AMENDMENT NUMBER 2

REQUEST FOR PROPOSALS FOR THE SUPPLY AND IMPLEMENTATION OF AN INTEGRATED SOFTWARE SOLUTION FOR ADVANCED DATA PROCESSING AND ANALYTICS, INTELLIGENT RISK PATTERNS IDENTIFICATION, INVESTIGATION AND CASE MANAGEMENT SYSTEM TO STRENGTHEN THE AML AND SHAREHOLDERS' MONITORING CAPABILITIES OF THE NATIONAL BANK OF MOLDOVA

Title:	**NBM SOFTWARE SOLUTION**
RFP Number:	**FSTA-2020-01**
Procurement Method:	**International Full and Open Competition**
Contracting Entity:	**International Development Group Advisory Services, LLC** 1100 North Glebe Road, Suite 950, Arlington, Virginia, 22201
Funded By:	**United States Agency for International Development (USAID)**

CONTENTS

List of terms and abbreviations

AML/CFT	Anti money laundering /counter financing of terrorism
Beneficiary	National Bank of Moldova
BRR	Bank Risk Rating
CRMS	Central Risk Monitoring System
CRR	Credit Risk Register
CSD	Central Securities Depository
ETL	Extract Transform Load
FIU	Financial Intelligence Unit
FSTA	USAID Moldova Financial Sector Transparency Activity
IDG	International Development Group Advisory Services, LLC
HW	Hardware
IMF	International Monetary Fund
KPI	Key performance indicator
KYC	Know your customer
MDL	Moldovan leu (local currency in Moldova)
ML/TF	Money laundering/terrorism financing
NBM	National Bank of Moldova
NBM Software Solution	Integrated software solution for advanced data processing and analytics, intelligent risk patterns identification, investigation and case management system to strengthen the AML and Shareholders' Monitoring capabilities of the NBM
PEP	Politically exposed person
RFP	Request for proposal
SAR	Suspicious activity report
STR	Suspicious transactions report
UBO	An individual who ultimately holds or controls either the proposed acquirer or the shareholder who directly or indirectly owns a holding in the bank's share capital
USAID	United States Agency for International Development

Section 1. IDG Background and Information Sheet

Issue Date	April 27, 2020
Questions Due	May 21, 2020
Closing Date	June 24, 2020

International Development Group Advisory Services, LLC (International Development Group LLC or IDG), is soliciting proposals from qualified organizations interested in providing a software solution to monitor the National Bank of Moldova's shareholder's transparency and offsite analysis of anti-money laundering and countering financing of terrorism (AML/CFT), associated implementation services and warranty services (maintenance and support services). IDG is a U.S. consulting firm located in the Washington D.C. area. As the implementer of the USAID Moldova Financial Sector Transparency Activity (FSTA), IDG has been contracted by the United States Agency for International Development (USAID) to procure the software solution for the National Bank of Moldova.

This procurement will require a formal technical and cost proposal submission as outlined by the Request for Proposals (RFP). This procurement will be conducted as a full and open competition process under which any type of organization is eligible to compete.

The awarded contract will be a firm fixed price contract type and the estimated period of performance will be July 2020 through July 2021. The USAID principal geographic code for this contract is 110 and 937. The place of performance is Moldova and the successful bidder's headquarters location.

Any questions regarding this RFP should be submitted no later than 5:00 PM Eastern Standard Time (EST) on May 21, 2020. These submissions should be made by email address to procurement@internationaldevelopmentgroup.com. In the subject line reference: **Questions – NBM Software Solution.**

RFP proposals must be submitted no later than 5:00 PM EDT on June 24, 2020. These submissions must be made by email address to procurement@internationaldevelopmentgroup.com. In the subject line, please reference: **RFP – NBM Software Solution.**

Bidders must submit both Technical Proposals and Financial Proposals electronically. The proposals must be submitted in separate emails. Proposals must be submitted in English and must remain valid 120 days after the submission date.

IDG's technical representative is Mr. Matthew Macellaro and IDG's contractual representative is Ms. Jessica Tolliver.

Issuance of this solicitation and the submittal of a proposal do not constitute a commitment on the part of IDG to make an award; neither does it constitute an obligation for any costs incurred in the preparation and submission of a proposal.

After reviewing all questions, a virtual bidder's conference might be scheduled to answer these questions and further discuss the requirements of the National Bank of Moldova. The Bidder's conference is tentatively scheduled for May 28, 2020.

Section 2. NBM Background information

1. General information about NBM

1.1. The National Bank of Moldova (NBM) is the central bank of the Republic of Moldova. The activity of the NBM is regulated by Law no. 548-XIII on the NBM, adopted by the Parliament of the Republic of Moldova on July 21, 1995. In accordance with the above-mentioned law, NBM is an autonomous public legal entity and is responsible to the Parliament.

1.2. As a central bank, the NBM performs various activities similar to most other central banks. These activities include, but are not limited to, the following:

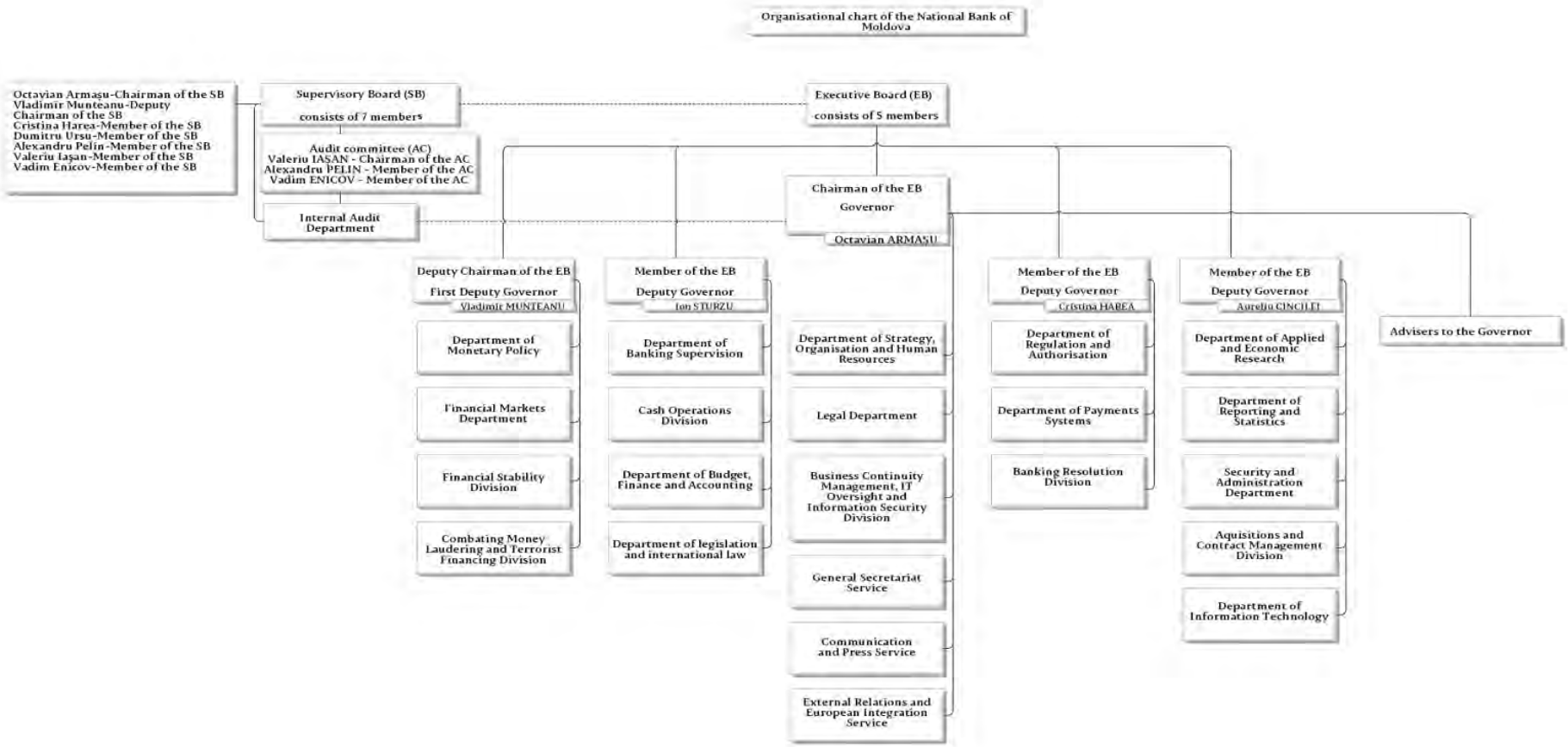
a. To establish and implement the state monetary and foreign exchange policy.
b. To act as banker and agent of the state;
c. To license, supervise and regulate the activities of the financial institutions and branches of foreign banks;
d. To establish, license, operate, regulate and supervise the financial market infrastructure, promote its stable and efficient functioning, act as the sole issuer of the national currency;
e. To regulate and supervise the AML/CFT activities of financial institutions;
f. To establish the exchange rate regime of the national currency and to hold and manage foreign exchange reserves of the state;
g. To provide credit to banks, as a lender of last resort;
h. To prepare the balance of payments of the state, the international investment position and the statistics of the external debt of the Republic of Moldova;
i. To perform foreign exchange regulation on the territory of the Republic of Moldova; and,
j. To license, regulate and supervise the activity of providing payment services and the issuance of electronic currency.

1.3. NBM is located at 1 Grigore Vieru Avenue, in Chisinau, Republic of Moldova.

1.4. The organizational structure of the NBM is presented in *Figure 1*.

1.5. A working group at NBM was established to oversee and monitor the implementation of the Software Solution. The working group consist of representatives from several subdivisions including: Banking Supervision Department, Anti-Money Laundering and Terrorist Financing Division, Payment System Department, Financial Market Department, Department of Information Technologies, Regulation and Authorization Department, Reporting and Statistics Department, Business continuity, management, information security and IT supervision Division and the Department of Strategy, Organization and Human Resources.

Figure 1: NBM's organizational chart



2. Project Description Overview

2.1. To meet international standards and practices, the NBM, as the supervisory authority, aims to promote a strong and competitive financial system with low risk. The Moldovan banking sector is subject to a wide range of risks including credit, operational, transparency risk, and most especially AML/CFT risks. Accordingly, to maintain financial stability throughout the banking sector and at each individual licensed bank, continuous monitoring by the NBM is required.

2.2. In order to significantly improve the risk monitoring capabilities, the NBM developed the Central Risk Monitoring System (CRMS), aimed to ensure early identification of risks and potential frauds that might become or lead to significant losses for banks. This platform helps ensure that the corrective actions, undertaken by the NBM, are based on a process of analytical and interpretative investigation using a variety of procedures and techniques. However, given the peculiarities of the banking sector of the Republic of Moldova, the NBM needs a Software Solution to monitor the shareholders' transparency and ML/TF risks on a continual basis.

2.3. The Software Solution will enable NBM to continuously assess and monitor the banks' shareholders at the system and group level both on-site and off-site. This in turn will create opportunities for optimizing and strengthening prudential regulation of banks in the macro-prudential supervision framework for shareholders' transparency and related party activity of banks. It will also help to reduce time pressure on licensed banks during on-site inspections, by reducing the amount of information required, by using data from the information systems of the NBM.

2.4. One of most important objectives of the Software Solution is to assist in the full implementation of a risk-based approach in the supervision process.

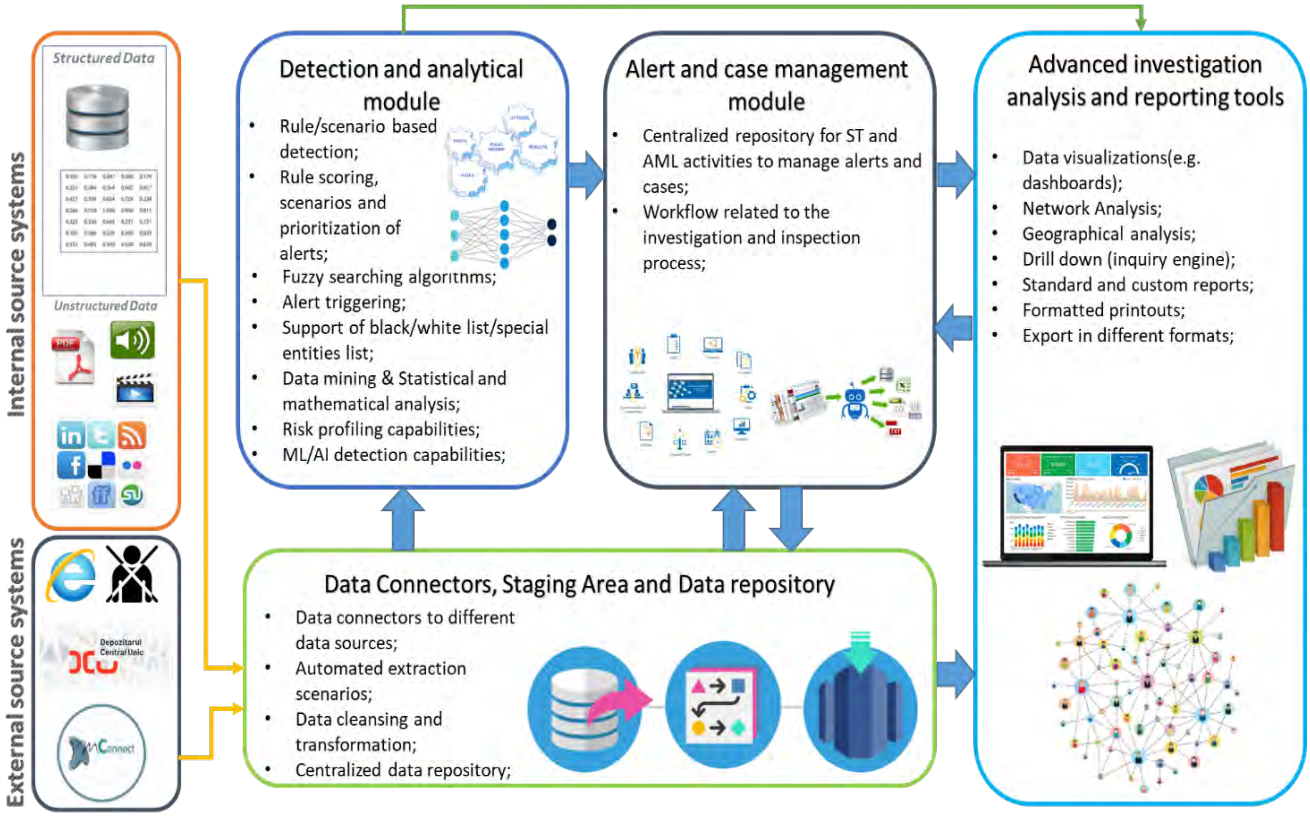
2.5. The Software Solution procured and implemented for this project should represent a system to readily monitor and process information and data on direct and indirect holders of shares. As this information and data relates to the banks' capital, their ultimate beneficiary owners (UBO) and the transactions of these shareholders, individuals and legal entities that are related as well as possible AML/CFT suspicious transactions for any of the parties mentioned above. *Figure 2* shows the conceptual representation of the Software Solution.

2.6. The procurement and implementation of the Software Solution will improve the efficiency of the monitoring process of shareholders' transparency and AML/CFT risks ensuring achievement of at least the following outcomes and objectives:

a. Register and process information and data on direct and indirect holders of shares in the capital of banks and UBOs of such shareholders and determine the concerted activity of shareholders;
b. Monitor transactions for the purpose of shareholders' transparency, including identifying any changes in the ownership structure of banks, identifying affiliated persons and undeclared groups and AML/CFT associated risks;
c. Identify any interconnections between shareholders, administrators, debtors, and clients of banks and determine the suitability and integrity of shareholders and administrators of banks;
d. Allow prompt verification of any suspicions related to direct and indirect holders, beneficiary owners of shareholdings in the capital of banks or ML/TF transactions;

e. Provide the possibility to create an overall clear and accurate image of the risks related to ownership structure of banks and ML/TF;
f. Ensure digitalization and transformation of the information handled within these processes, so that to maximize its value in decision-making processes;
g. Provide NBM users with a modern, transparent, efficient, flexible, measurable, maintainable and lasting instrument intended to facilitate the accomplishment of main tasks by increasing the level of process automation;
h. Increase the capacities of re-using the information in the context of other processes inter-correlated with those in the project;
i. Align to the best practices in the management of monitoring processes of shareholders' transparency and ML/TF risks;
j. Provide the possibility to promptly identify the transactions or activities of the banks and their customers that pose a high risk of ML/TF;
k. Identify and assess the ML/TF risks, including high risky transactions with non-transparent jurisdictions etc.; and
l. Monitor the payments flow both for local and international cash transactions and identify suspicious patterns, trends and typologies.

Figure 2: Conceptual representation of the software solution



2.7. It is very important to note that NBM does not intend to overlap with (i) transaction monitoring rules applied by each bank in the Moldovan market; or, (ii) the authority and responsibility of the

Office for the Prevention and Fighting against Money Laundering--the Republic of Moldova's Financial Intelligence Unit (FIU) which analyzes suspicious transaction reports (STRs) and suspicious activity reports (SARs) received from the range of obliged entities including financial institutions. Individual banks in the Moldovan market monitor the activities of their clients and report SARs/STRs directly to the Moldovan FIU.

2.8. It should be highlighted that the Software Solution sought by the NBM is substantially different from the operations of AML software used at commercial banks that primarily focus on single (customers') transactions in order to stop such transactions and perform subsequent investigations of related clients or transaction parties. The Software Solution for the NBM should focus on the whole chain of transactions conducted in the banking sector as well as the actions of individuals using more advanced AML/CFT schemes involving transactions at a number of banks that may not be suspicious when reviewed independently. At the same time, the Software Solution should identify patterns and typologies of transactions derived from the relation between commercial banks and their customers that pose a high risk of ML/TF.

2.9. In line with this concept, NBM is considering implementing a solution that could offer the most optimal and efficient way to achieve its objectives. Thus, considering the existence of classical solutions based on pre-established analysis rules and scenarios on the one hand and the new technological trends related to Machine Learning / Artificial Intelligence on the other hand, NBM needs alternative solutions that would achieve the project objectives in a more efficient way. For this case, when filling the answers to the tender requirements, the Bidder should indicate for each individual requirement the proposed alternative solution that would cover NBM's needs and the project scope.

Section 3. Business Units' descriptions and activities

1. Business architecture

The following section provides background information including the responsibilities and processes of the two main users: the Shareholder Transparency Unit (Unit) and AML/CFT Division (Division), to be supported by the Software Solution.

2. Introduction of the Shareholder Transparency Unit

2.1. Transparency of the commercial banks' shareholder structure is crucial to ensure the stability of the Moldovan banking sector. Historically, this was one of the key weaknesses undermining risk management and corporate governance within banks and was one of the main factors leading to the bankruptcy of three banks in 2015.

2.2. The Shareholder Transparency Unit of the NBM was established to ensure sound and prudent management of the banks' shareholders' transparency. This Unit is part of Off-site Supervision and Shareholders Monitoring Division within Banking Supervision Department.

2.3. From its establishment to the present, the Unit has been focused on retrospective analysis of current shareholders of Moldovan banks. The Unit ensures that all non-transparent shareholders are removed from the market as soon as possible. Once the planned review of all shareholders above one percent (1%) of ownership is finished, the Unit should be able to act proactively, rather than reactively, to identify any suspicious shareholders that might appear.

2.4. As such, the main responsibility of the Unit is to monitor banks' shareholders by analyzing reports and information regarding shareholders, UBOs and groups of shareholders acting in concert with a commercial bank. In case of misreporting, suspicious behavior of shareholders, non-disclosures of a true UBO or groups acting in concert, or any other breach of law, the Unit informs NBM's Board about the necessary legal actions to ensure a high level of transparency of the bank structure. To achieve this, the Unit analyses reports submitted by banks, information submitted by shareholders, information from other state institutions and any other relevant information. Currently, most of its investigations focus on indications that two or more shareholders of the same bank may be acting in concert without the permission of the NBM and acting in a way that represents a potential breach of legislation.

2.5. The Unit has broad ranging legal powers to perform its activities and to take specific actions against non-transparent shareholders. The Software Solution is expected to facilitate and enhance these efforts. The Software Solution, to the extent possible, should indicate the difference between a suspicious transaction and one that is supported by reliable evidence.

2.6. Process overview

2.6.1. The following section describes the main processes of the Unit to be supported by the Software Solution. It also includes the reporting requirements of the Unit and details about the information flow between various units within the NBM.

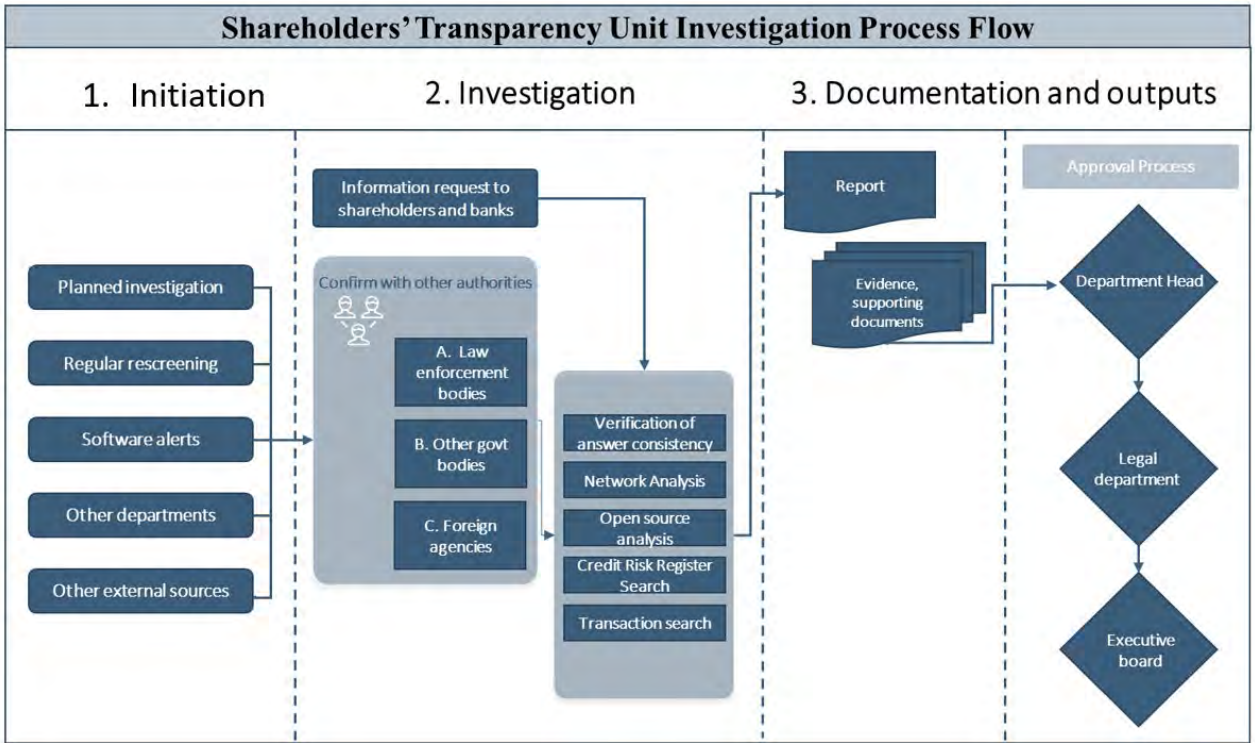
2.6.2. The Unit currently holds information in paper form (electronic reports began in the year 2000 and have less information than on paper) about all existing or historical shareholders.

It also holds has information, to a lesser extent, about shareholders not (or not yet) approved by the Regulation and Authorization Department. This information/data is used to initiate the investigative process.

2.6.3. It is expected that reliable and up-to-date information about all recent shareholders will come from other sources, including Central Securities Depository (CSD) and Licensing Authorizing and Notification systems.

2.6.4. *Figure 3* represents a high-level overview of the investigation process of the Unit. It consists of three main logical components, (1) initiating the investigation, (2) the investigation itself and (3) documentation of the findings. Each part of the process is described in more details in the following paragraphs, with examples of the main tasks.

Figure 3: Shareholder Transparency Unit – investigation process flow



2.7. Initiation of investigation

2.7.1. The investigation process (review process) can be initiated in a number of ways. Most of the reviews are currently being initiated by a yearly plan of activities of the Unit or by planned on-site inspections of the banks.

2.7.2. Except for the yearly plan, an investigation may be launched on an ad-hoc basis for both existing shareholders and/or proposed acquirers. The triggers vary and can be divided into internal and external based on the source of the information. The major triggers are described in more detail below.

Yearly plan of investigations

2.7.3. Currently, the NBM reviews the shareholders of all banks according to an agreed yearly plan. The current review is performed for all shareholders who hold more than one percent (1%) of shares and those under one percent (1%) where there are doubts. Future plans include investigation of all shareholders who hold less than one percent (1%) of shares of banks as well. The regular re-screening of previously reviewed shareholders is also part of the yearly plan.

2.7.4. Other internal triggers:

a. Licensing may request further information about proposed acquirers.
b. On-site Supervision Division (On-Site) identifies the relevant information about shareholders or bank related parties during the inspections.
c. The AML/CFT Division may also request further information about certain shareholders or may provide valuable information based on their analyses.

2.7.5. External triggers:

a. Adverse news related to a shareholder or a Moldovan bank that was found in local or international media or on social media.
b. Whistle-blowers and letters from other authorities (i.e. Ministry of Finance, FIU) are another important source of information on which an investigation may be initiated.
c. Regular review analysis of sanctions and blacklists may be a trigger as well.

Software Solution requirements for initiation of investigation[1]

2.7.6. The Software Solution should facilitate all methods for initiating an investigation:

a. Open cases based on the yearly plan;
b. Scheduling a re-screening of shareholders after a certain period of time;
c. Support user case creation to address ad-hoc requests and information obtained from internal and external sources – this can be done for both existing shareholders approved by the Regulation and Authorization Department and proposed acquirers that will be imported from different data sources.

2.7.7. Additionally, one of the main objectives of the Software Solution is an automated alert triggering (should be able to limit false positives) based on the number of rules. The rules should be customized and differ for individuals and entities. The following are examples of internal triggers (this list is not exhaustive);

a. Identifying new shareholder(s);
b. Buying /registering shares in the same hour/day or near period of time in the same bank;
c. Buying a similar number of shares, usually under the amount, for qualifying holding;
d. Using the same financial source to buy shares;
e. Using the same broker/intermediary to buy shares;
f. Directing of dividends to the same person or group of persons;
g. Using their voting rights, the same way; and

[1] For a more detailed description, please refer to the functional requirements.

h. Having the same legal representative etc.

2.7.8. It is assumed that the number of planned investigations will decrease after the Software Solution is adopted and more reviews will be initiated automatically. The Software Solution should support automatic case allocation that is flexible based on the number of rules set by the NBM.

2.8. Analysis

2.8.1. Once there is a trigger alert and the case is open, the Unit starts the analysis process. While performing the review, the examiners follow an established set of steps.

Information requests

2.8.2. The investigation process starts with a request for information from shareholders and/or a bank. This is done by sending a physical letter to a shareholder and/or its representatives with a predefined list of questions. Some answers can be entered into an electronic form (i.e. structured format) but other portions of the requested information are in the form of various documents (e.g. official confirmations) which must be attached as word/scanned documents (i.e. unstructured format).

2.8.3. Shareholders are obliged by law to disclose the requested information. If the answers are not provided, the NBM may impose penalties.

2.8.4. At the same time, a physical letter request for information is sent to other governmental bodies and law enforcement authorities. Members of the Unit also perform searches within publicly available sources or paid databases to collect relevant supporting documentation needed for the analysis.

2.8.5. Software Solution requirements for case management information gathering include:

a. Contain all information and details about the case require.
b. Process and display information on the shareholder available in Licensing Authorizing and Notification and CSD systems.
c. Allow for attachments from users.
d. Support the functionality of case creation by users for existing shareholders within the databases; and, for potential shareholders that do not exist in any databases yet.
e. Support the full text indexing of attached documents in order to be able to search through the data repository.

Analysis

2.8.6. Once answers are received from the bank and shareholder (or governmental bodies), the analytical work starts. This usually covers, among others, the following actions:

a. Verify/Validate of the consistency of answers provided by the shareholder by comparing them with information obtained from other sources;
b. Perform network analysis of the shareholder to understand their links to other shareholders, companies and individuals. This includes ownership of companies, employment links or membership in statutory bodies of companies, present on a sanction or other list, payment links, physical movements through borders,

representation by the same person in a shareholder meeting etc. The network analysis is usually expanded to additional levels to see links to other people or entities and includes historical information if available;

c. Identify possible hidden connections between shareholders who might be acting in concert without declaring it;
d. Search against commercial registers, sanction/blacklists, Credit Risk Register (CRR), CSD, payment data, open source data, Land Register, tax reports as available; and,
e. Search for other previous involvement in investigations/penalties.

2.8.7. If needed, ad-hoc on-site visits to the bank with detailed inspections can be performed.

Software Solution requirements for analysis

2.8.8. The analytical functionality of the Software Solution should be able to automate a number of the steps in an investigation, for instance:

a. Allow creation of flexible workflows in order to cover all existing and possible new steps of investigation;
b. Support network analysis[2] based on internal and external information, finding hidden connections including manual tasks;
c. Search the population of international and domestic payments for information related to the shareholder or affiliated persons;
d. Search the CRR and CSD data for information related to the shareholder or affiliated persons;
e. Search historical cases – if the shareholder or any of the affiliated parties are the subject of an investigation to determine if there were any penalties imposed etc.;
f. Search for information existing in different the databases, i.e. commercial registers, sanctions and blacklists etc.;
g. Each step of the workflow should have an "upload attachment" functionality as well as a free text box for writing summaries and notes;
h. Each step/part of the workflow should be automatically included in the final report; and;
i. Allow for merging cases (multiple alerts for one (1) shareholder could merged into one (1) case, or cases for different shareholders merged into one (1) or related cases).

2.9. Documentation and approval process

Documentation and storage

2.9.1. Once the analysis is finished, the Unit is required to prepare a report with all findings. The report is currently written manually and contains a description of all the relevant information identified during the investigation. The document does not contain the supporting source evidence collected such as print screens, original mail letters, information provided by other authorities etc. The evidence is scanned and stored in separate files on a shared drive.

[2] Network analysis can be regarded as a set of techniques with a shared methodological perspective, which allow researchers to depict relations among actors and to analyze the social structures that emerge from the recurrence of these relations.

Approval process

2.9.2. The final report is reviewed and approved by the head of the Unit, head of division and head of the department and sent to the Legal Department for further review. The Legal Department provides their comments and indicates if any additional evidence or documentation is needed. Once these deficiencies are addressed, the report is sent to the Executive Board of the NBM for approval and final decision about potential sanctions and penalties.

2.9.3. Shareholders have and often use the right to appeal an NBM decision. During court hearings, the NBM uses all evidence and documentation prepared during the investigation.

2.9.4. The documentation phase of investigations is extremely important but time consuming. Therefore, it is expected that the Software Solution will support this part of the process by:

a. Facilitate the preparation of a report – e.g. populate information from analytical parts to a predefined template;
b. Store the supporting evidence related to the case and allow for the creation of a package which could be used in a court proceeding;
c. Define, if possible, various user roles with different access rights: e.g. searching, analysis, approval and access to users from other units;
d. Provide full audit trail functionality.

2.10. Cooperation with other departments

2.10.1. The Unit has on-going cooperation with other units within the Banking Supervision Department and other units of the NBM.

2.10.2. Cooperation with the Licensing Department goes both ways. During the acceptance process of new shareholder, the Licensing Department may request support from the Unit in order to obtain further information about the potentially suspicious shareholder. At the same time, the Unit requests data from the Licensing Department or AML/CFT Division during their own investigation. They have access to historical data and the shareholder's on boarding documentation.

2.10.3. The Unit is also involved in on-site inspections of the banks. The Unit members can participate in planned on-site reviews with the On-site Supervision Division to verify a bank's compliance with regulations regarding its shareholders or initiate their own on-site review for the purposes of an investigation. Information obtained on a specific shareholder and links with other companies can be used by On-site Supervision Division in a bank's related parties lending review.

2.10.4. In addition, the Unit might request additional information from various departments of NBM. For instance, from the Department of Payment systems, Cash Operations Division or Department of Reporting and Statistics etc.

2.11. Metrics and Reporting

2.11.1. The Unit reports statistical information about its performance and results of investigations. Therefore, the Software Solution should be able to facilitate this type of information (including the ability to create customized reports) to provide an effective statistical overview, approximately 30 to 50 reports. The areas of coverage should include but not be limited to:

a. Statistical overview of open alerts/cases/investigations, i.e. current work in progress;
b. Statistical overview of investigations conducted, closed cases, triggered alerts, i.e. overall performance of the Unit;
c. Comparison to yearly KPIs;
d. Duration of different stages of investigation (per phase, per employee, per bank etc.); and,
e. Management dashboard focusing on information about banks – both current state and historical views:

i. Number of shareholders per bank;
ii. Number of transparent and non-transparent shareholders;
iii. Percentage of non-transparent shareholders per bank;
iv. Number of cases;
v. Results of investigations;
vi. Shareholders' transparency risk rating of the bank (please see the detailed description below);
vii. Statistical information on jurisdiction of shareholder; and,
viii. Other data and ad-hoc reports as required.

2.12. Shareholders transparency Bank Risk Rating (BRR)

2.12.1. For the successful monitoring and reviewing of shareholders and banks, the NBM developed a risk rating methodology. The Unit in planning and various other stages of the investigation as well as for the general score of the bank in the Supervisory Review and Evaluation Process risk rating use this score, which is a component of the BRR.

2.12.2. The BRR is also one of the factors affecting the scoring of the alerts and their triggering. It should also be considered during the prioritization of case allocation, part of the final decision of a specific shareholder's transparency etc. While most factors contributing to the risk rating are quantitative, others are qualitative, for instance a bank's reputation. This makes it necessary to set weights for each factor. The Software Solution should have several methods for the identification of risk ratings, at the shareholder and bank level, automatically calculated and user defined.

2.12.3. The following factors can be used as core risk factors for the purposes of BRR. The list, which is not exhaustive, represents some examples and is enhanced by the NBM's knowledge of the banking sector:

a. Jurisdiction of shareholders/beneficial owners;
b. Number of shareholders holding less than 1% of shares and the shares owned;
c. Jurisdiction of the parent company;

d. Total number of shareholders and the shares owned;
e. Frequency of changes in the structure of the shareholders;
f. Frequency of participation in Shareholders' Meetings;
g. Number of shareholders represented by proxy at shareholders Meetings;
h. Approval or disapproval by the NBM of Board members submitted by shareholder;
i. Beneficial owners of shareholders;
j. Exposure of bank to shareholders' loans issued to shareholders or their affiliates;
k. The situation where shareholders / UBO were given sanctions or sanctioning measures by the NBM. The manner of interaction with NBM (the shareholders present the complete / incomplete information or the delay, the shareholder is not cooperative and transparent in the relationship with the NBM);
l. Information on the financial soundness of shareholders / beneficial owners; and,
m. Information on the integrity and reputation of the shareholders / beneficial owners.

3. Introduction of the AML/CFT Division

3.1. Increasing the intensity of AML/CFT supervision of banks is one of the key objectives of NBM. Implementing MoneyVal and International Monetary Fund (IMF) recommendations will contribute to better enforcement of regulations in this area and in the enhancement of overall corporate governance of the Moldovan banking sector.

3.2. The AML/CFT unit was established within the NBM ten years ago to manage the risk of ML/TF not just related to a particular bank but instead to the whole Moldovan banking sector. Starting February 2017, a new structure of the NBM was approved and the AML/CFT Unit was transformed into a separate Division having the responsibility to monitor the banking sector (and other entities supervised by the NBM). The Division's aim is to perform the necessary activities in order to ensure an efficient AML/CFT system in the banks and other institutions (payment system providers and FX offices) supervised by NBM. The Division has the following major objectives:

a. oversee the AML/CFT systems in banks and other supervised institutions to ensure use in the supervised institutions and to ensure they are not engaging in illicit/criminal activities;
b. facilitate national and international cooperation in the field in order to foster development of an effective AML/CFT system; and
c. Identify and assess identification and assessment of ML/TF risks, as well as, the development of proper tools in order to minimize the identified risks. A specialized software solution is expected to be implemented to facilitate these efforts.

3.3. The Software Solution will provide the NBM with information and updates on bank clients or each bank separately which may be suspected of involvement in ML/TF transactions and operations. Thus, in order to increase the efficiency of the solution, the following criteria must be followed:

a. Using flexible tools and techniques while applying necessary verifications;
b. Allowing the NBM to follow all the necessary procedures to identify the client and monitor its transactions; and,
c. Applying intelligent methods of risk identification and monitoring of banks' activity.

3.4. The implementation of the Software Solution will enable broad application of the risk-based approach to supervision. It will allow the use of early information related to potential risks and

will provide the supervisor the capability to perform quicker assessments of the need for targeted inspections, and effective allocation of the resources.

3.5. Afterwards, it will create a favorable context for further improvement of compliance by the banking sector with the required standards and will increase the accountability of decision makers on the needs of investors.

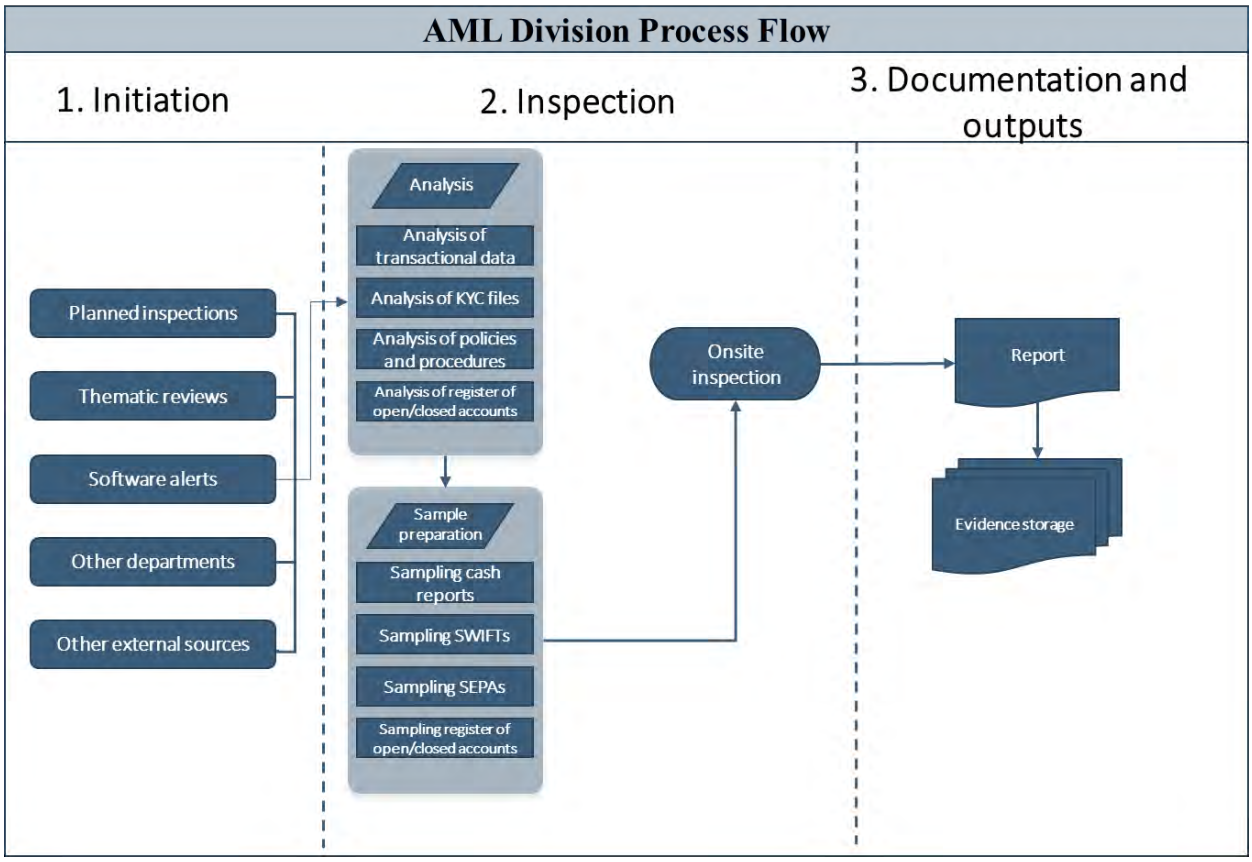
3.6. The Software Solution will be used by the Division to monitor domestic and international transactions with the aim of identifying structural money laundering and terrorism financing risks for the Moldovan banking sector. The Division expects that the Software Solution will support their activity of identifying ML/TF risks.

3.7. The Division will be able to investigate a limited number of alerts. It is expected that tens of alerts will be investigated annually. Therefore, the software solution should have advanced functional capabilities and a library of detection rules in order to limit the number of false-positive alerts.

3.8. The results of investigations and analysis conducted off-site usually become a source of information for regular or thematic/targeted on-site inspections of the banks in question. The Software Solution should have the ability to document the off-site investigation materials and incorporate and structure the findings and documents prepared during on-site inspections.

3.9. Process overview

Figure 4: AML/CFT Division Process



3.9.1. The following section describes the main processes of the AML/CFT Division, which should be supported by the Software Solution. It also includes the reporting needs of the AML/CFT Division. Every part of the described process contains a sub-section with the samples of the requirements for the software solution. This is included in order to provide further details about the relations between process needs and the functional requirements which are described in detail in *Section 4.* Solution and services requirements

3.9.2. The process, represented in *Figure 4*, is divided into the tasks that are performed off-site (i.e. the team performs analysis, investigations and preparation work using the data and information available in the NBM) and on-site when members of the AML/CFT Division visit the particular bank and perform deeper investigation steps. The process consists of three main components, (1) initiating the investigation, (2) the investigation itself and (3) documentation of the findings.

3.9. Initiation of inspection

3.10.1. There are two different ways of initiating an inspection within a bank:

a. Planned complex inspections based on the annual approved Inspection Plan; and,
b. Ad-hoc thematic (targeted) reviews focusing on specific severe issues identified during initiation and preparation phases or at another authority's request.

3.10.2. The thematic reviews are currently triggered by important information coming from:

a. Findings from planned inspections at other banks or results of previous inspections;
b. Off-site analysis of payment data (cash, local and international);
c. Other departments as a result of their reviews and investigations (e.g. Banking Supervision Department);
d. Adverse media; and
e. Other domestic and international authorities' requests and information.

Software requirements for initiation of inspection

3.10.3. Increasing the number of thematic inspections as well as a more transparent and clear mechanism for initiating such reviews were identified in the MoneyVal and IMF reports as needed areas for improvement. It is expected that the Software Solution will enable the Division to have an automated detection and alert mechanism which will monitor both individual banks as well as the banking financial sector as a whole. The Software Solution should provide the NBM with an automated indication (trigger alert) of trends: fluctuations in money flow, chains of suspicious transactions on the market, identified patterns and typologies, unusual customer's transactions or increased activity of customers presented on blacklists or sanction lists[3].

3.10.4. Some examples of detection rules can be the following:

a. Significant inflow/outflow of foreign currency in/from the Moldovan banking sector within a short period of time;
b. Trend in increasing transactional activity with high-risk jurisdictions;

[3] It is not required to stop the transactions, but only trigger the alert in case of increase of described activity

c. Rapid movement of funds in a local/foreign currency between local banks;
d. Significant inflow/outflow of cash occurring in a bank/banks without any clear business rationale;
e. Transactions in foreign currency with "banks" from Transnistria;
f. Significant transaction in local currency (MDL) performed with Clearing and Settlement house in Tiraspol;
g. Systematic split of the transactions below reporting limit (200 thousand MDL in cash and 500 thousand MDL for wire transfers) on same day, consecutive or close days;
h. Identification of transactions performed with persons (partners) from blacklists;
i. Identification of significant transactions performed with high risk customers (PEP, non-residents etc.);
j. Increased number of transactions with sanctioned/blacklisted or high-risk countries;
k. Transactions involving individuals or entities on the UNSCR 1373 list; and,
l. Any transactions involving an identified state sponsor of terrorism.

3.10.5. The above rules should trigger an alert. These alerts can vary in time and frequency as set by the user. It is not required that the monitoring of transactions and other sources run online (or real time). The aim of the monitoring is not to stop transactions but to draw attention to certain patterns, trends, typologies and risks and prepare supporting evidence for thematic or planned on-site inspection.

3.10.6. The solution also supports other ways to initiate inspections:

a. Scheduler for planned inspections;
b. User case[4] creation capabilities.

3.10. Inspection

3.11.1. Each inspection consists of two main parts: preparation (prep) work and actual on-site inspection.

Preparation phase

3.11.2. The prep phase is done off-site and includes a number of analytical tasks prior to the on-site inspection. This usually involves the following actions:

a. Analysis of international payments (SWIFT messages), domestic payments, cash reports, reports on the purchase and sale operations of foreign currency performed by licensed banks;
b. Analysis of the register of open and closed accounts, including correspondent accounts;
c. Search of high-risk customers within commercial registers, sanction/blacklists, PEPs list, CRR etc.;
d. Analysis of bank's activity with high risk countries or customers;
e. Performing network analysis for identified suspicious transactions/clients;
f. Negative media search;
g. The analysis of previous inspections, findings and potential penalties imposed;
h. Other information from competent authorities.

[4] The case represents the whole process of the inspection of a bank in the software solution.

3.11.3. During the preparation phase, the Division creates a list of requested items which are sent to the bank under review in order to receive additional documentation during on-site inspections. The areas of interest are large-scale transactions (including cash, blacklisted entities/countries/individuals), PEPs transactions or other high-risk clients' transactions, significant outflows of foreign currency outside of Moldova, compliance with the normative acts in the field, development of the internal control system etc.

Software requirements for preparation phase of the inspection

3.11.4. The software solution should support analytical steps related to a review of any alert triggered by the Software Solution. At the same time, it should support the entire prep phase of the inspection including the following:

a. Allow sampling, sorting, ordering, searching in various fields and filtering within the population of transactions and other sources of information (registry of accounts);
b. Support network analysis based on internal and external information, finding hidden connections, inserting manual parts;
c. Search within CRR data for information related to the banks and their customers;
d. Search within the documentation of previously performed inspections (i.e. the inspections which will be documented in the software solution once implemented);
e. Search within the database of commercial registers, Wisconsin risk report, sanction lists and blacklists;
f. Search within the database of high-risk countries or customers;
g. Allow creation of flexible workflow in order to cover all existing and possible new steps of analysis;
h. Each step of the workflow should have the "upload attachment" functionality, as well as a free text box for writing summaries and notes;
i. Allow merging of cases (multiple alerts created for one bank could be merged into 1 case);
j. Allow merging of multiple records of different alias for a client; and
k. Allow merging of multiple clients into one case.

3.11. On-site inspection

3.12.1. The on-site inspection focuses on a number of predefined topics, where the practical aspects of different AML/CTF areas of the bank are tested, for instance:

a. Review of the detailed documentation prepared for the sample of transactions and customers;
b. Assess internal AML/CFT Risk Assessment Report and of existing policies and procedures for Know Your Customer (KYC) and their alignment with current regulations;
c. Assess the internal control system in the field;
d. Review the Enhanced Due Diligence rules and practical applications;
e. Assess the process of identification of Ultimate Beneficial Ownership of customers;
f. Evaluate transaction monitoring policies and procedures existing in the bank, testing results of the transaction monitoring activities conducted at the bank etc.

3.12.2. Every step of the on-site inspection is documented and supporting evidence is gathered by the examiner.

Software requirements for on-site inspection

3.12.3. During the on-site inspection, members of the Division should be equipped with the findings of the initiation and preparation phase. Based on the detailed information from the reviewed bank, it is expected to perform additional analytical and documentation steps similar to those described in the preparation phase (the analysis of additional documentation held by banks related to the activity and transactions performed by customers).

3.12.4. On top of this, the Software Solution should provide a checkbox for each step of the investigation during the on-site inspection. This will be used for a tracking purposes that all necessary/planned steps of the inspection have been fulfilled and documented.

3.12. Report preparation and storage of evidence

3.13.1. Once the on-site part of the inspection is completed, members of the Division start preparing a summary report containing all the findings and recommendations. The report is reviewed and approved by the head of Division and becomes a part of a broader report covering the whole scope of the on-site inspection and presented for approval to the NBM's Executive Board.

Software requirements for report preparation

3.13.2. The documentation phase of investigations is extremely important but at the same time is very time consuming. Therefore, it is expected that the Software Solution will support even this part of the process, for instance:

a. Facilitate preparation of a report – e.g. populate information from analytical parts to a predefined template;
b. Facilitate incorporation of diagrams, charts and other statistical tables from existing sources of data;
c. Store the supporting evidence related to the case and allow creation of a package which could be sent to FIU or other authorities or for use in court proceedings;
d. Define various roles with different access rights: e.g. analyst, approver, Legal approver, Board approver;
e. Allow access by users from other units;
f. All final report should be searchable for future purposes; and,
g. Provide full audit trail functionality.

3.13. Metrics and reporting

3.14.1. The Software Solution will provide various types of reports, dashboards and visualizations (charts, graphs, diagrams). The reporting functionality should cover operational metrics of the AML/CFT Division but also a set of reports displaying trends and patterns in money flows which could support the investigative function.

3.14.2. Operational metrics:

a. Statistical overview of open alerts/cases/inspections, i.e. current work-in-progress;
b. Statistical overview of inspections conducted, closed cases, triggered alerts, types of violations found, sanctions applied, i.e. overall performance of the unit;
c. Comparison to yearly KPIs.

3.14.3. Dashboards focusing on information about banks and the Moldovan market – both current state and historical views, with monthly/quarterly/yearly statistics and trends, for instance:

a. Total values of domestic and international transactions, break down per bank;
b. Number of domestic and international transactions, break down per bank;
c. Balances of the banks, displaying the changes from previous period;
d. Distribution of transactions by product types;
e. Distribution of transactions by product currencies;
f. Distribution of transactions by product jurisdictions;
g. Distribution of transactions simultaneously by product type, currency, jurisdiction, domestic/international, date etc.
h. Number of cases per bank;
i. Results of inspections; and,
j. Other data requests

4. Other users

There are several business units which can be considered ‘interested stakeholders’ in this project. They are mainly data providers. Their particular interest is to obtain additional value from the data provided. Considering the capabilities of the solution, they would benefit from enriched output reports. During the analysis and design phases, additional discussions will be arranged with these business units in order to address their needs.

Section 4. Solution and services requirements

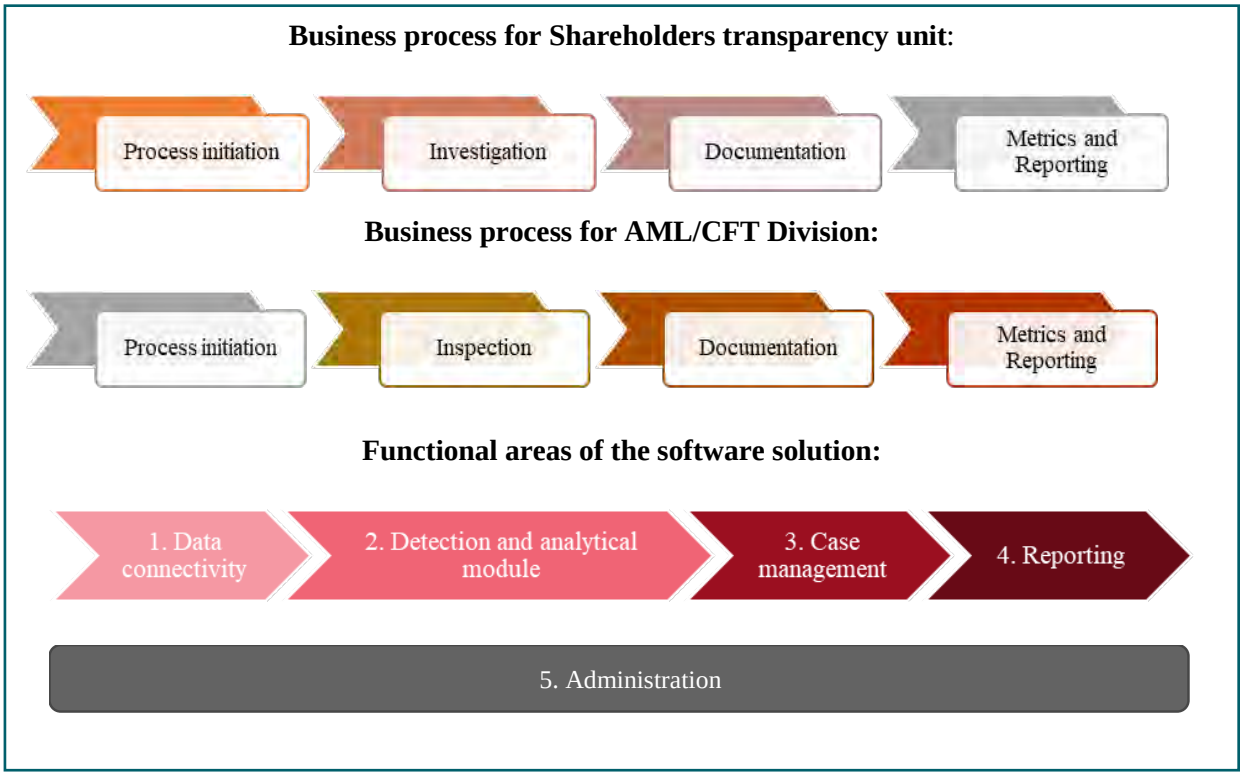
1. Functional requirements

1.1. As explained in the process description section (*Section 3.* Business Units' descriptions and activities), The Business Unit Descriptions and Activities Sections, the Software Solution should support the desired business processes. It should empower the Shareholders Transparency Unit and AML/CFT Division with the corresponding functional areas that represent groups of requirements.

1.2. Key functional requirements of the Software Solution are split into five categories according to the stage to which they relate within the Shareholders Transparency investigation process and AML on-site inspection process: (1) data connectivity, (2) detection and analytical module, (3) case management, (4) reporting and (5) administration. The chart below presents a high-level overview of the key components of the processes mapped to the functional areas of the required Software Solution.

1.3. Both processes have similar requirements in the documentation and reporting areas as well as they are using the same data sources for the analysis (*Figure 5*). The main difference is in the analytical part e.g. different modus operandi observed by the Shareholder Transparency Unit and AML/CFT Division require different detection scenarios and rules.

Figure 5: Overview of the processes and corresponding software requirement areas



1.4. It is expected that the Software Solution will cover the following capabilities:

a. *Data connectivity:* allows for connection to internal data sources of NBM as well as external data sources, which are in various formats and supports various connection types as defined in Section 4, *Table 3: Application Architecture (Integration perspective)*.
b. *Detection and analytical module:* allows for searching within the data sources, building, maintaining and executing search terms, provides the scoring model that would consist of the detection rules and alerts generation algorithms, monitors data source changes and takes the local language specifics into account; provides the user with the reasons why a particular alert was created, gives tools and visualizations that allow further analysis of the underlying data;
c. *Case management*: enables the managing of the workflow related to the investigation and inspection process, manages alerts and cases, supports the investigation steps and on-site inspection checks, gives multiple cooperation options for the users/groups of users, allows automation of the reviews but still supports the ad-hoc manual or scheduled opening of cases;
d. *Reporting*: allows for the creation of standard and tailored reports that present data, investigation and inspection results, detection and operational effectiveness on different levels of sophistication for different types of beneficiaries;
e. *Administration*: provides options to manage different types of users, granting them appropriate rights and permission to access the system.

1.5. A detailed list of functional requirements is in *Table 1*, covering requirements of processes for Shareholder Transparency Unit and AML/CFT Division within the NBM. For each of the requirements, we indicated its importance by either marking it as "Mandatory", or "Preferable". This section is only for informational purposes, please refer to Section 10 which provides the full template that will need to be completed as part of the Technical Proposal.

Table 1: Importance of functional requirements

ID	Requirement	Description	Importance
1. Data Connectivity and Data Management			
FR 1.01	Connectors to data providers and registers	The solution should be capable of connecting to a number of commercial databases, public registers and other databases that have standard connectivity options or be able to continually download various (sanctions/black/other) lists. Please describe the connection options provided within your solution. Note: The definition of the source databases used by the NBM is in *Table 3: Application Architecture (Integration perspective)*. All databases and data sources will be provided by the NBM in a standardized and structured form.	Mandatory
FR 1.02	Data extraction, transformation and loading	The solution should provide Extract Transform Load (ETL) like capabilities, that would enable data extraction, processing, validation and loading into a centralized repository. ETL tool should be able to extract data from basically all the data sources available and described in *Table 3: Application Architecture (Integration perspective)*.	Mandatory

ID	Requirement	Description	Importance
		At the same time, it should not be limited to the described data sources, allowing extraction from almost any source heterogeneous data source (e.g., files: ex. xml, txt, csv, xls etc., database: ex. Oracle, Microsoft SQL etc.). The ETL tool should provide the possibility to initiate and establish various connection types (e.g., FTP, calling web services), according to a set time schedule or according to predefined events. It should be able to detect and extract automatically all the new data according to established scenarios. It should support best practices in the field of data extraction techniques in use today (e.g., in scheduled batch type regime, sequential, parallelized, incremental extractions etc.). It should allow configuration of data importing scenarios for each source / type of data separately. In order to ensure efficient operations and to ensure high quality of data, the toolkit should provide complex mechanisms of validation, cleansing and transformation of data. To this end, it should provide adequate and intuitive tools that allow designing/ management of processes (flows) and validation, cleansing and transformation rules. The important functions of ETL tool should be able to access/use by friendly GUI interfaces. All operations of planning, coordinating, execution of data extraction procedures should be easily configured through graphical interface, using standard functions of ETL tool. ETL tool should provide a GUI-like development environment, which will allow modelling and managing of processes related to extraction, validation, transformation and loading of data into data repository in an intuitive manner, drag-and-drop type. For this purpose, the Bidder should indicate in the description of the proposed toolkit an explanation of how it can support all the above-mentioned requirements.	

ID	Requirement	Description	Importance
FR 1.03	Web crawler	It is recommended that the tool has a web crawling functionality to search online sources that do not have standard interfaces (API) or other connectors. It should be possible to easily and quickly add a new data source via a web crawler. It would be sufficient to provide the hyperlink to the website with the content matching the search query.	Preferable
FR 1.04	Social media and networks	It is recommended that the solution has the ability to search a number of social networks (Twitter, Facebook, YouTube, Flickr, Instagram, Tumblr, Odnoklassniki, LinkedIn etc.), blogs, discussions related to articles in news, web forums and other discussion platforms and similar sources.	Preferable
2. Detection and Analytics			
FR 2.01	Rule based detection	The solution should use a rule-based approach for triggering alerts. A rule represents a risk indication. NBM will provide a number of major rules which should be implemented within the solution. The solution needs to be flexible enough to enable the definition of new rules / modification of the existing ones. There should be no restrictions to the number of simultaneous active rules. The rules differ for the purposes of AML/CFT Division and Shareholder Transparency Unit. Sample of common detection rules for Shareholder Transparency Unit (the full list might total approximately 50 rules): - New shareholder; - Buying /registering shares in the same hour/day or near period of time in the same bank; - Buying similar number of shares, usually under the amount for qualifying holding; - Using the same financial source to buy shares; - Using the same broker/intermediary to buy shares; - Directing of dividends to the same person or group of persons; - Using their voting rights, the same way; - Having the same legal representative; - Having the same administrator/director/UBO/shareholders/associates;	Mandatory

ID	Requirement	Description	Importance
		- Having the same address, phone, headquarters; etc. Sample of detection rules for AML/CFT Division (the full list might total approximately 50 rules): - Significant inflow/outflow of foreign currency in/from the Moldovan banking sector within a short period of time; - Trend in increasing transactional activity with high-risk jurisdictions; - Rapid movement of funds in a local/foreign currency between local banks without any clear business reason; - Significant inflow/outflow of cash occur in a bank/banks without any clear business rationale; - Increased number of transactions with sanctioned/blacklisted countries. Note: The rule-based detection can be complemented by an advanced analytics approach (machine learning etc.).	
FR 2.02	Monitoring changes	The solution will be used to continuously monitor the shareholders and UBOs. It is necessary that the solution enable the setting up of a number of rules which will monitor relevant changes in selected data sources, e.g. name that matches the name of UBO/shareholder/administrator of the shareholder was added to a sanction list.	Mandatory
FR 2.03	Transactions monitoring	It is required that the solution be able to integrate transactions (local, international – SWFT MT103/202 – as well as cash, report on purchase and sale operations of foreign currency – excel reports) for monitoring if there are any suspicious patterns (as define through the rules). It is not the aim of the NBM to monitor the transactions online or to block transactions. Note: The definition of the source databases transactional database is *Table 3: Application Architecture (Integration perspective)*. All databases and data sources are/will be provided by the NBM in standardized structure form.	Mandatory
FR 2.04	Aggregation of detection results per Shareholder/ Customer/Bank	It is required that the detection rules be linked into combined scenarios with results for one shareholder/UBO/customer/bank incorporated into one alert.	Mandatory

ID	Requirement	Description	Importance
FR 2.05	Rule scoring, scenarios and prioritization of alerts	The solution will provide prioritization of Alerts (identified hits) according to their severity. The scoring of Alerts will be based on weights of risk related to each of the rules and combine multiple searching rules into a scenario.	Mandatory
FR 2.06	Customization and set up of new search terms and/or detection rules done by end users	It is required that NBM analysts have the possibility to edit existing and add new detection rules, combine them into scenarios and set up weights of the rules. This should be possible via tools that are easy to use by non-technical staff (no programming needed). It is required that NBM analysts will be trained to set up new rules and as part of the training phase as additional rules will be implemented.	Mandatory
FR 2.07	Custom scheduling and triggering of rule execution	It is required that NBM analysts be able to schedule detection rules individually. For example, some rules might be triggered by an event, some will run every day, some – every first day of the month etc.	Mandatory
FR 2.08	Search through various data sources	It is required that the solution will integrate all available data sources and will allow NBM analysts to select relevant data sources and columns/attributes in source. The searching functionality will be also used for the detection rules. For example, the solution should allow the following: - Search within the population of international and domestic payments for information related to the shareholder or his affiliated persons; - Search within the CRR data for information related to the shareholder or affiliated persons; Search within the historical cases – was the shareholder or any of the affiliated parties a subject for investigation, was there any penalty/withdrawal of shares imposed etc.; - Search within the population of both local and international payments with the data from the daily banks' reports on foreign exchange transactions performed on intra and inter-bank market; - Search within the database of commercial registers data, sanction lists and blacklists. Note: The definition of the source databases transactional database is in *Table 3: Application*	Mandatory

ID	Requirement	Description	Importance
		Architecture (Integration perspective). All databases and data sources are/will be available with the NBM in standardized structure form.	
FR 2.09	Advance searching operators	The solution will allow the analyst to use wildcards, Boolean, proximity, date filters and other operators in order to make the search term more precise and limit the number of false positive hits. This functionality will be used also for the detection rules.	Mandatory
FR 2.10	Transliteration of search terms	The solution should allow the number of UBOs which can be citizens of countries where the Latin alphabet is not used. Therefore, it is important that the solution is able to automatically transliterate the search terms into other alphabets (Cyrillic). This functionality will be used also for the detection rules.	Mandatory
FR 2.11	Fuzzy searching algorithms	It is required that the solution will use fuzzy searching algorithms in order to identify all potentially relevant hits, including different transliterations, spelling mistakes, typos, phonetic matching etc. The functionality should allow NBM analysts to set a similarity score and has to be available also for the detection rules. Please describe distance functions or fuzzy searching algorithms used by the solution.	Mandatory
FR 2.12	Search within the attached documents and historical cases	The software should support the full text indexing of attached documents within the historical cases. This functionality will be used also for the detection rules.	Mandatory
FR 2.13	Network analysis	It is required that the solution support the review and investigation and use network analysis, i.e. automatically joining every piece of relevant data together and creating a network of important information describing the whole situation. This may include analytical reports and visualizations like network charts of an ownership structure, payment flow etc. The networks should be dynamically expandable to the next level in order to see further related parties or transactions. Analysts should be able to include information manually into the network chart.	Mandatory
FR 2.14	Drill down (inquiry engine)	It is required that the system be able to display detailed information for the Alert based on source data. The drill down should be available directly from the case management.	Mandatory
FR 2.15	Support of black/white list/special entities list	It is required that the solution support black and white lists functionality including its upload from a spreadsheet or a text file.	Mandatory

ID	Requirement	Description	Importance
FR 2.16	Data mining & Statistical and mathematical analysis	It is required that the detection and/or Alert scoring can be enhanced through further data mining or other techniques that improve the scoring and limit the number of false positive hits. For example, it should have the ability to detect risky situations/behaviors based on a prediction analysis. Please specify what data mining and further analytical functionality is supported.	Mandatory
FR 2.17	Visualizations	It is required that the solution provide a number of highly configurable visualizations, including financial data visualization, network visualization, e.g. flows and entities and dependencies between them to identify hidden connections between the bank's customers.	Mandatory
FR 2.18	Transparent reasons for triggering alert	It is required that the solution provide descriptions for creating an alert with further details of the entities involved, e.g. display the underlying data with a reason why it was triggered. In turn, this trigger will be used for the on-site visit and any associated previous alerts in the system.	Mandatory
FR 2.19	Bank Risk Rating (BRR)	The software solution should calculate and use the BRR on the shareholder and bank level. BRR will be also one of the factors affecting scoring of the alerts and their triggering. While most factors contributing to risk rating are quantitative, other are qualitative, for instance bank's reputation. This brings the need to set the weights of each factor.	Mandatory
FR 2.20	Predefined rules library for detection of anomalies	It is considered as an advantage if the solution already contains a library of rules. Please list examples of scenarios/packages that are covered by the rules' library, (e.g. Frequency analysis of data (dates, addresses, names) to find outliers or unusual concentrations etc.)	Preferable
FR 2.21	Instant translation of search term	It would be beneficial for the solution to be able to translate the search terms into other languages (Romanian, English, Russian etc.).	Preferable
FR 2.22	Geographical analysis	It will be considered an advantage if the solution provides geographical analysis. For example, display entities on map, highlighting entities located at the same address or locations with high density of searched entities. Please specify how geographical analysis is supported.	Preferable
FR 2.23	Self-learning component	It will be considered an advantage if the detection and/or Alert scoring is enhanced through a self-learning component that recognizes recurrence, statistically aberrant behavior or improves the scoring based on history of analysts'/investigators'	Preferable

ID	Requirement	Description	Importance
		actions etc. Please specify how machine learning component is supported.	
3. Case Management			
FR 3.01	General requirements	It is required that the solution will provide full lifecycle support for the management of the cases related to ST and AML activities, like: - Determine automatic case allocation that should be flexible and based on the number of rules set by the NBM; - Support for the user case creation; - Allow creation of flexible workflow in order to cover all existing and possible next steps of investigation; - Facilitate preparation of a report – the ability not only to document the off-site investigation materials, but also to incorporate and structure the findings and documents prepared during on-site inspections; - Provide capabilities to populate information from analytical parts to a predefined template; - Store the supporting evidence related to the case and allow for the creation of a package which could be used in a court proceeding; - Search within historical cases – was the shareholder or any of the affiliated parties the subject of an investigation, was there any penalty/withdrawal of shares imposed etc.; - Define various roles with different access rights: e.g. searching, analysis, approval, allow access to users from other units; - Full audit trail functionality.	Mandatory
FR 3.02	Alert Management	It is required that the alert management include all the modules and serve as the main interface for users to see alerts and perform the analysis.	Mandatory
FR 3.03	User case creation	It is required that the solution support user case creation to address the ad-hoc requests and information obtained from internal and external sources – this can be done for both existing shareholders approved by the Licensing Unit and shareholders which are waiting for approval, as well as in AML/CFT purposes.	Mandatory
FR 3.04	Alert details view	The software should display all information about the alert and shareholder in question no matter if it was opened manually, automatically triggered or opened based on the scheduled plan. Display	Mandatory

ID	Requirement	Description	Importance
		source data including the reason why an alert was triggered.	
FR 3.05	Workflow editing, workflow definition	The solution should enable NBM analysts to customize the workflow.	Mandatory
FR 3.06	Multiple workflows	The solution should support multiple workflow scenarios to cover various types of investigations. Multiple (up to 5) workflows should be implemented. Each step of the workflow should have the "upload attachment" functionality, free text box for writing summaries and notes, possibility to export the step to word document, picture (for network analysis) or PDF.	Mandatory
FR 3.07	Enable follow up of the Alerts	It is required that alerts will (have to) be followed up in the case management workflow.	Mandatory
FR 3.08	Record steps taken	The case management should enable (and/or require) to record all steps taken by a reviewer or an investigator.	Mandatory
FR 3.09	Attach supporting evidence in various formats	It is required that the supporting evidence will be attached to the case management in various formats.	Mandatory
FR 3.10	Export of the evidence documents	It is required that the solution will allow creation of a package (a folder of the selected attachments and analysis to be exported) of evidence documents related to the case which could be used for a court proceeding.	Mandatory
FR 3.11	Custom attributes in case management	The solution should allow NBM's designers to set new attributes in the case management. New attributes will be used for searching and filtering.	Mandatory
FR 3.12	Delegation, escalation and assignment of alerts and tasks	The solution should allow analysts to automatically or manually assign the Alerts and tasks to a certain user or group of users. It will be possible to delegate or bulk re-assign the tasks to other users. Aging Alerts may be escalated.	Mandatory
FR 3.13	Filtering and searching through all cases and Alerts in the system	The case management should allow investigators to filter and search using various fields within all alerts and cases that have not been archived yet.	Mandatory
FR 3.14	Complete history of all alerts and cases	The solution requires that all cases and Alerts need to be saved. After a certain period of time, they can be archived.	Mandatory
FR 3.15	Connecting case management module and data analysis module	It is required that the case management and data analytical modules are directly connected to allow investigators to understand the related alerts/scoring and further investigate them in the data analysis module, e.g. perform a network analysis, search within payments, CRR or other sources etc.	Mandatory

ID	Requirement	Description	Importance
FR 3.16	Connecting, linking, merging of cases	The solution should allow for related Alerts to be linked or cases to be manually merged.	Mandatory
FR 3.17	'Yearly plan' trigger of analysis	It is recommended that within the solution there will be an option to manually trigger the analysis. For example, open the investigation of all the shareholders of one particular bank; open the investigation of all shareholders that hold shares above a certain threshold; and/or open investigation of customers posing a high risk of ML/TF.	Preferable
FR 3.18	Re-screening after certain period of time.	It is recommended that within the solution there will be an option to set the parameters to allow automatic opening of investigations of shareholders after a certain period of time after previous investigation, as well as for previous ML/TF analyzed cases.	Preferable
FR 3.19	Direct query to the database of case management	It will be considered an advantage if a (super) user can analyze case data without using the application part but using the querying required data and cases directly in database. Either standard querying language (SQL and similar) or a graphical query builder is expected.	Preferable
FR 3.20	Multiple custom expiration intervals/reminders for each case	It is recommended that the solution provide an option to set multiple custom expiration limits for each case. Certain cases may be of high importance and may require different treatment.	Preferable
		4. Reporting	
FR 4.01	Investigation report templates	It is required that the solution will facilitate preparation of the investigation report and populate information from analytical parts to a predefined template.	Mandatory
FR 4.02	Expected reports	It is required that the solution provide a set of standard reports to various users and recipients, e.g. shareholder transparency monitoring unit, internal audit, management of the bank, AML risk monitoring etc. The following areas of coverage should include but not be limited to: a. Statistical overview of open alerts/cases/investigations, i.e. current work in progress; b. Statistical overview of investigations conducted, closed cases, triggered alerts, i.e. overall performance of the unit and of the particular user; c. Success rate, level of false positive alerts; d. Comparison to yearly KPIs (which would be inserted manually by administrator);	Mandatory

ID	Requirement	Description	Importance
		e. Duration of different stages of investigation (per phase, per employee, per bank etc.); f. Management dashboard focusing on information about banks – both current state and historical views; g. Number of shareholders per bank; h. Number of transparent and non-transparent shareholders; i. Percentage of non-transparent shareholders per bank; j. Number of cases; k. Results of investigations; l. Shareholder's transparency risk rating of the bank (please see the detailed description below); m. Statistical overview, including charts, for payment flows both local, international and cash; n. Risk scoring for identified AML vulnerabilities and suspicious; o. Statistical overview, including charts, for payments flow involving high risk jurisdictions/customers/products. The definitive list of output reports will be determined during analysis phase, but will not exceed 100 customized reports.	
FR 4.03	User-defined reports	The solution should allow our analysts and investigators to create ad-hoc reports, based on all the available data from the repository. NBM analysts should be able to use: a. filters on any required column; b. aggregation by any required column; c. usage of basic statistical functions (count, sum, avg, median, min, max); d. usage of logical functions (and, or, not, if) and basic text functions.	Mandatory
FR 4.04	Formatted printouts/exports to MS Office	It is required that the reporting outputs be available at least in MS Office formats, PDF and images (JPEG, PNG, EMF or similar) for visualization/charts.	Mandatory
FR 4.05	Preparation of statistical reports and dashboards for transactions volumes/ geographies involved etc.	It is required that the solution provide the possibility to create a sample of the transactions according to the specified by the user parameters and return the list of the transaction matching them.	Mandatory
FR 4.06	Export of the samples prepared	It is required that the solution support export to an excel file of the transactions matching the user query (see FR 4.05)	Mandatory

ID	Requirement	Description	Importance
5. Administration			
FR 5.01	Audit trail history of changes made	It is required that all user actions, the changes of the rules, scheduling and any actions done in case management will be tracked. The audit trail should be fully searchable. The audit trail should allow answering following questions related to: - what was updated / added / deleted / viewed - store original value and new value; - when - exact timestamp; - by whom - application username, operation system username, role.	Mandatory
FR 5.02	User management	The solution should include user management functionality including management of user groups/roles with various privileges. The desired business processes consist of numerous tasks performed by different specialized Unit members and other bank representatives (i.e. users of the Software Solution). The roles can be shared (e.g. Head of the Unit can have "Approver", "Rules designer" and "Admin" role at the same time) within one user profile. Hence the Software Solution needs to provide flexibility in access rights management to allow, in particular: 1. Separate user groups with different access rights to be set up in order to make the communication between the responsible Unit and other NBM stakeholders efficient. Example of types of users and sample of the related tasks would include: a. For the Shareholders Transparency Unit: i. Analyst (Investigator) represents the main users performing the investigation on alerts and cases assigned to him/her. After finishing all the steps as indicated in the previous section and completing the report, the status of the case should be changed and made available to an approver. Regulation and Authorization Department in some cases can have this function. ii. Head of the Unit and Head of the Department (Approvers) represent the users who review, validate and approve the investigation performed and documented within a case. They should have an option to either send the case back to the analyst or approve the case.	Mandatory

ID	Requirement	Description	Importance
		Further workflow and approval/review process is expected to be done outside of the Solution. iii. Regulation and Authorization Department and on-site team members (Viewers) may be allowed to have read-only access to search module or a specific case, based on given rights. iv. Rules designers are users who are responsible for the creation and update of the detection rules and scoring model. v. Admin users are responsible for user and access management, definition or roles by granting the appropriate rights and permissions. b. For the AML/CFT Division: i. Analysts represent the main users performing the on-site inspection, review of alerts and cases assigned to him/her. After finishing all the steps as indicated in the process description section and completing the report, the status of the case should be changed and made available to an approver. ii. Head of the Division (Approvers) represents the user who reviews, validates and approves the analysis and reviews steps performed before and during the on-site inspections that are documented within a case. Approvers should have an option to either send the case back to the analyst or approve the case (results of the inspections). iii. Team members from Department of Banking Supervision (Viewers) may be allowed to have read-only access to the search module or a specific case, based on given access rights. iv. Rules designers are users who are responsible for the creation and update of the rules and scoring model. v. Admin users are responsible for user and access management, definition or roles by granting the appropriate rights and permissions.	

ID	Requirement	Description	Importance
		c. To ensure that cases marked as, for instance, “strictly confidential” are not accessible (not even as “read only”) to any other NBM stakeholders. d. Allow sufficient flexibility of access rights even for the reporting the functionality and availability of dashboards and statistics.	
FR 5.03	Export of the data	It is required that the tool allow users/NBM to export its data into different data formats (e.g. xml, xls, csv, pdf, docx etc.)	Mandatory
FR 5.04	Backup/Recovery Process	It is required that provided solution should be delivered with tools/scripts for define custom backup policy at database level.	Mandatory

2. Non-functional requirements

2.1. Non-functional specifications establish requirements not directly related to the functionality provided by the Software Solution, but determine its ability to be used, maintained and adjusted to business needs over time. The Software Solution should meet the non-functional requirements set below.

2.2. A detailed list of non-functional requirements is in *Table 2*. For each of the requirements, we indicated its importance by either marking it as “Mandatory”, or “Preferable”. This section is only for informational purposes, please refer to Section 10 which provides the full template that will need to be completed as part of the Technical Proposal.

Table 2: Importance of non-functional requirements

ID	Requirement	Importance
1. Overall Architecture		
NF 1.01	The architecture should be aligned to best practices and standards to meet the highest criteria for security, compatibility, performance and reliability.	Mandatory
NF.1.02	The solution will have an open and modular architecture, which will allow easy integration with different systems and data sources.	Mandatory
NF 1.03	Due to the high amount of processed data and to ensure increased productivity, the solution should have native integrated capabilities such as in-memory processing, multi-thread processing, parallel execution of jobs etc.	Mandatory
NF 1.04	The solution should ensure a high level of stability and operational performance. In this regard, the solution should have effective mechanisms for handling errors, in order to avoid data loss, system-wide blocking processes, system failure etc.	Mandatory
NF 1.05	The solution should have the ability to be adapted in a timely manner to new business needs. It is very important that this will be possible only through parameterization and configuration adjustments in the applications (versus changes in code), thus minimizing adjustment costs supported by the NBM.	Mandatory

ID	Requirement	Importance
NF 1.06	The solution should be easy maintainable. In this regard, the solution architecture should allow implementation of new versions delivered by the software provider without affecting the architecture of existing customizations, components implemented by the NBM and interfaces with other external applications.	Mandatory
NF 1.07	The solution should have user-friendly interfaces, be simple and intuitive in use.	Mandatory
NF 1.08	The solution should ensure a very high level of security, taking into account the sensitivity of the data so that control measures provided at the system level are proportional to the risks involved. In this regard, the most important security objectives to be achieved are: a. ensure confidentiality, authenticity, and integrity of information during processing, storage or transmission of information (including messaging / packages / files); b. ensure an effective control of access and prevent any unauthorized access to its data; c. ensure an effective auditing by monitoring and logging user activities at the system level; d. prevent loss, modification or misuse of information within the system;	Mandatory
NF 1.09	Platform technologies presented in the solution architecture should be open technologies or widely used technologies.	Mandatory
NF 1.10	The proposed solution will meet the minimal infrastructure requirements described in *Table 4 refers to infrastructure* requirements from the client and server side. *Table 4: Minimal infrastructure requirements*.	Mandatory
NF 1.11	The technological and infrastructure architecture represents all software and hardware components necessary to ensure the operating environment in which all solution components should run. The technological platform includes development platforms, database management systems, operating systems that can run solution components, specific system software required to be installed for correct run of the solution, hardware platform that can run solution components etc. In order to be scalable, flexible and easily maintainable, it is recommended that all solution components have a minimum level of dependence on the technological platform on which it runs.	Preferable
2. System Management and Administration		
NF 2.01	One of the most critical concerns for the NBM is to have full control over the implemented Software Solution. This is crucial in order to ensure sufficient flexibility when (any) changes and updates to the regular operation are needed. Therefore, the members of Shareholder Transparency Unit and AML/CFT Division should be able to manage independently the following tasks: 1. Maintenance of detection rules including setting up new detection rules, scenarios and parameters and calibrating them; 2. Alert monitoring and assigning to the Unit members based on automatic rules or manually; 3. Case monitoring and controlling; 4. Access right authorization to new or existing users;	Mandatory

ID	Requirement	Importance
	5. Monitoring of activities, i.e. logging and possibility of monitoring all activities performed within the Software Solution; and 6. Creation of various reports.	
NF 2.02	The solution should allow NBM to define and integrate easily with new data sources (e.g., external database, external web service, external file). In this regard, the solution will provide all the tools needed for this purpose: data mapping, data transformation. The main data sources, which have to be integrated during the implementation project, are described further in *Table 3: Application Architecture (Integration perspective)*.	Mandatory
NF 2.03	The solution should allow at least the following user configurable operations: a. define/customize business rules/criteria for data analysis; b. define/customize automated actions based on different events, time schedule; c. define new reports, based on customizable templates.	Mandatory
NF 2.04	The solution must provide friendly GUI interfaces for administrators to allow the customization/configuration activities, where most operations can be performed by drag-and-drop.	Mandatory
NF 2.05	The solution must be able to store all operational and historical data for a minimum of five years, without affecting its performance.	Mandatory
NF 2.06	The system must support some data archiving procedures. Vendor has to describe archiving approach and automated / manual procedures supported by the solution.	Mandatory
NF 2.07	NBM will operate at least the following environments for the tendered solution: a. *Production*: This will be the main environment to deploy the solution for production; b. *Testing*: NBM will maintain the test environment even after going into production, for development and testing purposes for 2 users; In this regard, the Bidder will consider these facts, when calculating the number of licenses.	Mandatory
NF 2.08	The solution should provide the needed functionality to allow the transfer of data between different environments.	Mandatory
NF 2.09	The solution should have in place some mechanisms to assure puzzling or depersonalization of the data when copied from production to test environment.	Preferable
	3. User Interface	
NF 3.01	The time required for training in order to use the solution should be minimal. Users should have access to information anytime in order to facilitate the proper use of the solution.	Mandatory
NF 3.02	Documentation related to the solution should contain complete guides, detailed and updated for all groups of users.	Mandatory
NF 3.03	The solution should allow saving intermediate work and operations initiated by the user (automatically or at user request).	Mandatory
NF 3.04	User interfaces should allow easy navigation through solution forms, by using complementary mechanisms (e.g., mouse and/or keyboard and/or special functions).	Mandatory

ID	Requirement	Importance
NF 3.05	The solution should allow users to customize its own workspace (e.g., adding menu items to favorites, displaying the latest hits, save searches, save templates etc.).	Preferable
	4. Security	
NF 4.01	All access credentials used by the application should be configurable in the administrative interface. Applications should not contain hardcoded credentials for access.	Mandatory
NF 4.02	None of the solution components should contain stored access credentials in open form (in databases, configuration files).	Mandatory
NF 4.03	All solution related system processes should run with minimum privileges needed to execute the tasks assigned.	Mandatory
NF 4.04	For user management, identification, authentication and access control the following requirements are applicable: a. The solution should allow granular management of access rights to all data and possible operations with them. A typical example of granular use case, is the segregation of user access rights by banks, where different persons will have access to the data based on the origin bank b. Authorization method within the solution should be based on the principle “everything which is not explicitly allowed is forbidden”. c. The solution should allow for the definition of groups of users and roles in the application, and the association of users in the application to these groups and roles. d. The solution should allow granting of access rights at the level of users, groups and user roles. A group can contain multiple subgroups / roles. A user can be assigned to one or more groups and roles; their access rights are determined cumulatively. e. The solution should allow granting of access rights based on business rules (e.g., modifying a template only if the user is an author). f. The solution should allow temporary delegation of rights owned by a user to another user. The delegation of rights should be made with preservation or suspension of the rights owned by the user to whom the rights are assigned. g. The solution should have interfaces and reports relating to existing access rights to data. They can be parameterized according to at least the following parameters: user group/role in the applications, user ID, data category, operations permitted. h. Users from all groups should be identified and authenticated based on integration with directory services of the Beneficiary (LDAP / Active Directory). i. The system should disconnect individual user after idle period expiration. j. The system must block a user after a preconfigured number of unsuccessful login attempts.	Mandatory
NF 4.05	For auditing and security monitoring, the following requirements are applicable: a. The proposed solution will have audit components that will centrally collect and manage audit records at each component level. b. Audit component should allow granular configuration of audit policies.	Mandatory

ID	Requirement	Importance
	c. The proposed solution should allow for determining the specific characteristics of events that must be registered (e.g. products in a certain period, certain events, and facts). d. Application should allow auditing of any event within the application. e. Each audit record should contain at least: i. Moment in time of the event; ii. Subject of the event (User ID); iii. Categories of affected data/parameters; iv. Event that happened; v. IP address of the source that initiated the event, or any other information permitting to identify the source; f. Audit component should use the system clock set to the operating system that runs the audit component. g. Audit component should be able to be integrated with solutions based on open standards, such as SIEM (Security Incident and Event Management) to take over the audit records produced in the solution by SIEM. h. The solution should have also its own user interfaces for accessing and processing recorded log events, including filtering of audit records by any field owned and their export in the usual format. The proposed solution should have secure mechanisms to protect the integrity of audit information recorded.	
NF 4.06	The solution will be able to encrypt sensitive data stored in the database.	Preferable
5. Performance		
NF 5.01	The required solution must have the ability to process in a timely manner the analysis performed by NBM, according to volumes resulting from NBM's activity, namely for the following parameters: a. Response times - time of response to a user operation / query should not exceed one second, excepting the report generation and complex data analysis scenarios which will not exceed 15-25 seconds; b. Number of concurrent users - it is expected that the application should manage easily up to maximum of 10 concurrent sessions; c. Data volumes - in the initial stage the expected amount of data to be processed is about 50 million records per year. On average, each data record will have at least 20-25 data facts (columns); d. Data increments over time - it is expected that the increments for data volumes for data sources will double each 4 years; e. Number of transactions to be processed within given time - it is estimated a number of 50 to 250,000 records to be imported and processed from different data sources daily; f. Deadline for processing data for previous day – the processing of data for previous day should be done within the night window allocated for the application (max. 8 hours).	Mandatory
NF 5.02	Please provide a minimum hardware (VM configuration, storage, network requirements etc.) and software configuration for the host system that will be required to meet the performance requirements mentioned above. In addition, please state the minimum requirements for the client systems (PC's).	Mandatory
6. Licensing		

ID	Requirement	Importance
NF 6.01	Bidder will describe the tendered licensing model, giving details on why the proposed model is the best for NBM needs and will display a comparative chart of licensing models the Bidder is usually tendering.	Mandatory
NF 6.02	Bidder will provide a break-down of the proposed licensing model (e.g. by modules, by user/group of users/server/processor – as applicable).	Mandatory
NF 6.03	When calculating the number of licenses, the Bidder should consider the following situation. NBM will maintain the test environment even after going into production, for development and testing purposes. The Bidder will take into account such situation, and if additional licenses are needed associated costs will be shown.	Mandatory
NF 6.04	All delivered software licenses should include the price for one year of support and maintenance, provided by license's manufacturer, which will start from the final acceptance date. In case of earlier activation of licenses, all the costs for support and maintenance services, provided by license's manufacturer during the implementation stage, will be supported by the Bidder.	Mandatory
NF 6.05	Bidder will provide the optimal licensing model considering the following facts: a. It is expected a total number of 18 users: from which at least 8 analysts and up to 8 different users with access to reports, search and data visualization. b. 2 users with administrative privileges for solution and user management and solution customization.	Mandatory
NF 6.06	Financial Proposal should include all costs related to solution licenses.	Mandatory

2.3. *Table 3* refers to various data application and files that will be accessed by the NBM Software Solution.

Table 3: Application Architecture (Integration perspective)

Data providing Application	Data consuming Application	Description of data flow from the providing to the consumer application	Type of interface
SAPI – Automated Interbank Payment System	Shareholder Transparency and off-site analysis of ML/TF	Provides the financial messages for domestic payments in MDL	Structured data/Exported XML Files
SwiftFinInform	Shareholder Transparency and off-site analysis of ML/TF	Provides a copy of all SWIFT messages MT103 and MT202	Structured data/Exported XML Files or Oracle Database connection
CRR – Credit Risk Register	Shareholder Transparency and off-site analysis of ML/TF	Provides the following data: a. Loan portfolio data b. List of affiliated persons	Structured data/ Exported XML Files or Oracle Database

Data providing Application	Data consuming Application	Description of data flow from the providing to the consumer application	Type of interface
Licensing, authorizations and notification system	Shareholder Transparency and off-site analysis of ML/TF	Provides the following data: a. Requests for authorizations, notifications for transactions b. Information about the new bank's shareholders c. Information about new bank's administrators	Structured data/ Exported XLS files
CSD – Central Security Depository	Shareholder Transparency and off-site analysis of ML/TF	Provides standardized updated list of the bank's shareholders and upon request detailed information about a shareholder and all the related transactions with shares during a certain period of time.	Structured data file
SIRBNM – Reporting system to the NBM	Shareholder Transparency and off-site analysis of ML/TF	Provides cash transactions performed by banks in amount larger than 50,000 MDL	Structured data/Exported XML Files
Data file	Shareholder Transparency and off-site analysis of ML/TF	Register of all accounts and accounts holders.	Structured data/Exported XML Files
SIRBNM	Shareholder Transparency and off-site analysis of ML/TF	Report on purchase and sale operations of foreign currency performed by licensed banks	Structured data/Exported XML Files
MConnect – Governmental platform for interoperability	Shareholder Transparency and off-site analysis of ML/TF	Information regarding the incomes, paid taxes by person ID; Other information available from public registries, based on standard inquires.	Web service inquire
Shareholder Transparency and off-site analysis of AML/FT	Licensing, authorizations and notification system	Information of potential existence of risk related to banks or their administrators.	Structured data
Data file	Shareholder Transparency and off-site analysis of ML/TF	List of designated persons (EU, OFAC, UN)	Structured data/Excel or CSV Files
Data file	Shareholder Transparency and off-site analysis of ML/TF	List of PEP and list of other high risk identified persons (i.e. acting in concern persons etc.)	Structured data/Excel or CSV Files
Data file	Shareholder Transparency and off-site analysis of ML/TF	List of detailed transactions with banks shares (date, broker, seller, buyer, amount etc.)	Structured data/Excel or CSV Files
Data file	Shareholder Transparency and off-site analysis of ML/TF	Letters with detailed information requested from shareholders or from other state institutions (CV, criminal record, previous working place, tax declaration etc.)	Unstructured data (OCR-pdf)

Data providing Application	Data consuming Application	Description of data flow from the providing to the consumer application	Type of interface
Data file	Shareholder Transparency and off-site analysis of ML/TF	Daily data on banks' FX transactions against the MDL with their clients	Structured data/Excel or CSV Files
Data file	Shareholder Transparency and off-site analysis of ML/TF	Agents and Accounts Databases, which allows to make a connection between the FX transactions and SWIFT messages	Structured data/Excel or CSV Files

2.4. *Table 4* refers to infrastructure requirements from the client and server side.

Table 4: Minimal infrastructure requirements

Client side:	Hardware (HW) requirements	Requirements for HW should be as minimal as possible. It must run on VDI infrastructure of NBM without any visible impact on the performance of the virtual desktop machine.
	Operating environments	Windows 10 / VDI Citrix XenDesktop 7.5 and newer operating systems
	Software type:	Recommended: Thin client running on standard Web browser (IE, Chrome, Mozilla)
Server side:	Supported HW platform	x86 platform
	Supported operating systems	Linux or Windows Server family
	Supported versions for operating systems	OS must be maintained by their manufacturers and to be one of the last two major versions
	Supported database systems	Oracle 18c, MS SQL 2016, or newer
	Requirements for virtualization	Must support virtualized infrastructures based on XenServer or VMware hypervisors
	The minimal accepted requirements for cryptographic algorithms in NBM	a. AES-256 for encryption of electronic data; b. SHA-2 for message digest; c. RSA 2048bit for end-point private keys.

3. Implementation requirements

3.1. A detailed list of implementation requirements is in *Table 5*. This section is only for informational purposes, please refer to Section 10 which provides the full template that will need to be completed as part of the Technical Proposal.

Table 5: Implementation requirements

ID	Requirements
	1. Analysis and Design
IS 1.01	**Phase objectives:** 1. The purpose of this phase is to create common understanding of the target solution, explain the priorities within review them against the chosen solution and to create detailed software requirements specification and acceptance criteria of the solution. This

ID	Requirements
	section should ensure a common understanding of the processes, requirements and major gaps in the chosen solution in order to implement a solution that meets the expectations of the NBM. 2. It is expected, that this phase will build upon designed processes and requirement specifications proposed by this RFP and on the proposal of the Bidders, which will identify to which extent the target solution will cover the requirements within out of the box functionality and which will require customization/custom development of the target solution. 3. The Bidder should translate functional requirements into a workable design (functional specification), support the analysis by delivering prototypes of designed features and should prepare the necessary environment for the configuration of the solution. 4. The Bidder should describe the methodology and instruments used for analysis and design phase and should provide sample of deliverables.
IS 1.02	**Main activities:** 1. NBM will present thoroughly current and future requirements regarding the project scope. 2. NBM will present processes inside the scope of the project. 3. For each part of the designed process and requirements the Bidder will demonstrate vanilla version of the solution and explain the way how the system works. For all core functionalities, Bidder will prepare prototyped screens adjusted to NBM requirements. 4. All gaps identified during the RFP will be reviewed in detail and adequate solution will be proposed by the Bidder. 5. NBM will present the data sources together with data samples to be integrated into the solution's data model. Based on this, the Bidder will review the changes to be made in the data model, will define the data quality assurance strategy / model and will propose the solution. 6. Analyze the information about users and their roles. 7. Review the existing IT and network technical infrastructure and develop proposals / recommendations for architecture and related infrastructure of the Solution, considering keeping under control the complexity of IT infrastructure and reusability of existing resources. 8. Define and produce a functional specification that would meet the requirements, given the functional and technical constraints imposed. 9. Document design specifications for solution functionalities based on the software requirements specification (including the link of them to keep clear traceability). 10. Document detailed specifications of the solution (e.g. interaction interfaces and diagrams (Data Flow Diagrams), Use Cases, retrieval scenario, validation scenario, data uploading scenario, analysis scenario etc.). 11. Document test strategy and test analysis in connection to the acceptance criteria and functional specification. 12. Establish the applicable configuration parameters. 13. Define the specifications for customization, configuration and integration with other sources of data/applications.
IS 1.03	**Deliverables:** At the end of this phase, the following will be delivered: 1. Document on the detailed functional specification of the solution, which should cover both technical and functional aspects. From a technical standpoint, the deliverable should document the solution architecture (applications/tools, model integration of these, data model, interfaces and interaction diagrams, security etc.), and technology platform

ID	Requirements
	agreed and signed by both parties. The document should include the following information: a. solution overview (diagrams that provide an overview of the solution architecture accompanied by a narrative description); b. integration platform of solution components, interfaces (the name that will be integrated with the solution, the type of interface (e.g., supplier, consumer, symmetric), solution and the impact of the failure of the interfaces); c. solution architecture attributes (software and hardware technologies, services, components, portability, capacity, availability and reliability, scalability); d. data architecture (context diagrams, logical data model); e. security architecture (overview of security solution); f. other aspects. 2. Document on solution configuration/setting up, which will document in detail all the parameters set for all components of the solution. 3. Document High Level Test Plan and test analysis that will link to and cover all above mentioned specifications. 4. Other documents according to the best-practice and delivery methodology of the Bidder.
2. Build phase	
IS 2.01	**Phase objectives** The purpose of this phase is to transpose functional requirements into application functionalities by applying the agreed solutions in analysis and design phase.
IS 2.02	**Main activities** 1. Install the production and test environments (OS/DB/apps). 2. Implement customization, integration and configuration of the solution, according to specifications of the deliverables accepted at design phase. 3. Produce the blueprint for the logical and physical architecture of the application and database servers. 4. The Bidder should describe the methodology and instruments used for build phase and should provide sample of deliverables. 5. Test analysis is further detailed – complete set of test scripts is elaborated and finalized.
IS 2.03	**Deliverables** 1. Solution, configured and installed in: a. Production Environment b. Test environment 2. Solution should meet the requirements agreed in the above chapters and that should include: a. Functional and non-functional requirements provided in the analysis document; b. Validation rules, workflows, analysis scenarios, reports provided in the analysis document; c. Interfaces specified in the analysis document; d. Security (user rights, other security configurations); e. Documentation provided as per NBM request; 3. Solution architecture document updated as necessary.
3. Testing phase	
IS 3.01	**Phase objectives:** 1. The purpose of this phase is to test the quality of all the functional and technical elements of the solution. During this phase, the Bidder should establish the testing method and should prepare testing scripts for all testing activities that will cover the entire software development and implementation lifecycle.

ID	Requirements
	2. The Bidder should include the proposed approach and methodology for testing in the technical proposal, which will cover at least the scope, approach, resources, tools, sample of deliverables and schedule of the testing activities. The proposed testing approach should be validated/ agreed with the NBM at project initiation phase. The Bidder should indicate in its technical proposal the software instruments that will be used in order to track and monitor the potential open tickets for defects repair. It is obvious must that NBM representatives need to have access to this application. 3. The Bidder is also advised that for non-functional requirements testing, where applicable (e.g., performance testing, stress testing etc.), an automated test solution, or test scripts should be provided to the NBM. In case test results are poor (high rate of "failed" tests, more than 3 failed tests per functionality/application module), the entire module should be considered "unaccepted" and sent back for testing purposes.
IS 3.02	**Main activities:** 1. Testing should be performed according to BS-7925 or similar, and the test activities covered should include: test planning, test specifications, test execution, recording of results, checking for test completion. 2. All testing to be performed should be appropriately planned, prior to being executed. 3. The Bidder should be responsible for documenting and delivering system tests scenarios with logs and results, as a prerequisite for the NBM acceptance process. During system testing, the NBM testing team should participate as an observer (if applicable and/or possible). 4. User Acceptance Testing (UAT) should be the final stage of testing. NBM, with the Bidder's support, should perform this activity and the main objective is to ensure that the final system matches the original requirements defined by the business. NBM may choose to do any tests it needs, based on the usual business process. Testing should be carried out based on users' requirements. It should be performed under the responsibility of NBM to enable their determination as to whether accept the system software or not. 5. The Bidder should support NBM in UAT efforts to help identify problems and communicate them to the relevant team(s) for resolution. 6. The Bidder should ensure the necessary services for all testing activities that will cover at least: a. Prepare UAT documentation/ test scenarios, which should be revised by the NBM and business consultants. After the NBM validates the test scenarios, these documents can be used for testing purposes. b. Agree acceptance criteria and testing strategy. c. Conduct acceptance test. d. Documentation of the testing results. e. Agree the issue list by categories. f. Agree the action plan for solving the issues.
IS 3.03	**Deliverables:** 1. Acceptance test plan agreed and 'signed-off' by both parties. 2. UAT documentation/ test scripts and scenarios agreed and 'signed-off' by both parties. 3. Test results documents.
4. Training	
IS 4.01	**Phase objectives:** The purpose of this phase is to deliver a comprehensive training plan.
IS 4.02	**Main activities:** 1. The Bidder should conduct staff training to ensure an adequate level of knowledge and skills to use and manage efficiently the solution.

ID	Requirements
	2. The Bidder should conduct training sessions for the administration and maintenance and also for development teams designated by the Beneficiary to ensure a proper level of knowledge and skills as to be able to efficiently use the development tools available within the solution and to design and develop individually new scenarios for data source integrations, validation rules, data model, reports, screen forms etc. 3. The Bidder should develop and agree with the Beneficiary the following elements of the training component: a. Bidder's strategy on training and tutoring; b. Structure and content of the training course and manual for each user category. c. Methodology and tools for assessing and controlling the efficiency and sufficiency of training sessions
IS 4.03	**Deliverables:** 1. The training course should consist of different types of training, such as: a. training courses; b. presentations; c. workshops; d. self-learning materials or remote training; and, e. individual consultations. 2. The Deliverables of training sessions should comprise: a. the training plan; b. manual of the courses; c. testing and assessing questioners; and, d. the registry for assessing the knowledge and personnel satisfaction.
5. Go-live and final acceptance	
IS 5.01	System operation in the production environment and final acceptance should be made according to the following scheme: 1. Go-live preparation phase; 2. Soak period; 3. Final acceptance.
5.1 Go-live preparation phase	
IS 5.02	**Phase objectives:** The purpose of this phase is to facilitate the decision-making process in regard with lunching the solution into production.
IS 5.03	**Main activities:** 1. Review and assess readiness from multiple perspectives: a. IT readiness criteria: i. production system fully delivered and functional; ii. configuration document and design specification written and a handover made to the future Service Manager of the software; iii. User manual and Admin manual for the application delivered; iv. maintenance process agreed; v. technical training delivered; vi. no critical defects present after moving into productive environment, unless they are known and approved by the Beneficiary; b. Business readiness criteria: i. all functionalities required are present in the application; ii. no critical or high defects present; maximum of 15 medium and 30 low defects are acceptable; iii. reports are running and generating the correct output; iv. the data loss possible if the application crashes is not exceeding the RPO;

ID	Requirements
	v. help mechanisms for users are available; vi. user rights implemented according to the specifications; vii. user training performed. 2. Remediation Plan for defects is developed (defect list may contain defects with severity level 3 and 4). 3. The Bidder should describe the methodology and instruments used for go-live preparation phase and should provide sample of deliverables.
IS 5.04	**Deliverables:** 1. The solution is ready for launching into production (the solution was installed on production environment; testing was performed and no severity 1 and 2 defects were found). 2. Remediation plan for defects. 3. Bidder's self-assessment report of business and technical requirements (this document should cover at least the following information: requirement identifier, solutions associated with the requirement, % of requirement coverage in the application).
	5.2 Soak period
IS 5.05	**Phase objectives:** 1. The purpose of this phase is to extensively test solution behavior in daily operation to determine whether the solution meets the required qualities of capacity and stability. 2. This phase should be performed during a minimum period of 20 business days. 3. During this phase, the NBM should draft its own self-assessment report, which will be compared with that provided by the Bidder at the end of Go-live phase. 4. In case significant discrepancies are found (between NBM's self-assessment and Bidder's self-assessment), NBM reserves that right to ask the Bidder to fix or improve the coverage degree of certain business & technical requirements.
IS 5.06	**Main activities:** 1. Provide extensive offsite and if needed onsite support during the entire soak period for bug fixes and performance issues: log inspection and analysis/ problem prevention/ fine tuning. 2. For defects identified during soak period, a remediation plan should be agreed. 3. Solving of defects identified in remediation plan approved prior to go-live phase and also identified during soak period. 4. Providing assistance (help desk support) for end users. 5. Assistance for active monitoring of system's parameters. 6. If needed, the Bidder should provide any additional configuration or customization required in the solution, in order to comply with the formal set of requirements. 7. If needed, the Bidder should provide improvement works for system performance with regard to its accessibility and efficiency. 8. The Bidder should assist the Beneficiary in system administration/management. During the soak period, the Bidder should ensure full transfer of knowledge to the Beneficiary for proper system administration/management. 9. The Bidder should assist the Beneficiary in providing I and II-line support to the internal users of the Beneficiary and the reporting entities.
IS 5.07	**Deliverables:** 1. Remediation plan fully executed and all defects removed. 2. Status on remediation plan for defects occurred prior to and during soak period (weekly reports).
IS 5.08	**Acceptance criteria:** 1. All defects included in remediation plans are fully removed.

ID	Requirements
	2. No major bugs identified during soak period. 3. No discrepancies found between NBM's self-assessment report and Bidder's self-assessment report. In case discrepancies found, these should be removed prior to final acceptance of soak period. 4. An acceptance report should be signed by both parties within the agreed time period.
	5.3 Final acceptance
IS 5.09	**Phase objectives:** 1. The purpose of this phase is to formalize the complete delivery of system functionalities, documentation and services. 2. Such acceptance should be signed after formally closing the soak period for the solution. 3. After this final acceptance, the NBM should approve the final instalment payment and the contract of guarantee will become active.
IS 5.10	**Main activities:** 1. Review and assess the criteria defined below for final acceptance of the solution. 2. Criteria list for solution final acceptance is provided below. NBM should align and detail together with the Bidder the acceptance criteria at project initiation stage. a. Documentation/ deliverables for analysis and design phase provided and accepted by the NBM; b. Documentation/ deliverables for build phase provided and accepted by the NBM; c. Documentation/ deliverables for test phase provided and accepted by the NBM; d. Documentation/ deliverables for soak phase provided and accepted by the NBM; e. Documentation/ deliverables for training phase provided and accepted by the NBM; f. Criteria list for general acceptance is provided below. NBM should align and detail together with the Bidder the acceptance criteria at project initiation stage: 3. All above-mentioned documentation & deliverables are updated and fully provided by the Bidder. 4. The Beneficiary should analyze the documents and deliverables submitted by the Bidder in order to acknowledge the quality requirements. 5. Services included in the tender were fully executed by the Bidder.
IS 5.11	**Deliverables:** Criteria list revised and agreed by both parties.
	6. