

## Board of the National Bank of Ukraine

24 March 2016

Kyiv

No. 194

On approving the Guidelines on carrying out inspections of bank, their standalone subdivisions and foreign banks' branches to assess the sufficiency of the measures taken with respect to the risks related to publicly exposed persons.

Pursuant to Article 63 of the Law of Ukraine *On Banks and Banking*, Article 14 of the Law of Ukraine *On Prevention and Counteraction to Legalization (Laundering) of the Proceeds from Crime, Terrorism Financing and Financing of Weapons of Mass Destruction Proliferation*, Articles 7, 15 and 55 of the Law of Ukraine *On the National Bank of Ukraine*, and in order to increase the effectiveness of National Bank of Ukraine's supervision of the banks, their standalone subdivisions and foreign banks' branches with respect to their compliance with the Ukrainian laws governing relations in the area of AML/CTF, the NBU Board **hereby resolves:**

1. To approve Guidelines on carrying out inspections of bank, their standalone subdivisions and foreign banks' branches to assess the sufficiency of the measures taken with respect to the risks related to politically exposed persons (attached).
2. Kateryna Rozhkova, NBU Acting Deputy Governor, is entrusted with control over implementation of this Resolution.
3. The Resolution enters into force on the day following its official publication.

Govern  
or

Valeria  
Gontareva

APPROVED  
Resolution of the Board of the  
National Bank of Ukraine  
No. 194 of 27 March 2016

Guidelines on carrying out inspections of bank,  
their standalone subdivisions and foreign banks' branches to assess the sufficiency  
of the measures  
taken with respect to the risks related to politically exposed persons.

I. General provisions

1. These Guidelines have been developed to assist the employees of the structural subdivision of the National Bank of Ukraine (hereinafter - the NBU), which ensures realization by the NBU of the function of state regulation and supervision in the area of preventing and counteracting to legalization (laundering) of the proceeds from crime, terrorism financing and financing of weapons of mass destruction proliferation (hereinafter - the Department) with respect to carrying out inspections of banks, their standalone subdivisions and foreign banks' branches (hereinafter - the bank) to assess the sufficiency<sup>1</sup> of the measures taken regarding the risks related to politically exposed persons.

2. Taking into consideration the possibility of using banking services with the aim of legalization (laundering) of the proceeds from crime, including crimes related to corruption, it is important that banks take sufficient measures to identify, assess, monitor, control and manage the risks related to servicing politically exposed persons, persons related to or associated with them, with respect to which there is a risk of corruption offences, including bribery, and embezzlement of public funds.

It is also important that the banks' management implement effective (sufficient) procedures for financial monitoring, which should include measures on identifying politically exposed persons, persons related to or associated with them, identifying sources of funds and assets (in particular, wealth),

<sup>1</sup> The assessment of sufficiency of the measures taken by banks regarding risks related to providing services to politically exposed persons is the component of the general assessment of bank's activities with respect to their compliance with the laws governing relations in the area of prevention of legalization (laundering) of the proceeds from crime, terrorism financing and financing proliferation of weapons of mass destruction as well as of sufficiency of the measures aimed at the prevention and counteraction of legalization (laundering) of the proceeds from crime and terrorism financing. Sufficiency of the measures is based on professional judgment of persons carrying out the bank's inspection.

carrying out of a profound inspection and studying of the financial activity of such customers as well as providing of reports by a bank's authorized person to a manager of the bank's executive body /manager of foreign bank's branch pursuant to the laws in order to manage these risks.

3. Taking into account the high level of laundering the proceeds of corruption through the banking system, it is important that banks may manage the risks related to politically exposed persons. It is also important that banks' management has the possibility of implementing the effective risk-based systems (approaches) aimed at studying such customers, customer's risk monitoring, informing the specially authorized body (hereinafter - SAB), as applicable, and exercising the right provided for in Article 10, part one of the AML/CTF Law and Article 64, part six of the Law of Ukraine *On Banks and Banking* (hereinafter- -the Law on Banks) concerning refusal to enter into contractual relations or conduct financial transactions.

In general, the responsibilities specified in Annex 1 to these Guidelines and accountability of entities subject to financial monitoring with respect to politically exposed persons are specified by the Law on Banks, AML/CTF Law, Regulation on Financial Monitoring Execution by Banks approved by the NBU Board Resolution of 26 June 2015 (as amended) (hereinafter - Regulation No. 417).

Additional explanations are also provided by the Guidelines on identifying politically exposed persons and ensuring execution of financial monitoring of their financial transactions, which are published on the official site of the State Financial Monitoring Service of Ukraine in the Section "Financial monitoring arrangements".

4. The terms and definitions used in the above Guidelines shall have the meaning pursuant to their meaning specified in the Law on Banks, AML/CTF Law, Regulation No. 417, and other laws and NBU regulatory documents.

5. The requirements for organization and carrying out of bank's scheduled and unscheduled on-site inspections on prevention and counteraction of legalization (laundering) of proceeds from crime, terrorism financial and financing of weapons of mass destruction proliferation (hereinafter - the inspection) are specified in the Procedure for Organization and Carrying out Inspections on Prevention and Counteraction of Legalization (Laundering) of Proceeds from Crime, Terrorism Financing and Financing of Weapons of Mass Destruction Proliferation, which was approved by NBU Board Resolution No. 197 of 20 June 2011 (in the wording of NBU Board Resolution No. 499 of 31 July 2015) registered by the Ministry of Justice of Ukraine as No. 852/19590 on 13 July 2011 (as amended) (hereinafter - Regulation No. 197).

6. The inspections of banks' actions concerning identification, verification and studying of politically exposed persons shall be carried out by an inspection team during every inspection.

## II. Engagements

7. The inspection shall include the following tasks:

1) to assess the sufficiency of the measures on managing the risks of legalization of proceeds from crime/terrorism financing, which are defined in bank's internal documents, taking into account the requirements specified by the laws, which regulate the bank's procedures related to establishing of business relations/conducting of a non-current financial transaction in sizable amount with customers - politically exposed persons, and their further servicing;

2) to identify the compliance of bank's internal documents on financial monitoring (hereinafter - bank's internal documents) with the requirements of the laws on financial monitoring;

3) to identify whether the measures, which were taken by the bank with respect to managing risks related to establishing business relations/conducting a non-current financial transaction to a sizable amount with customers - politically exposed persons, and their further servicing, were sufficient and compliant with the laws on financial monitoring;

4) to identify whether the bank's employees and managers acted in compliance with the requirements set forth in bank's internal documents;

5) to identify availability of required documents and information requested by the bank for establishing the affiliation of a person who wants to open an account/establish business relations/ conduct a non-current financial transaction to a sizable amount, or of his/her representative with publicly exposed persons, pursuant to the laws on financial monitoring;

6) to identify sufficiency of the measures on obtaining of a permission for establishing (maintaining/proceeding) of business relations, concluding of agreements, opening of an account, conducting of a non-current financial transaction to a sizable amount;

7) to identify whether the bank's authorized employee/bank's structural subdivision on financial monitoring takes part in the process of obtaining a bank manager's permission for establishing (maintaining/proceeding) business relations with PEPs;

8) to identify whether the issue on sufficiency of the measures taken by the bank with respect to PEPs are covered by the annual inspection of a bank's internal audit subdivision concerning bank's compliance with the requirements of the laws on financial monitoring;

9) to identify whether the bank studies, on a regular basis, financial activities of the customers who are politically exposed persons;

10) to identify sufficiency of the measures taken by the bank with respect to the PEP customers to detect financial transactions subject to financial monitoring, and providing information about them to specially authorized bodies.

11) to assess sufficiency of the measures taken by the bank to manage the risks related to politically exposed persons;

12) to give recommendations to the bank regarding changes to be made to bank's internal documents and/or tougher relevant measures to manage risks related to politically exposed persons, if they were recognized insufficient.

### III. • Internal control questionnaire

8. Based on the analysis of bank's internal documents and results of the assessment of risks of using the bank for legalization of proceeds from crime, which were carried out by a subdivision of the Department carrying out on-site inspections and a systematic analysis according to the Methodology for carrying out of the assessment of risks of using of the bank and foreign bank's branch for legalization (laundering) of proceeds from crime, terrorism financing and financing of weapons of mass destruction proliferation, which was approved by NBU Board Resolution No. 191 of 24 March 2016, and on other available information, and taking into account the results of an interview with the bank's authorized person (in the event of its conducting), the inspection team shall fill in the internal control questionnaire on the issues concerning the risks related to politically exposed persons, which shall include answers to the questions given below:

1) has the Program for identifying, verifying and studying of a bank's customer (if available) and other internal documents regulating the procedure for identifying verifying and studying of bank's customers, particularly, politically exposed persons, been approved by the bank's board? Please. describe the procedure for approving the bank's internal documents here;

2) how often were amendments made in the above bank's internal documents with the aim of assessing sufficiency of the measures concerning their updating, taking into account the requirements of the applicable laws and/or occurrence of events in bank's activities, which may affect the risks of legalization of proceeds from crime (particularly, amendments in the laws in the area of financial monitoring and/or changes in the list of products/services provided by the bank and/or substantial changes in official duties of bank's employees, etc.)? Please indicate the dates of approving new bank's internal documents/making amendments to them for the period subject to inspection;

3) has the bank provided for the procedure for establishing the fact of belonging of customers/customers' representatives to politically exposed persons (in particular, are the questionnaires or other alternative sources containing such information used)? Are the measures taken by the bank sufficient (please analyze this procedure)?

4) does the bank take measures to establish the sources of funds and assets (in particular, wealth), including with respect to the funds for conducting financial transactions by politically exposed persons involving the bank? Please describe the procedure established in the bank;

5) does the bank take measures for profound inspecting of politically exposed persons, and which measures does the bank take when further servicing politically exposed persons (particularly, with respect of carrying out financial transactions)? Please describe the measures taken to conduct a profound inspection and analysis of financial transactions of bank's customers that are politically exposed persons;

6) is the permission for establishing (maintaining/continuing) business relations, concluding agreements, opening accounts, conducting non-current financial transactions in a sizable amount with politically exposed persons, granted by a bank's manager? Please describe the procedure for granting a relevant permission by the bank's manager;

7) is an increase/decrease in the total number of bank's customers, that are politically exposed persons, observed from the date of conducting of the last inspection concerning compliance with the laws on financial monitoring? Please provide the bank's vision concerning a tendency peculiar to the bank (indicate the factors that may cause/facilitate an increase/decrease in this indicator);

8) has the bank taken measures with the aim of studying/training the employees in the area of identification of politically exposed persons among the bank's customers as well as among the persons addressing the bank in order to establish business relations/conduct non-current transactions in a sizable amount? Please describe the measures taken by the bank with the aim of relevant training of the bank's personnel;

9) does the bank use a software and/or other alternative sources for carrying out inspections/searching for (including at the expense of information reflected in external databases purchased by the bank) politically exposed persons at the moment of the initial inspection (screening) when identifying/specifying/additional specifying of information concerning identification/studying of a customer? Please describe the procedure for taking measures related to using the relevant software and/or alternative sources for carrying out inspections/searching for information;

10) do the manager of the foreign bank's branch obtain the report(s) concerning:

the list of politically exposed persons, with whom it is allowed to establish (maintain/continue) business relations (except for the cases when such permission is directly granted by the manager of the bank's executive body/manager of the foreign bank's branch);

the list of politically exposed persons that were refused establishing (maintaining/continuing) of business relations.

Are the reports containing other information about politically exposed persons submitted?

It should be noted which reports contain the above information. Are the report(s) submitted timely to be considered by the manager of the bank's executive body/manager of the foreign bank's branch or to other bank's managers (if any), taking into account the requirements of the Ukrainian laws and requirements of the bank's internal documents (if granting of the relevant information/ report(s) is provided for exclusively by the bank's internal documents)? If the bank has available reports that are provided for exclusively by the bank's internal documents, it is necessary to indicate the list of information included in them, frequency and procedure for their submission. Please obtain the copy of the last submitted report(s) from the bank;

11) how are the files of PEP customers formed (in particular, how are copies of the documents identifying and verifying the politically exposed person verified)?

12) has the bank informed the specially authorized bodies about the politically exposed persons, which had intentions to establish business relations or conduct a non-current transaction in a sizable amount and were refused based on Article 10 of the AML/CTF Law?

