not offer services and products on asset management. The bank does not offer such products and services.	Customer, whom bank offers services and products on asset management for a period longer than 3 years, while bank offers such products and services for a period longer than 5 years.	Customer, whom bank offers services and products on asset management, while bank offers such products and services for a period less than 5 years.
11.	Customers who transfer or receive a limited number and volume of cash flows to/from abroad (individuals <MDL 3 thousands per month; legal entities <MDL 500 thousands per month).	Customers who transfer or receive a moderate number and volume of cash flows to/from abroad (individuals >MDL 3 thousands per month and <MDL 15 thousands per month; legal entities >MDL 500 thousands per month and <MDL 3 million per month).	Customers who transfer or receive a high number and volume of cash flows to/from abroad (individuals >MDL 15 thousands per month; legal entities >MDL 3 million per month).
12.	Bank reports to the Office for Prevention and Fight Against Money Laundering a limited number and volume of transactions (< MDL 1million per month).	Bank reports to the Office for Prevention and Fight Against Money Laundering a moderate number and volume of transactions (>MDL 1million per month and < MDL 3 million per month).	Bank reports to the Office for Prevention and Fight Against Money Laundering a high number and volume of transactions (> MDL 3 million per month).
			Bank reports to the Office for Prevention and Fight Against

13.	Bank does not report to the Office for Prevention and Fight Against Money Laundering transactions suspected of terrorist financing.	Bank reports to the Office for Prevention and Fight Against Money Laundering a limited number of transactions suspected of terrorist financing (<5 transactions/quarter).	Money Laundering suspicious transactions of terrorist financing a high number of transactions suspected of terrorist financing (<5 transactions/quarter) .
14.	Customers who do not perform transactions with so- called „bank" from Transnistria region.	Customers who perform a limited number and volume of transactions (<MDL 500 thousands per month) with so-called „bank" form Transnistria region.	Customers who perform a high number and volume of transactions (>MDL 500 thousands per month) with so-called „bank" form Transnistria region.
15.	Customers who perform transactions and to whom the bank does not apply enhanced know-your-customer measures.	Customers who perform transactions and to whom the bank applies a limited number of enhanced know-your-customer measures (max. 2 measures).	Customers who perform transactions and to whom bank applies enhanced know-your-customer measures.
16.	Bank's policies in the field of prevention and combating money laundering and terrorist financing have been updated during the year.	There is a draft for amending bank's policies in the field of prevention and combating money laundering and terrorist financing for their amendment during the year.	Bank's policies in the field of prevention and combating money laundering and terrorist financing have not been updated during the year.
17.	There have been organized more than 6 trainings for employees in the field of prevention and combating money laundering and terrorist financing.	There have been organized trainings for employees in the field of prevention and combating money laundering and terrorist financing.	There have been organized less than 3 trainings for employees in the field of prevention and combating money laundering and terrorist financing.
18.	Bank's employees responsible for taking measures in the field of prevention and combating money laundering and terrorist financing have more than 5 years of work experience.	Bank's employees responsible for taking measures in the field of prevention and combating money laundering and terrorist financing have little work experience.	Bank's employees responsible for taking measures in the field of prevention and combating money laundering and terrorist financing have less than 2 years of work experience.
19.	Internal control division has performed more than 5 controls/inspections during the year in the field of prevention and combating money laundering and terrorist financing.	Internal control division has performed a small number of controls/inspections during the year in the field of prevention and combating money laundering and terrorist financing.	Internal control division has performed less than 2 controls/inspections during the year in the field of prevention and combating money laundering and terrorist financing.
20.	During the year, there have been made no recommendations for activity improvement and no sanctions where applied by the	During the year, there have been made recommendations for improvement of bank's activity in the	During the year, there have been applied sanctions by the supervisory authorities in the

20.	supervisory authorities in the field of prevention and combating money laundering and terrorist financing.	field of prevention and combating money laundering and terrorist financing.	field of prevention and combating money laundering and terrorist financing.
n.	...	...	...

Table description:

Determination of the maximum level of each above-mentioned risk will provide a starting point for the bank to review its internal policies and procedures aimed to minimize the major risks of money laundering and terrorist financing. This table may facilitate this process by calculating a coefficient for each cell, determining the share of each listed factor (the bank may determine a number of "n" factors to consider in the risk assessment). This share may be registered as a coefficient or percentage and it is important that the amount for each field / row is equal to 1 or 100%, respectively. At the end, the coefficient assigned to each column or risk is calculated using the arithmetic mean, and the obtained maximum value will indicate the major share of the risk of money laundering and terrorist financing in the bank. Table no.3 shows an example, which includes 3 factors for assessing the risk of money laundering and terrorist financing:

Table no.3. Example of calculating individual risk levels assigned, taking into account factors / questions from Table no.2.

	Low risk	Moderate risk	High risk
1	30%	45%	25%
2	17%	80%	3%
3	80%	8%	12%
Total	42,3%	44,3%	13.3%

Based on the data from Table no.3, we conclude that the bank is exposed to a moderate risk of money laundering and terrorist financing.

46. Risk assessment is performed in order to detect bank's activities, sectors, services, products and customers etc. which involves increased risks of money laundering and terrorist financing. As a result of knowing these risks, the executive board and / or the bank's board shall approve the directions for minimizing the risks with major impact, by developing appropriate policies and procedures, specifying the level of risk acceptable to the bank. In order to control and minimize the risks of money laundering and terrorist financing, a regular review and update of policies, procedures, measures and controls of the bank is required, and taking into account the trends related to crimes of money laundering and terrorist financing, risk assessment requires annual update.

47. In identifying the risks of money laundering and terrorist financing, it is important to understand the risks to which the bank is exposed in its activity of providing products and services to customers. There are two basic types of risk:
a) Activity risk - which may include the following categories of risk:
- Customers;
- Products and services;
- Practice of offering products and services;
- The countries or jurisdictions where the activity is performed;

b) Regulatory risk - which is associated with non-compliance with the requirements for prevention and combat of money laundering and terrorist financing and includes:
- Improper conduct of customer identification and verification;
- Failure in identifying the beneficial owner;
- Failure in identifying the source of funds;
- Insufficient training of employees;
- Lack of a programme and an adequate policy;
- Lack of monitoring of transactions, lack of reporting to the competent authority etc.

48. Following the identification of the risks of money laundering and terrorist financing, it is necessary to measure or assess them. In this context, another method that can be used in the bank's risk assessment of money laundering and terrorist financing is the qualitative method, which means the combined use of the probability of the risk occurrence and its impact on bank's activity. The probability of risk should be based on previous experiences and the impact the risk can have represents the influence on the operational process, financial process, or other bank's activity, including reputation.

49. According to this method, as in another methods, a matrix is formed that indicates, on the one hand, the factors that influence the risk and, on the other hand, the indicators that measure the risk; in this case it represents the probability of materialization and the impact on business. Subsequently, the level of risk is calculated and measures are taken to minimize the risks identified as high. A simple illustration of those described above is shown in Table no.4.

Table no.4. Risk assessment matrix

Likelihood				
Very likely	Medium 2	High 3	Extreme 5
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2
	Low	**Moderate**	**High**
	Impact		

Table description:

After identifying the risk factors, the risk level of money laundering and terorrist financing can be calculated using the above matix (Probability * impact= risk level). The probability degree refers to potential risks of money laundering and terrorist financing that can arise in bank's activity and can be defined by a necessary number for an adequate risk assessment. Although the illustrated model highlights three levels of probability (very likely, likely, unlikely), each bank may define a number of different levels of risk likelyhood adapted to its activity (for example, another model may be: not applicable, rare, unlikely, likely, very likely and guaranteed).

The description of the 3 levels of likelihood is as follows:
a) very likely - the risk is very likely to occure based on previous experiences and will probably occur several times a year;
b) likely - the risk may occur based on previous experiences and there is the probability that it will occur once a year;
c) unlikely - the risk is unlikely to occur based on previous experiences.
In similar circumstances, the bank may also define the level of impact on its business. The above model shows three levels of impact (low, moderate and high), but each bank may define a number of different

levels of risk impact adapted to its activity (for example, another model may be: not applicable, insignificant, low, moderate, high and extreme).
It is essential to mention that the level of impact relates to the consequences of resulting losses and the severity of damage occurred if risks materialize. They may materialize, depending on the activity of each bank, and may be emphasized by the current risk of loss, reputational risk, risk of damage, risk of sanctions etc.
The description of the 3 levels of impact is the following:
a) high - the event would have serious consequences by causing major losses or would influence serious terrorist acts and money laundering;
b) moderate - the event would have a moderate impact and consequences on the activity;
c) low - the event would have an insignificant or reduced impact on the activity.
The description of potential risks presented in the matrix in Table no.4 is as follows:
a) extreme (5) – the materialization of risk is certain and it will have very serious consequences on bank's activity, such as: sanctions from the supervisory authority, loss of customers, loss of personnel, large financial losses and a major impact on bank's activity;
b) high (3) - high probability of materialization of risk and it will have major consequences on bank's activity, such as: moderate sanctions from the supervisory authority, loss of a significant number of customers, loss of key personnel, major financial losses and a significant impact on bank's activity;
c) medium (2) - low probability of materialization of risk and it will have insignificant consequences on bank's activity, such as: minor sanctions from the supervisory authority, loss of a small number of customers and key personnel, insignificant financial losses;
d) low (1) - no significant concerns regarding bank's activity in case of materialization of risk.
Based on the above, the risk assessment of money laundering and terrorist financing in the bank may be performed by using the method described, as shown in the example of Table. 5:

Table no.5. Example of calculating the risk level in the bank, based on the matrix from Table no.4.

Group of risk/factors:	**Customers/Services**		
	Likelihood	**Impact**	**Risk level**
New customers	Likely	Moderate	2
Customers making significant cash transactions	Likely	Very High	3
Customers making significant wire transfers	Very Likely	Very High	5
NGO Customers	Likely	Very High	3
Customers not benefiting from e-banking services	Likely	Low	1
Asset management services	Likely	Very High	3
Customers - correspondent institutions with business relations longer than 5 years	Likely	Low	1
n	...	...	...
Total risk (geometric mean calculation of factors and potential risks)			**2**

50. Risk assessment will allow the bank to determine the vulnerable sectors of its activity and will provide accurate information about the areas towards which existing resources should be directed in order to achieve the aim of reducing the risks of money laundering and terrorist financing. For this, the risk assessment will be made known to the management and will form the basis for the development of internal policies and procedures in the field, which, ultimately, will reflect requirements for bank risk, stating the acceptable risk level. Consistent application of controls and precautions will allow the bank to adequately manage potential situations of involvement in money laundering operations and terrorist financing, and the policies and procedures to minimize the risks of money laundering and terrorist financing, taking into account the risk assessment results, will lead to the optimal implementation of the recommendations of relevant international and national standards applicable in the field.

See also

Tags

risk based approach [1]

money laundering [2]

terrorist financing [3]

internal control [4]

96 [5]

Source URL:
https://www.bnm.md/en/content/recommendations-banks-risk-based-approach-actions-taking-relation-their-customers-context

Related links:

[1] https://www.bnm.md/en/search?hashtags[0]=risk based approach [2] https://www.bnm.md/en/search?hashtags[0]=money laundering [3] https://www.bnm.md/en/search?hashtags[0]=terrorist financing [4] https://www.bnm.md/en/search?hashtags[0]=internal control [5] https://www.bnm.md/en/search?hashtags[0]=96