

UDC 336:330.341:334(477)

Ponomarenko V.

*Doctor of Economics, Professor, Rector,
Simon Kuznets Kharkiv National University of Economics, Ukraine;
e-mail: pvs@hneu.edu.ua*

Kyrkach S.

*Ph. D. in Economics,
Associate Professor of the Banking and Financial Services Department,
Simon Kuznets Kharkiv National University of Economics, Ukraine;
e-mail: kirkachsn@ukr.net*

Pleskun I.

*Ph. D. student of the Banking and Financial Services Department,
Simon Kuznets Kharkiv National University of Economics, Ukraine;
e-mail: inna.pleskun1993@gmail.com*

Lozynska O. I.

*Ph. D. student of the Banking and Financial Services Department,
Simon Kuznets Kharkiv National University of Economics, Ukraine;
e-mail: olgalozinskaya1@gmail.com*

RISK-ORIENTED APPROACH IN THE PRIMARY FINANCIAL MONITORING BY BANKS

Abstract. The ongoing changes in the legal regulations for banks to conduct financial monitoring make the research on the risk-oriented approach implementation in the Ukrainian banking sector relevant. The declining share of information bearing the signs of internal financial monitoring in the total amount of information provided by banks highlights the need to further improve the methods used to assess suspicious financial transactions conducted by banks and the risks associated with them, given the effectiveness of their detection and depth of consequences. The article is aimed to improve the risk-oriented approach in the primary financial monitoring by banks through the substantiated elements composing the system of significant risks associated with money laundering and terrorist financing. While substantiating the elements composing the system of significant risks associated with money laundering and terrorist financing, it is crucial to consider the international risk management standards based on the assessment of threats, vulnerability to threats and their consequences for the bank and national security at all levels. Implementing the following steps: threat identification considering the type and jurisdiction of customers and types of financial transactions and channels for their implementation, justification of banks' vulnerability to middle and high level threats, significant consequences of money laundering and terrorist financing risks allowed presenting in detail the areas of interest for the bank risk management. The research determined financial transactions subject to the recommendation to use high, increased and traditional prudence while identifying and verifying transactions. The proposed banks' prudence areas built in reliance on the analysis of the legal framework for combating money laundering and terrorist financing, statistics provided by the State Financial Monitoring Service and the NBU allow banking institutions to focus on the risks posed by money laundering and terrorist financing, which have a significant impact on their activities. Further research should focus on forming a mathematical tool for assessing the bank's risks in the financial monitoring of money laundering and terrorist financing.

Keywords: risk, bank, financial monitoring, money laundering, terrorist financing.

Formulas: 1; fig.: 5; tabl.: 3; bibl.: 20.

Пономаренко В. С.

*доктор економічних наук, професор, ректор,
Харківський національний економічний університет імені Семена Кузнеця, Україна;
e-mail: pvs@hneu.edu.ua*

Киркач С. М.

*кандидат економічних наук, доцент кафедри банківської справи і фінансових послуг,
Харківський національний економічний університет імені Семена Кузнеця, Україна;
e-mail:kirkachsn@ukr.net*

Плескун І. В.

*аспірант кафедри банківської справи і фінансових послуг,
Харківський національний економічний університет імені Семена Кузнеця, Україна;
e-mail: inna.pleskun1993@gmail.com*

Лозинська О. І.

*аспірант кафедри банківської справи і фінансових послуг,
Харківський національний економічний університет імені Семена Кузнеця, Україна;
e-mail: olgalozinskaya1@gmail.com*

РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД У ПЕРВИННОМУ ФІНАНСОВОМУ МОНІТОРИНГУ БАНКІВ

Анотація. З огляду на зміни законодавчих підстав для проведення банками фінансового моніторингу актуальності набувають дослідження проблематики впровадження ризик-орієнтованого підходу в банківському секторі України. Тенденція зменшення частки інформації з ознаками внутрішнього фінансового моніторингу в загальній кількості поданої банками інформації свідчить про потребу подальшого вдосконалення методів оцінки підозрілих фінансових операцій банків та ризиків, пов'язаних із ними, урахуваючи результативність їх виявлення та глибину наслідків. Метою роботи є удосконалення ризик-орієнтованого підходу в первинному фінансовому моніторингу банків через обґрунтування елементів системи суттєвих ризиків відмивання капіталу та фінансування тероризму.

Обґрунтування елементів системи суттєвих ризиків відмивання капіталу і фінансування тероризму ґрунтується на міжнародних стандартах ризик-менеджменту, виходячи з оцінки загроз, уразливості до загроз і їхніх наслідків для банку та національної безпеки всіх рівнів. У результаті реалізації кроків: визначення загроз у розрізі типу та юрисдикцією клієнтів видами фінансових операцій та каналів їх реалізації обґрунтування вразливості банків до загроз середнього та високого рівня, значних наслідків ризиків відмивання капіталу та фінансування тероризму, деталізовано зони особливої уваги банківського ризик-менеджменту. Установлено фінансові операції, для яких рекомендовано застосування високої, підвищеної та традиційної обачності в ідентифікації та верифікації операцій. Пропоновані зони обачності банків, сформовані на основі аналізу законодавчої бази з протидії відмивання капіталу та фінансування тероризму, статистики Державної служби фінансового моніторингу та НБУ, уможливають акцентування уваги банківських установ на ризиках відмивання капіталу і фінансування тероризму, які мають суттєвий вплив на їхню діяльність. Перспективою подальших досліджень має стати формування математичного апарату для оцінки ризиків банку у фінансовому моніторингу фактів відмивання капіталу та фінансування тероризму.

Ключові слова: ризик, банк, фінансовий моніторинг, відмивання капіталу, фінансування тероризму.

Формул: 1; рис.: 5; табл.: 3; бібл.: 20.

Introduction. The issue of combating money laundering (anti-money laundering)/terrorist financing (ML/TF) is recognized worldwide. Its solution is based on implementing the recommendations provided by the *Financial Action Task Force on Money Laundering (FATF)* in the domestic practice [1].

Banking institutions credited as primary financial monitoring subjects (PFMS) are empowered to identify financial transactions bearing ML/TF signs and report on them to the state financial monitoring subjects. At the same time, the Basel Committee's recommendations on the ML/TF risk management [2] lay an emphasis on the fact that banks' neglect of a high-quality and

effective ML/TF risk management system exposes them to negative consequences due to reputational, operational, compliance and concentration risks, which may lead to significant financial costs met by the bank. Changes in the legal regulations for banks to conduct financial monitoring, represented in the Resolution adopted by the Board of the National Bank No.65 as of 19/05/2020 [3], highlight the need for further research on the risk-oriented approach implementation in the Ukrainian banking sector.

Research analysis and task assignment. ML/TF risks in the banking sector belong to the sectoral risks of the national system governed by laws and regulations. The *FATF* Guidance for a Risk-Based Approach for the Banking Sector [4] establishes its binding nature and provides basic principles and implementation examples on a country-by-country basis. In particular, it is suggested to substantiate the factor analysis in determining the ML/TF risk through banks relying upon the assessment of the geographical activity area and customer database, structure and type of bank customers, structure of products and services, channels for their provision by financial institutions, which are divided into high, middle and low risks.

The domestic regulatory framework for combating ML/TF using banks comprises the provisions set out in the Law of Ukraine «On the National Bank of Ukraine» (Articles 7, 15, 55, 56) [5], the Law of Ukraine «On Banks and Banking» (Article 63) [6], the Law of Ukraine «On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Terrorist Financing and Financing the Proliferation of Mass Destruction Weapons» [7] and the Resolution adopted by the Board of the National Bank «On Approval of the Regulations on Financial Monitoring by Banks» [3; 20].

In recent years, the risk-oriented approach to financial monitoring in the banking sector has been considered in the scientific literature by the following scientists: Zh. Andrijchenko and N. Vnukova [8], O. Ghlushhenko and I. Semeghen [9], S. Jekhorycheva [10], O. Kolodiziev, O. Lebidj, O. Vejc [11], B. Samorodov [12], O. Utkina [13, 14].

While positively noting the domestic scientists' work, as well as the statistics provided in the report by the State Financial Monitoring Service of Ukraine [15] concerning the increased amount of information from banks on financial transactions showing the financial monitoring signs, the declining share of information bearing the signs of internal financial monitoring in the total amount of information provided by banks highlights the need to further improve the methods used to assess suspicious financial transactions conducted by banks and the risks associated with them, given the effectiveness of their detection and depth of consequences.

The article is aimed to improve the risk-oriented approach in the primary financial monitoring by banks through the substantiated elements composing the system of significant risks associated with ML/TF.

Research results. The methodology used to assess the risks of money laundering and terrorist financing in Ukraine [16; 19] at a nationwide scale is based on the international risk management standards. The probable negative events (risks) are determined with respect to the assessment of threats, vulnerability to threats and their consequences.

Applying these provisions to the ML/TF risks using banks allows defining the sectoral risk function as follows:

$$R_{\delta} = f[(T_{\delta}), (V_{\delta})] \cdot C,$$

where R_{δ} — the ML/TF risk function using banks;

T_{δ} — the identified ML/TF threats using banks;

V_{δ} — the identified vulnerability to threats;

C — the level of negative consequences caused by threats and vulnerabilities of the bank.

The first step in determining the ML/TF risk through banking institutions should be the threat identification. It is proposed to consider the type and jurisdiction of customers and types of financial transactions and channels for their implementation during such an assessment.

The Law of Ukraine «On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Terrorist Financing and Financing the Proliferation of Mass Destruction

Weapons» establishes an unacceptable risk for transactions in which it is impossible to identify and/or verify the transaction participant, identify the participants' ultimate beneficial owners, unreliable information submitted by customers, the existing reasonable suspicions/grounds testifying to the fact of accomplishing the ML/TF transactions by customers, their affiliation to «shell companies», and if the bank with which the correspondent relationship is established is a shell bank and/or maintains correspondent relations with a shell bank [7]. Provided the above circumstances exist, the assets involved in the transaction are blocked and the bank must abandon it.

High-risk zones include four types of threshold financial transactions, which are subject to mandatory monitoring: transactions performed by PEPs (PEP — *Politically Exposed Person*), their family members and/or persons related to a politically exposed person; transfers abroad, including offshore zones; cash transactions; transactions where the participant/bank is from a country that fails to comply with the FATF recommendations if the transaction amount is equal to or exceeds UAH 400 thous. (UAH 30 thous. for business entities that provide services in the field of lotteries and/or gambling) [7]. Article 5 of the Law of Ukraine «On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Terrorist Financing and Financing the Proliferation of Mass Destruction Weapons» also defines a high risk for transactions with: foreign financial institutions; foreign politically exposed persons and members of their families; customers subject to sanctions and customers whose place of residence (stay, registration) is a state enlisted as an offshore zone [7]. According to the Resolution adopted by the Board of the National Bank «On Approval of the Regulations on Financial Monitoring by Banks» the high-risk zone also applies to: transactions performed by customers operating with virtual assets; customers in respect of whom the bank suspects ML/TF transactions, committing other crimes or their affiliation to shell companies [3]. The existence of such bank's transactions requires enhanced identification and verification.

Annex 19 to the Regulations on Financial Monitoring by Banks specifies risky types of customers that fall into the middle risk category: based on the commercial or personal activities performed by the customer or its UBOs (ultimate beneficial owners) when cash settlements predominate in the activities, in particular, the transactions associated with a high corruption risk; the term and legal form of establishment, complicated customer's ownership structure; the reputation of the customer or its UBOs; citizenship, registration, location, business activities of the customer, its UBOs and the customer's key counterparties in the countries where the ML/TF combating regimes are poor or countries characterized by an increased corruption risk [3]. The existence of such bank's transactions also requires enhanced identification and verification and an effective system of internal risk management.

The low-risk zone includes transactions performed by companies that effect simple transactions and individuals who are not suspected of ML/TF. Minimum requirements for identification and verification apply to such transactions.

The minimum risk zone is associated with financial transactions involving public authorities, diplomatic missions of foreign countries, public legal entities with shares listed on internationally recognized exchanges, persons who have accounts for wages and social benefits, housing and utilities infrastructure.

Identification of bank threats in the two-dimensional plane «type of transaction participant/nature of banking products, services and their supply channels» requires to consider the volume of risky transactions addressed in Annex 19 to the Regulations on Financial Monitoring by Banks as those including: private banking services, obtaining loans secured by financial tools or other bank guarantees, customer's use of asset management services, complexity of a transaction due to its multi-stage nature, anonymity and presence of numerous participants, cash transactions, international transfers, e-commerce [3].

In our opinion, cash transactions should be included in the high-risk zone. Thus, the State Financial Monitoring Service emphasizes that «cash used as the main facilitator (a tool that facilitates achievement of a goal) in the money laundering cycle is a problematic issue, the relevance of which is monitored at both levels — highly developed countries and developing countries» [17]. According to the NBU, in recent years the amount of cash transactions through the

banks' cash departments has been increasing, and their amount for the period January-March 2020 is UAH 531.7 billion by revenue and UAH 536.6 billion as issued [18].

Money transfers without opening a bank account also pose a high risk of ML/TF, in particular, recognizing the tendency to increase the dynamics of transfers from abroad to Ukraine through banking institutions (*Fig. 1*).

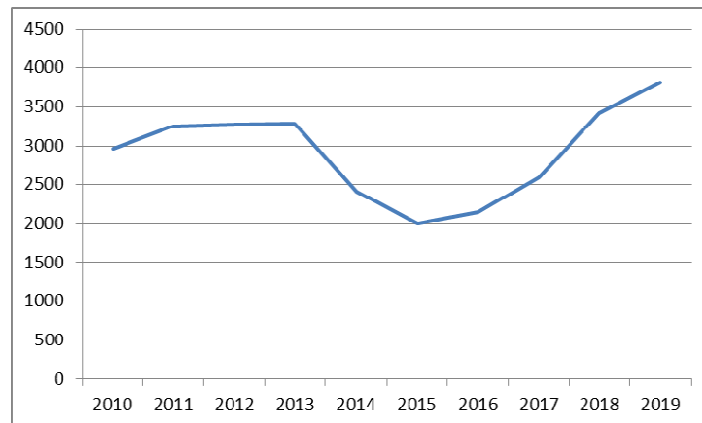


Fig. 1. Dynamics of money transfers from abroad to Ukraine through banks, USD mln
Source: formed according to the NBU [18].

The high risk of using electronic money in Ukraine is associated with the complexity of customer identification, easy and fast cross-border movement of funds, which makes this tool attractive especially for TF. The tendency to intensify this direction (*Fig. 2*) necessitates increased attention considering the banking institution's risk.

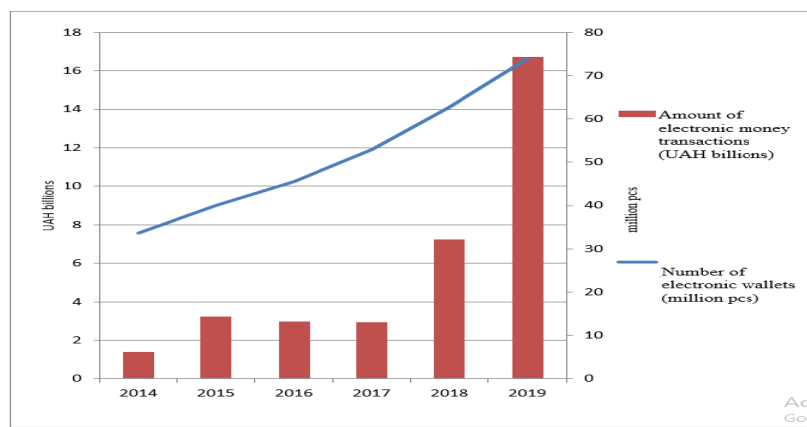


Fig. 2. Dynamics of electronic money development in Ukraine

Source: formed according to the NBU [18].

Securities transactions can be considered high-risk in the field of financial monitoring due to the possible facts of their fictitiousness.

It is proposed to include financial transactions related to servicing deposit and credit accounts in the middle risk zone due to the difficulty faced by the bank while verifying the sources of deposit funds and credit expenditure directions.

Currency exchange involving insignificant amounts (up to UAH 30 thous.) represents a transaction where the customer identification is not necessary and thus it belongs to the zone of low ML/TF risk. The same zone includes cash and transfer transactions with insignificant amounts.

Transactions in the amount of up to UAH 5 thous. or maintenance of accounts for social/pension payments, payments of wages, fines, taxes by customers will be assigned to the minimum risk zone.

In this respect, financial transactions can be grouped according to the risk level as follows (*Table 1*).

Table 1

Risk zones formed by the nature of banking products, services and their supply channels

Risk zone	Transaction characteristics
Unacceptable risk	Any transaction in any amount based on the customer’s features listed in [3; 7]
High risk	Any transactions in the amount over UAH 400 thous. or transactions in the amount of UAH 30 thous. and more up to UAH 399.999 thous. regarding: cash withdrawals from customers’ accounts; acceptance of cash for transfer or transfer payments without opening an account; transactions using electronic means, with securities
Middle risk	Any transactions in the amount of UAH 30 thous. and more up to UAH 399.999 thous. or: servicing deposit and credit accounts, renting out an individual safe without a list of values
Low risk	Transactions up to UAH 30 thous. including currency exchange and cash transactions and transfers
Minimum risk	Transactions in the amount of up to UAH 5 thous. or maintaining accounts for social/pension payments, payments of wages, payments of fines and taxes by customers

Further we will form a threat matrix according to the given risk parameters for the customer type and the nature of banking services/transactions (Fig. 3).