13) is information about identification and studying bank's customers (particularly, politically exposed persons) adjusted/additionally adjusted, as specified by the Ukrainian laws and bank's internal documents (in particular, in order to find out that a politically exposed person has become a beneficial owner (controller) of bank's existing customer)? Please describe the procedure for adjusting/additional adjusting of information about identification and studying, which is used by the bank;

14) does the bank keep, pursuant to the Ukrainian laws on financial monitoring, e-copies of the documents/e-documents regarding identification of politically exposed persons (customers, customers' representatives) and politically exposed persons that were refused to conduct financial transactions, customer's studying, adjusting/additional adjusting of information about a customer, and all the documents related to business relations (conducting of a financial transaction) with a customer (including findings of any analysis when carrying out measures on customer's verification or profound inspection)? What are the retention periods for the above documents/e-documents?

#### IV. Verification procedure

9. Once the internal control questionnaire has been filled out, do the following in order to check whether or not the procedures the bank applies to politically exposed persons are in line with the relevant laws and the bank's financial monitoring documents.

10. Analyze the information specified in Chapter III of this document.

11. Check whether copies of the bank's program for identifying, verifying and collecting information about its customers and any other similar internal documents are in line with the relevant financial monitoring laws (as amended).

12. Check the adequacy and effectiveness of the bank's system for checking whether or not the bank's customers and persons (or their beneficiary owners) who want to establish business (contractual) relations with the bank or to carry out a one-off financial transaction involving a large amount of money are politically exposed persons.

13. Require the bank to provide the following information and/or documents:

1) information (in the form of a statement) about:

the number of its customers who are politically exposed persons;

the number of its customers (private individuals) who are close or related to politically exposed persons;

the number of its customers (legal entities) the beneficiary owners (controllers) of which are politically exposed persons, their family members or people who have business or private relations with such persons;

the number of its customers (legal entities) that are related to politically exposed persons (apart from legal entities the beneficiary owners (controllers) of which are politically exposed persons, their family members or people who have business or private relations with such persons);

the number of all of its customers broken down into customer types (legal entities<sup>2</sup> or private individuals);

2) a list of all customers (in the form of a statement) broken down into the categories specified in paragraph 13, subparagraph 1, indents 1 to 4 of this document (provided that banks have politically exposed customers who meet the criteria for breaking down customer files into categories set forth in Annex 2 to this document);

3) trial balance-sheet;

4) book of open/closed accounts;

<sup>2</sup> Entities that entered into collaboration agreements without establishing a legal entity (collaboration of legal entities), as well as individual entrepreneurs and legal entities' subsidiaries and representative offices are classified as legal entities.



5) a list (in the form of a statement) of one-off financial transactions involving a large amount of money that were carried out by the bank's customers during the inspection period;

6) a list (in the form of a statement) of customers that had securities accounts with the bank as of the inspection date;

7) a list (in the form of a statement) of customers and persons authorized to act on behalf or on the instructions of the customers, managers and beneficiary owners (controllers) of corporate customers;

8) a list (in the form of a statement) of customers with whom the bank has business or contractual relations. This statement must list only the bank's customers that have taken out loans, use bank safes or any other bank products that do not require opening an account (customers that use the said services and have accounts with the bank are not included in the list);

9) reports provided by the bank's internal audit function during the inspection period;

10) managerial reports provided by the bank's responsible staff during the inspection period;

11) any other information and/or documents that the head/deputy head of the inspection team may deem necessary for the inspection.

Inspections should aim to assess banks' ability to manage risks to politically exposed persons using the banks for money laundering, including money that may have been earned via a corruption offence. Inspection should also aim to assess the actual effectiveness of the banks' system to manage risks related to politically exposed persons, including identifying, and decreasing to an acceptable level, the possibility that the banks' beneficiary owners, major shareholders or top managers use their position at the banks for money laundering, including money that may have been earned via a corruption offence.

14. Once the information and/or documents specified in paragraph 13, Section IV of this document have been received and processed, see if the bank has customers who meet the criteria set forth in Annex 2 to this document, and review customer files to check whether or not the bank complies with the relevant financial monitoring laws (in particular where they relate to know your customer and due diligence procedures). Customer files should contain, but are not limited to, know your customer and due diligence documents and documents showing a customer's sources of funds and that were provided by the customer to open an account/establish (maintain/extend) business relations, carry out a one-off financial transaction involving a large amount of money. These files should also contain, but are not limited to, documents showing sources of assets (in particular, wealth), expected

volumes of financial transactions via the account(s) opened at the bank (types and volumes of financial transactions), permission given by the bank's top manager to establish (maintain/extend) business relations, a questionnaire, and documents to conduct due diligence (if required).

15. Check if the financial transactions that were carried out by politically exposed persons and listed, as set forth in Section IV, paragraph 13 of this document, are in line with the politically exposed persons' financial standing and nature of business. Special attention should be paid to unusual or suspicious financial transactions, which may be a sign that the financial transaction, people involved in the transaction, activities of the people involved, or their sources of assets are related to money laundering.

16. Once the information and/or documents specified in paragraph 13, Section IV of this document have been received and processed, see if the bank has customers who meet the criteria set forth in Annex 3 to this document, and review customer files (taking into account any other information the inspection team may have) to check if the bank failed to classify some of its politically exposed customers as such.

The inspection team should scrutinize financial transactions that may entail a high money laundering risk (such as financial transactions involving cash, transfers to or from high-risk countries). These include countries (territories) that fail to comply (in full) with recommendations given by international or intergovernmental anti-money laundering and counter-terrorism financing organizations listed by Ukraine's Cabinet of Ministers; countries (territories) listed by Ukraine's Cabinet of Ministers as offshore areas; countries that meet the criteria set forth in subparagraph 39.2.1.2, subparagraph 39.2.1., paragraph 39.2, Article 39 of Ukraine's Tax Code, as set forth in Ministerial Decree No. 977-p of 16 February 2015.

17. Check if the financial transactions that were carried out by politically exposed persons and listed, as set forth in Section IV, paragraph 16 of this document, are in line with the politically exposed persons' financial standing and nature of business. Special attention should be paid to unusual or suspicious financial transactions, which may be a sign that the financial transaction, people involved in the transaction, activities of the people involved, or their sources of assets are related to money laundering.

18. Check whether or not customers, persons authorized to act on behalf or on the instructions of customers, as well as the managers and beneficiary owners (controllers) of corporate customers are included in the list of national politically exposed persons used by the National Bank of Ukraine and any other data bases (if available). If you find any persons or entities on this list, check if the bank correctly indicated the level of risk related to such customer(s), whether or not the bank has taken all the actions required by its internal documents and the relevant financial monitoring laws, as well as whether or not the actions taken are sufficient. The head or the deputy head of the inspection team decides on the number of customers to be

checked (taking into account the number of customers found on the list and any other available information).

19. If you identify unusual or suspicious financial transactions after taking the actions specified in Section IV, paragraphs 15, 17 and 18 of this document, discuss them with the bank's designated officer to check whether or not the officer identified these transactions when carrying out regular inspections, and whether or not they informed the designated authority of these transactions (as set forth in Resolution No. 417, paragraph 90). If the designated officer did not inform the designated authority, check whether or not the assessment carried out by the officer was sufficient.

20. On the basis of the findings made by the inspection team after carrying out the actions specified in Section IV of this document, decide whether or not the bank's management of risks to money-laundering and terrorism financing by politically exposed persons is adequate.

In order to analyze the bank's information systems, obtain the technical data and parameters (qualitative and quantitative) that are used to monitor financial transactions, and check whether or not the bank complies with financial monitoring laws where they relate to limiting risks to money laundering by politically exposed persons. Check whether the bank is able to identify financial transactions specified in Articles 15 and 16 of the AML/CTF Law and information that must be sent to the designated authority (mandatory financial monitoring) or may be sent to the designated authority (internal financial monitoring).

21. Obtain reports by Internal Audit Service of the bank written during the period of inspection, which include opinions and findings of the audits related to PEPs.

22. Analyze the reports by Internal Audit Service, focus on any issues related to PEPs mentioned there, and determine what appropriate measures were taken or are been implemented.

23. Determine whether the Internal Audit Service is able to ensure efficient AML/CTF compliance auditing (including sufficiency of the measures taken by the bank for managing the AML/CTF risks).

24. Check whether the external audit of the bank included issues related to PEPs. If yes, obtain the most recent external auditor report and review the scope of engagement, opinion and measures taken by the bank to eliminate the revealed violations.

25. On the basis of review of PEP customers' files determine whether the documents obtained for "know-you-customer" procedure are kept in accordance with the requirements specified in bank's internal regulations and the laws where

they relate to such data keeping.

## V. Documenting inspection results

26. Upon carrying out measures set forth in Section IV of these Guidelines, the following steps are to be undertaken.

27. Discuss the obtained results and opinions made at this stage of the inspection with a relevant bank official and draft a statement on inspection. If financial monitoring reveals signs of risky activities pertaining to PEPs, ask the bank official to provide evidence (based on a documented justification) that there are no signs of risky activities in the actions of a customer or a bank.

28. Initiate and submit necessary documents / information to designated employees/structural units of the NBU to adjust the risk profile, supervisory strategy and working papers. Such information/documents are meant to simplify future inspections and measures aimed at such a bank.

29. Based on the findings of the analysis of internal documents and measures undertaken by a bank regarding PEPs, the inspection team must assess the effectiveness of internal documents and the measures taken by the institution with due regard to existing accounts of PEPs that are opened with the bank, as well as the adequacy of the bank's measures aimed at reducing a risk of its services being used for money laundering purposes, including with funds obtained as a result of corruption.

30. The inspection group is required to assess the effectiveness of the bank's financial monitoring of financial transactions effected by PEPs, taking into consideration the volume of those transactions identified by the bank that are subject to financial monitoring (particularly, based on internal financial monitoring criteria), the value of assets, customer base of the institution, etc.

31. Upon the completion of inspection, the inspection team prepares an opinion on sufficiency/insufficiency of the measures implemented by the bank to prevent money laundering, including with the use of proceeds obtained as a result of corruption, particularly, regarding efficiency/inefficiency of the development and functioning of the interbank system to prevent money laundering, to ensure proper management of risks of the bank's services being used by PEPs for money laundering purposes, including those obtained as a result of committing corruption. The inspection findings shall be used to assess a risk management level at the bank with regard to the risk of the bank's services being used by PEPs for money laundering purposes (pursuant to Annex 4 to these Guidelines).

32. In the event of any deficiencies identified in the development and functioning of the intrabank system, recommendations have to be provided designed to enhance the efficiency of the risk management system. In case of violations of legal requirements on financial monitoring/bank's risky activities that threaten the interests of depositors or other creditors of the bank, particularly in case of the bank's failure to undertake sufficient measures for identification, verification and scrutiny of customers - PEPs, proposals are to be made regarding the consideration of a possibility to apply corrective measures to the bank.

Director, Financial  
Monitoring Department

Ihor Bereza

Annex 1  
to the Guidelines on carrying out inspections of banks, their separate units and foreign banks' branches to assess the sufficiency of measures taken with respect to the risks relating to PEPs.

The list of main responsibilities and tasks faced by banks concerning PEPs, as provided for by the legislation

1. The legislation on issues related to financial monitoring requires that banks shall undertake the following steps with regard to PEPs:

1) to set a high level of risk (taking into consideration the requirements of financial monitoring legislation, namely Article 6 of the AML/CTF Law);

2) to identify the fact of qualification of a customer (except for customers referred to in Regulation No. 417, Section V, paragraph 58) or a person acting on its behalf, on behalf of their ultimate beneficial owners (controllers), beneficiaries to PEPs, and whether they are ultimate beneficial owners (controllers) or heads of legal entities (Article 6 of the AML/CTF Law, Regulation No. 417, Section V, paragraph 47);

3) to carry out measures stipulated by Regulation No. 417, Section V, paragraph 64;

4) establish business contacts, enter into agreements, open accounts, conduct non-recurrent financial transactions for significant amounts with PEPs after authorization by the bank manager (Article 6 of the AML/CTF Law, Regulation No. 417, Section V, paragraph 48);

5) prior to or in the course of developing business relationship, it is necessary to undertake steps aimed at ascertaining the source of funds (before or during financial transactions - the sources of funds that are used in financial transactions) and assets, rights to such assets, such persons on the basis of documents received from them and/or information from other sources, if such information is public (open), confirming the sources of their assets, rights to such assets, etc. (Article 6 of the AML/CTF Law, Regulation No. 417, Section V, paragraph 48);

6) to conduct primary financial monitoring of financial transactions, the participants or beneficiaries of which are PEPs in the manner specified for high-risk

customers (Article 6 of the AML/CTF Law), with due regard for NBU recommendations;

Annex 2 Continuation of

7) to make verification at least once per year of information about the customer (Article 6 of the AML/CTF Law, Regulation No. 417, Section V, paragraph 62);

8) ensure identification, registration in the register of financial transactions and provision to a specially authorized body of information on financial transactions effected by PEPs that are subject to financial monitoring if the amount of a transaction conducted equals or exceeds the amount in foreign currency, investment metals and other assets equivalent to UAH 150,000 (Article 6 of the AML/CTF Law);

9) to carry out measures stipulated by Regulation No. 417, Section V, paragraph 60;

Annex 2 to the Guidelines on carrying out bank inspections, their separate units and foreign banks' branches to assess adequacy of measures taken with respect to risks relating to PEPs.

Terms of customer files sampling - PEPs customers  
(in terms of specific categories)<sup>1</sup>

1. For customers - natural persons: the total amount of balances on all the accounts of a customer as of the date of inspection equals or exceeds the equivalent<sup>2</sup> of USD 50,000 and/or the total amount of credit turnover on the customer's all accounts for a year preceding the date of inspection equals or exceeds the equivalent of USD 250,000.

2. For customers - legal entities: the total amount of balances on all the accounts of a customer as of the date of inspection equals or exceeds the equivalent of USD 250,000 and/or the total amount of credit turnover on the customer's all accounts for a (1) year preceding the date of inspection equals or exceeds the equivalent of USD 1 million.

<sup>1</sup> If deemed necessary, the audit leader/his deputy may form at their own discretion a sample that will include a list of customers with ratios lower than those specified in this Annex.

<sup>2</sup> The equivalent is calculated according to the official exchange rate of the NBU set on the date of inspection.



Annex 3 to the Guidelines on carrying out bank inspections, their separate units and foreign banks' branches to assess adequacy of measures taken with respect to risks relating to PEPs.

#### Terms of customer files sampling (except PEPs)

1. A sample must include customers (separately for natural persons and legal entities) with the maximum total credit turnover on all the accounts during a (1) year preceding the date of inspection. The audit leader/his deputy will determine a number of customers for sampling, taking into consideration the total number of the bank's customers (particularly PEPs), a list of products/services provided by the bank, other available information, etc.

Annex 4 to the Guidelines on carrying out bank inspections, their separate units and foreign banks' branches to assess adequacy of measures taken with respect to risks relating to PEPs.

The scale to assess a risk management level with regard to the risk of the bank's services being used by PEPs for money laundering purposes

<b>Risk management level:</b>	<b>Characteristics of risk management level with regard to the risk of the bank's services being used by PEPs for money laundering purposes</b>
<b>Insufficient</b>	The risk after reviewing the adequacy and/or efficiency of control mechanisms to reduce the risk remains high and much higher than the acceptable level. A dangerous situation that requires immediate and effective remedial actions to eliminate the most serious risks that could threaten the integrity of the process. It may be necessary to discharge a bank's official of the position and/or apply other measures
<b>Satisfactory</b>	The risk after reviewing the adequacy and / or efficiency of control mechanisms to reduce the risk remains high and higher than the acceptable level. The situation must be restored to an acceptable (adequate) level through the implementation of the recommended corrective actions. Enforcement measures are necessary.
<b>Acceptable</b>	The risk after reviewing the adequacy and / or efficiency of control mechanisms to reduce the risk is assessed at the medium level and is within acceptable level. The situation is generally adequately controlled; comments reflect minor flaws that can be corrected in the normal course of business activity. Enforcement measures are possible.
<b>Sufficient</b>	Good in all aspects: the right balance between risk and their coverage. Remarks highlight minor flaws or there are no remarks at all. Minor actions are required or there is no need of action at all. It is possible to apply enforcement measures in the form written warning, sending written demand, letter to the bank or apply no response measures.