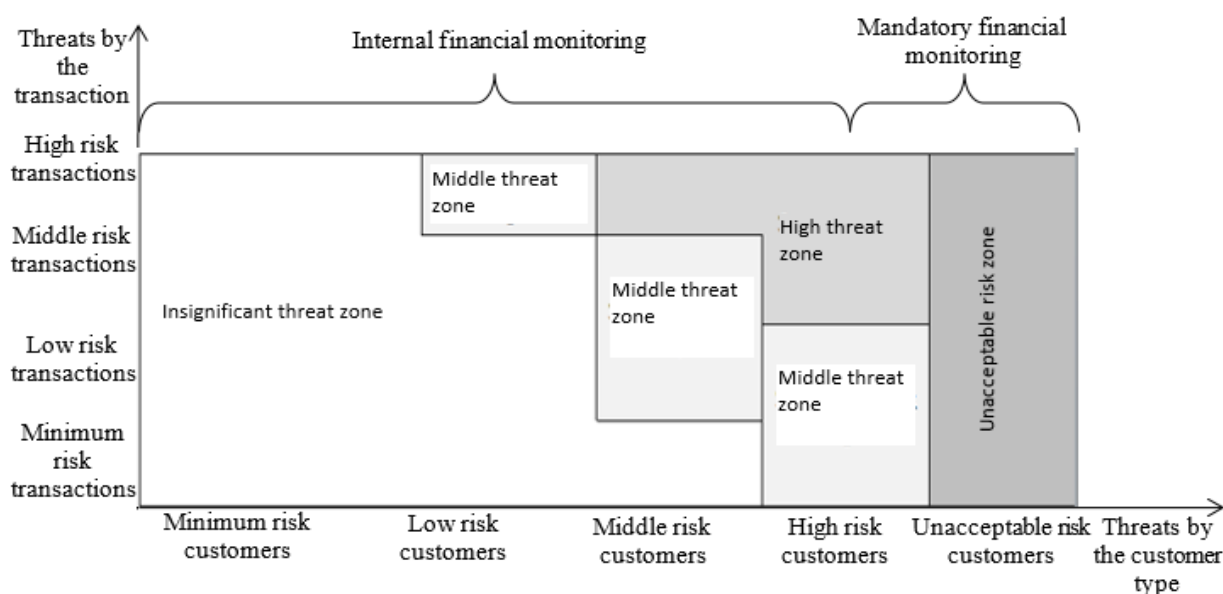


Fig. 3. Bank’s threat zones in the field of financial monitoring associated with ML/TF

Source: formed by the author.

It can be stated that the unacceptable risk and part of the high risk shall be subject to mandatory financial monitoring as it follows from the features of unacceptable risk customers and threshold transactions. At the same time, internal financial monitoring includes a number of middle and high threats detected by the bank.

As can be seen from the report produced by the State Financial Monitoring Service of Ukraine [15] (Table 2), the share of identified financial transactions bearing the signs of internal financial monitoring was 41.56% in total in 2005, and it amounted to only 2.55% in 2018. Such a state of affairs may testify to the vulnerability of the banking system to the ML/TF risk if put beyond the established mandatory norms.

Table 2

Structure of PFMS’ financial transactions registered by the State Financial Monitoring Service, %

Financial transactions/year	2005	2006	2007	2008	2009	2010	2011
Share of financial transactions bearing the signs of mandatory financial monitoring	55.43	61.96	67.94	72.89	74.24	70.08	43.12
Share of financial transactions bearing the signs of internal financial monitoring	41.66	35.49	30.74	26.24	25.00	28.62	37.81
Share of financial transactions bearing the signs of mandatory and internal financial monitoring	2.91	2.55	1.32	0.87	0.76	0.78	0.37
Share of financial transactions bearing tracking features	-	-	-	-	-	0.52	18.70

Table 2 (continued)

Financial transactions/year	2012	2013	2014	2015	2016	2017	2018
Share of financial transactions bearing the signs of mandatory financial monitoring	64.16	66.56	60.61	88.91	93.76	95.24	96.93
Share of financial transactions bearing the signs of internal financial monitoring	28.7	31.86	38.10	9.35	4.99	3.72	2.55
Share of financial transactions bearing the signs of mandatory and internal financial monitoring	0.71	0.87	0.90	1.39	1.25	0.94	0.52
Share of financial transactions bearing tracking features	6.43	0.71	0.39	0.35	-	0.10	-

Source: formed according to the State Financial Monitoring Service of Ukraine [15].

Vulnerabilities of banking institutions were identified with reference to the analyzed statistics on the revealed violations due to non-compliance with the financial monitoring requirements by domestic banks for the period of 2018 – 5 month of 2020 published by the NBU [18] (Fig. 4).

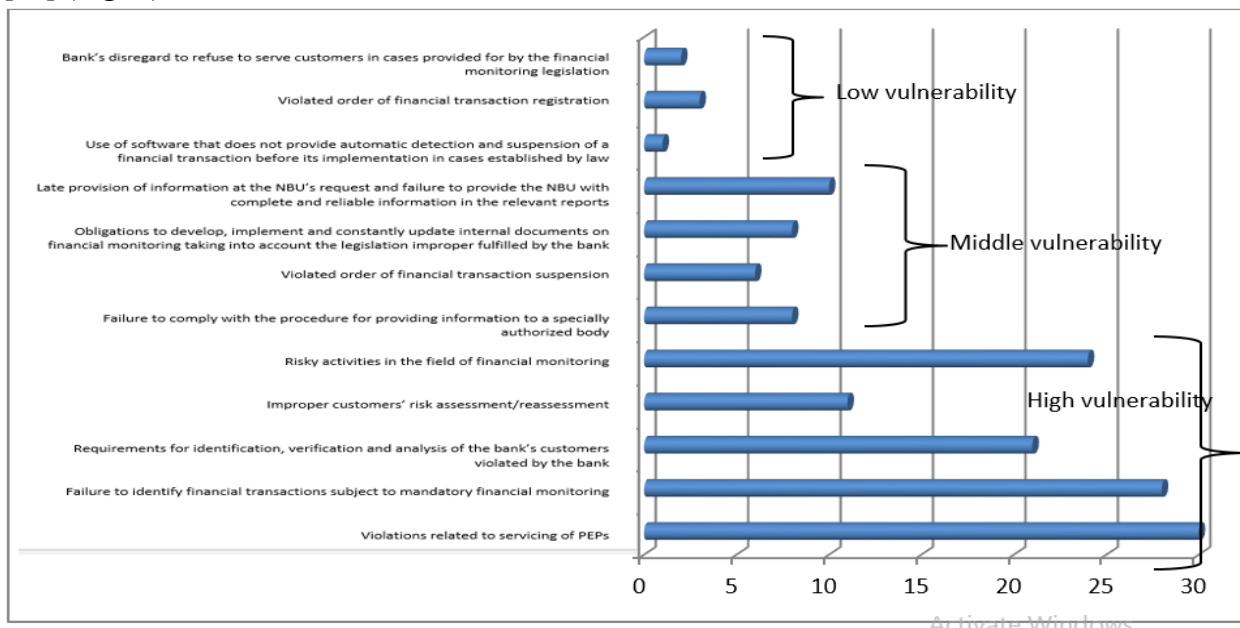


Fig. 4. The number of revealed violations due to non-compliance with the financial monitoring requirements by domestic banks for the period of 2018 — 5 month of 2020

Source: formed according to the NBU [18].

As expected above, high vulnerability zones for banks include violations of transactions bearing the signs of internal or internal and mandatory monitoring. Accordingly, the vulnerability is high if the bank applies imperfect systems and procedures to identifying and verifying customers and financial transactions, in particular, when the bank's internal monitoring fails to detect the mandatory monitoring signs, threshold transactions and take the appropriate measures.

The middle vulnerability zone includes organizational aspects of financial monitoring. That is, banks, even those with a well-established system applied to identify and verify customers and financial transactions, may be at ML/TF risk due to improper information and communication relations with the NBU and the authorized state financial monitoring body, failure to keep up with the updated legislation norms and the need for harmonizing the internal financial monitoring with regulatory changes.

Only a few violations are associated with the bank's disregard to refuse to serve customers in cases provided for by the financial monitoring legislation (unacceptable risk). Therefore, the low vulnerability zone should include threats related to the clearly statutory defined inability to identify and/or verify the transaction participant, identify the participants' ultimate beneficial owners, unreliable information submitted by customers, the existing reasonable suspicions/grounds testifying to the fact of accomplishing the ML/TF transactions by customers, their affiliation to «shell companies», and if the bank with which the correspondent relationship is established is a shell bank [7].

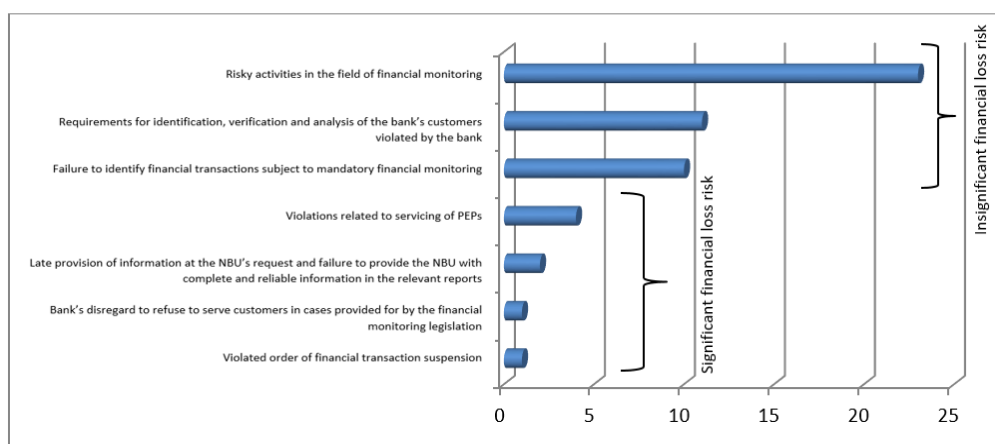
The bank’s vulnerability can be considered minimum if it applies an effective system to identifying and verifying customers and financial transactions and strictly adheres to the financial monitoring legislation rules.

The ML/TF risk consequences (the third step of the risk-oriented approach) afford grounds for distinguishing the following groups:

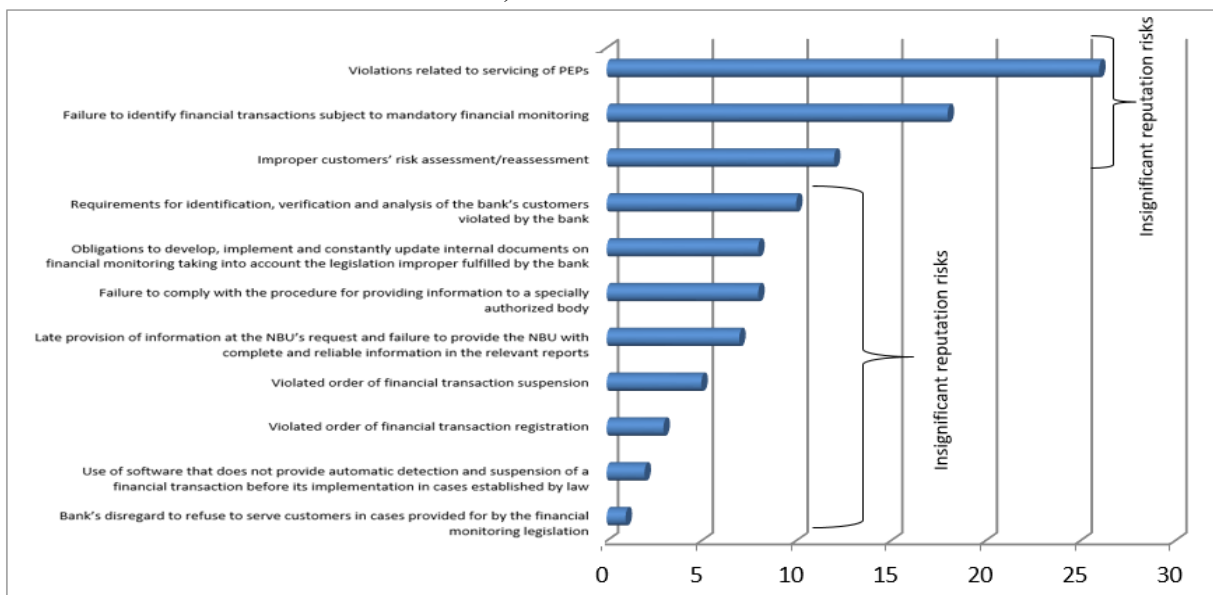
risks that have a significant impact on the national and international security. These include the unacceptable risk transactions and transactions performed by politically exposed persons (PEPs), their family members and/or related persons, participants/banks from a country that fails to comply with the FATF recommendations, which effect any transactions in the amount of UAH 400 thous. and more;

risks that lead to significant financial losses suffered by banks due to fines for violated transactions bearing the ML/TF signs detected by the State Financial Monitoring Service (Fig. 5a);

risks that expose banks to reputational risks due to the use of written warnings for violated ML/TF transactions detected by the State Financial Monitoring Service (Fig. 5b).



a) the number of fines



b) the number of written warnings

Fig. 5. The number of fines and written warnings for non-compliance with the financial monitoring requirements by domestic banks for the period of 2018 — 5 month of 2020

Source: formed according to the NBU [18].

Thus, focusing on zones of middle and high threats, middle and high vulnerability of banks, significant consequences of the ML/TF risks makes it possible to present in detail the areas of interest for the bank risk management (Table 3).

The proposed banks' prudence areas built in reliance on the analysis of the legal framework for combating ML/TF and the statistics provided by the State Financial Monitoring Service and the NBU allow banking institutions to focus on the risks posed by ML/TF, which have a significant impact on their activities.

Table 3

Areas of the banks' interest during financial monitoring

Bank's prudence area	Transactions recommended as subject to application	
High prudence areas related to identification and verification of transactions	Transactions performed by politically exposed persons (<i>PEPs</i>), their family members and/or related persons/participants/banks from a country that fails to comply with the recommendations provided by <i>FATF</i> /foreign financial institutions/foreign public persons and members of their families/customers subject to sanctions/customers whose place of residence (stay, registration) is the state enlisted as an offshore zone/customers operating with virtual assets/customers in respect of whom the bank suspects ML/TF transactions, committing other crimes or their affiliation to shell companies, for which the bank effects transactions amounting to UAH 400 thous.	
Increased prudence areas related to identification and verification of transactions	Transactions performed by politically exposed persons (<i>PEPs</i>), their family members and/or related persons/participants/banks from a country that fails to comply with the recommendations provided by <i>FATF</i> /foreign financial institutions/foreign public persons and members of their families/customers subject to sanctions/customers whose place of residence (stay, registration) is the state enlisted as an offshore zone/customers operating with virtual assets/customers in respect of whom the bank suspects ML/TF transactions, committing other crimes or their affiliation to shell companies/companies or their UBOs whose activities are characterized by predominant cash settlements/associated with a high corruption risk/incorporated recently or with a complicated ownership structure/with a low reputation/with a citizenship, registration, location, business activities (as well as their key counterparties) in the countries where the ML/TF combating regimes are poor or countries characterized by an increased corruption risk, for which the bank effects transactions amounting to over UAH 30 thous. for servicing deposit and credit accounts/cash withdrawals from customers' accounts; acceptance of cash for transfer or transfer payments without opening an account; transactions using electronic means, with securities/renting out an individual safe without a list of values	
Traditional prudence areas related to identification and verification of transactions	Transactions performed by companies that effect simple transactions and individuals who are not suspected of ML/TF, for which the bank effects any transactions amounting to over UAH 400 thous. or transactions amounting to UAH 30 thous. and more up to UAH 399,999 thous. regarding: cash withdrawals from customers' accounts; acceptance of cash for transfer or transfer payments without opening an account; transactions using electronic means, with securities	Transactions performed by politically exposed persons (<i>PEPs</i>), their family members and/or related persons/participants/banks from a country that fails to comply with the recommendations provided by <i>FATF</i> /foreign financial institutions/foreign public persons and members of their families/customers subject to sanctions/customers whose place of residence (stay, registration) is the state enlisted as an offshore zone/customers operating with virtual assets/customers in respect of whom the bank suspects ML/TF transactions, committing other crimes or their affiliation to shell companies/companies or their UBOs whose activities are characterized by predominant cash settlements/associated with a high corruption risk/incorporated recently or with a complicated ownership structure/with a low reputation/with a citizenship, registration, location, business activities (as well as their key counterparties) in the countries where the ML/TF combating regimes are poor or countries characterized by an increased corruption risk, for which the bank effects currency exchange and cash transactions and transfers up to UAH 30 thous.

Source: compiled by the authors.

Conclusions. The declining share of information bearing the signs of internal financial monitoring in the total amount of information provided by banks highlights the need to further improve the methods used to assess suspicious financial transactions conducted by banks and the risks associated with them, given the effectiveness of their detection and depth of consequences.

While substantiating the elements composing the system of significant risks associated with ML/TF, it is crucial to consider the international risk management standards based on the assessment of threats, vulnerability to threats and their consequences for the bank and national security at all levels. Implementing the following steps: threat identification considering the type and jurisdiction of customers and types of financial transactions and channels for their implementation, justification of banks' vulnerability to middle and high level threats, significant consequences of ML/TF risks allowed presenting in detail the areas of interest for the bank risk

management. The research determined financial transactions subject to the recommendation to use high, increased and traditional prudence while identifying and verifying transactions.

The proposed banks' prudence areas built in reliance on the analysis of the legal framework for combating ML/TF and the statistics provided by the State Financial Monitoring Service and the NBU allow banking institutions to focus on the risks posed by ML/TF, which have a significant impact on their activities.

Further research should focus on forming a mathematical tool for assessing the bank's risks in the financial monitoring of ML/TF.

Acknowledgment. The article is based on the results of the fundamental fiscal topic № 54/2018–2020 «Risk-oriented approach in combating money laundering, terrorist financing and proliferation of mass destruction weapons» (State registration number 0118U000058).

Література

1. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF. Paris, France, 2012–2019. URL : <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.
2. Sound management of risks related to money laundering and financing of terrorism. Bank for International Settlements. 2017. URL : <https://www.bis.org/bcbs/publ/d405.pdf>.
3. Про затвердження Положення про здійснення банками фінансового моніторингу: Постанова Правління Національного банку від 19.05.2020 № 65. URL: <https://zakon.rada.gov.ua/laws/show/v0065500-20#Text>.
4. Risk-based Approach. Guidance for the Banking Sector. FATF. Paris, France, 2014. URL : <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html>.
5. Про Національний банк України: Закон України від 20.05.1999 № 679-XIV. *Відомості Верховної Ради України*. 1999. № 29. URL: <https://zakon.rada.gov.ua/laws/show/679-14#Text>.
6. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III. *Відомості Верховної Ради України*. 2001. № 5–6. URL: <https://zakon.rada.gov.ua/laws/show/2121-14#Text>.
7. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. *Відомості Верховної Ради України*. 2020. № 25. URL : <https://zakon.rada.gov.ua/laws/show/361-20#n831>.
8. Андрійченко Ж. О. Фінансовий моніторинг у системі управління ризиками ринків фінансових послуг. Розвиток системи управління ризиками ринків фінансових послуг : монографія / наук. ред. і кер. кол. авт. Н. М. Внукова. Харків : Ексклюзив, 2014. С. 140–150.
9. Глущенко О. О., Семерен І. Б. Антилегалізаційний фінансовий моніторинг: ризик-орієнтований підхід : монографія / за ред. Р. А. Слав'юка. Київ: УБС НБУ, 2014. 386 с.
10. Єгоричева С. Б. Фінансова інклюзія в рамках системи протидії легалізації злочинних доходів та фінансуванню тероризму. *Фінансовий простір*. 2018. № 4 (32). С. 80–87.
11. Пономаренко В. С., Колодізев О. М., Лебідь О. В., Вейц О. І. Оцінювання системи запобігання та протидії легалізації сумнівних доходів клієнтів банку. *Фінансово-кредитна діяльність: проблеми теорії та практики* : зб. наук. пр. 2018. Вип. 3. С. 17–28.
12. Самородов Б. В., Уткіна О. В. Класифікаційні ознаки ризику банківської установи у сфері відмивання коштів або фінансування тероризму. *Вісник Університету банківської справи*. 2018. № 2. С. 47–51.
13. Уткіна О. В. Проблема належного виявлення ступеня ризику відмивання незаконно отриманих доходів банківськими установами України. *Фінансово-кредитна діяльність: проблеми теорії та практики* : зб. наук. пр. 2017. Вип. 2. С. 68–74.
14. Уткіна О. В. Характеристика управління банківським ризиком відмивання коштів / фінансування тероризму та напрями його вдосконалення. *Фінансовий простір*. 2019. № 4. С. 217–227.
15. Звіт про проведення національної оцінки ризиків у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму. *Державна служба фінансового моніторингу України*. 2019. URL : <https://fii.gov.ua/assets/userfiles/310/%D0%9D%D0%9E%D0%A0/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B8/Zvit.pdf>.
16. Методика національної оцінки ризиків відмивання коштів та фінансування тероризму в Україні. *Державна служба фінансового моніторингу України*. 2018. URL : <https://fii.gov.ua/assets/userfiles/310/%D0%9D%D0%9E%D0%A0/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B8/Methodology.pdf>.
17. Ризики використання готівки. *Державна служба фінансового моніторингу України*. 2017. URL : https://nfp.gov.ua/files/DepFinMon/%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA%D0%B8_%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B3%D0%BE%D1%82%D1%96%D0%B2%D0%BA%D0%B8_2017_Nalichka.pdf.
18. Офіційний сайт НБУ. URL: <https://bank.gov.ua>.
19. Lyulyov, O. V., & Pimonenko, T. V. (2017). Lotka-Volterra model as an instrument and innovative processes stability analysis. *Marketing and Management of Innovations, 1*, 159–169.
20. Zarutskaya, E., Pavlova, T., & Sinyuk, A. (2018). Structural-functional analysis as innovation in public governance (case of banking supervision). *Marketing and Management of Innovations, 4*, 349-360. <http://doi.org/10.21272/mmi.2018.4-30>

Статтю рекомендовано до друку 31.08.2020

© Пономаренко В. С., Куркач С. М., Плєскул І. В., Лозинська О. І.

References

1. FATF. (2012-2019). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris, France. Retrieved from <https://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.
2. Bank for International Settlements. (2017). Sound management of risks related to money laundering and financing of terrorism. Retrieved from <https://www.bis.org/bcbs/publ/d405.pdf>.
3. Natsionalnyi bank Ukrainy. (2020). *Pro zatverdzhennia Polozhennia pro zdiisnennia bankamy finansovoho monitorynhu: Postanova Pravlinnia vid 19.05.2020 № 65 [On approval of the Regulations on financial monitoring by banks: Resolution of the Board dated 19.05.2020 № 65]*. URL : <https://zakon.rada.gov.ua/laws/show/v0065500-20#Text> [in Ukrainian].
4. FATF. (2014). Risk-based Approach. Guidance for the Banking Sector. Paris, France. Retrieved from <http://www.fatfgafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html>.
5. Verkhovna Rada Ukrainy. (1999). Pro Natsionalnyi bank Ukrainy: Zakon Ukrainy vid 20.05.1999 № 679-XIV [On the National Bank of Ukraine: Law of Ukraine of 20.05.1999 № 679-XIV]. *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine*, 29. Retrieved from <https://zakon.rada.gov.ua/laws/show/679-14#Text> [in Ukrainian].
6. Verkhovna Rada Ukrainy. (2001). Pro banky i bankivsku diialnist : Zakon Ukrainy vid 07.12.2000 № 2121-III [On banks and banking activities: Law of Ukraine of 07.12.2000 № 2121-III]. *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine*, 5—6. Retrieved from <https://zakon.rada.gov.ua/laws/show/2121-14#Text> [in Ukrainian].
7. Verkhovna Rada Ukrainy. (2020). Pro zapobihannia ta protydiu lehalizatsii (vidmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, finansuvanniu terorizmu ta finansuvanniu rozpozsiudzhennia zbroi massovoho znyschennia: Zakon Ukrainy vid 06.12.2019 № 361-IX [On prevention and counteraction to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction: Law of Ukraine of 06.12.2019 №361-IX] *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine*, 25. Retrieved from <https://zakon.rada.gov.ua/laws/show/361-20#n831> [in Ukrainian].
8. Andriichenko, Zh. O. (2014). *Finansovyi monitorynh u systemi upravlinnia ryzykamy ryнкiv finansovykh posluh. Rozvytok systemy upravlinnia ryzykamy ryнкiv finansovykh posluh [Financial monitoring in the risk management system of financial services markets. Development of risk management system of financial services markets]*. N. M. Vnukova (Ed.). Kharkiv: Ekskluzyv [in Ukrainian].
9. Hlushchenko, O. O., & Semehen, I. B. (2014). *Antylehalizatsiinyi finansovyi monitorynh: ryzyk-orientovanyi pidkhid [Anti-legalization financial monitoring: risk-oriented approach]*. R. A. Slaviuk (Ed.). Kyiv: UBS NBU [in Ukrainian].
10. Yehorycheva, S. B. (2018). Finansova inkluziia v ramkakh systemy protydiu lehalizatsii zlochynnykh dokhodiv ta finansuvanniu terorizmu [Financial inclusion in the framework of the system of combating money laundering and terrorist financing]. *Finansovyi prostir — Financial space*, 4 (32), 80—87. [in Ukrainian].
11. Ponomarenko, V. S., Kolodiziev, O. M., Lebid, O. V., & Veits, O. I. (2018). Otsiniuvannia systemy zapobihannia ta protydiu lehalizatsii sumnivnykh dokhodiv klientiv banku [Evaluation of the system of prevention and counteraction to legalization of doubtful incomes of bank clients]. *Finansovo-kredytна diialnist: problemy teorii ta praktyky — Financial and credit activities: problems of theory and practice*, 3, 17—28 [in Ukrainian].
12. Samorodov, B. V., & Utkina, O. V. (2018). Klasyfikatsiinyi oznaky ryzyku bankivskoi ustanovy u sferi vidmyvannia koshtiv abo finansuvannia terorizmu [Classification features of the risk of a banking institution in the field of money laundering or terrorist financing]. *Visnyk Universytetu bankivskoi spravy — The Banking University Bulletin*, 2, 47—51 [in Ukrainian].
13. Utkina, O. V. (2017). Problema nalezhnoho vyavlennia stupenia ryzyku vidmyvannia nezakonno otrymanykh dokhodiv bankivskymy ustanovamy Ukrainy [The problem of proper identification of the risk of money laundering of illegally obtained income by banking institutions of Ukraine]. *Finansovo-kredytна diialnist: problemy teorii ta praktyky — Financial and credit activities: problems of theory and practice*, 2, 68—74 [in Ukrainian].
14. Utkina, O. V. (2019). Kharakterystyka upravlinnia bankivskym ryzykom vidmyvannia koshtiv / finansuvannia terorizmu ta napriamy yoho vdoskonalennia [Characteristics of bank risk management of money laundering / terrorist financing and areas for improvement. Financial space]. *Finansovyi prostir — Financial space*, 4, 217—227 [in Ukrainian].
15. Derzhavna sluzhba finansovoho monitorynhu Ukrainy. (2019). *Zvit pro provedennia natsionalnoi otsinky ryzykiv u sferi zapobihannia ta protydiu lehalizatsii (vidmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, ta finansuvanniu terorizmu [Report on conducting a national risk assessment in the field of prevention and counteraction to legalization (laundering) of proceeds from crime and terrorist financing]*. Retrieved from <https://fiu.gov.ua/assets/userfiles/310/%D0%9D%D0%9E%D0%A0/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B8/Zvit.pdf> [in Ukrainian].
16. Derzhavna sluzhba finansovoho monitorynhu Ukrainy. (2018). *Metodyka natsionalnoi otsinky ryzykiv vidmyvannia koshtiv ta finansuvannia terorizmu v Ukraini [Methods of national risk assessment of money laundering and terrorist financing in Ukraine]*. Retrieved from <https://fiu.gov.ua/assets/userfiles/310/%D0%9D%D0%9E%D0%A0/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B8/Methodology.pdf> [in Ukrainian].
17. Derzhavna sluzhba finansovoho monitorynhu Ukrainy. (2017). *Ryzyky vykorystannia hotivky [Risks of using cash]*. Retrieved from https://nfp.gov.ua/files/DepFinMon/%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA%D0%B8_%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B3%D0%BE%D1%82%D1%96%D0%B2%D0%BA%D0%B8_2017_Nalichka.pdf [in Ukrainian].
18. Natsionalnyi bank Ukrainy. (n. d.). Ofitsiinyisait [Official site]. Retrieved from <https://bank.gov.ua> [in Ukrainian].
19. Lyulyov, O. V., & Pimonenko, T. V. (2017). Lotka-Volterra model as an instrument of the investment and innovative processes stability analysis. *Marketing and Management of Innovations*, 1, 159—169.
20. Zarutskа, E., Pavlova, T., & Sinyuk, A. (2018). Structural-functional analysis as innovation in public governance (case of banking supervision). *Marketing and Management of Innovations*, 4, 349-360. <http://doi.org/10.21272/mmi.2018.4-30>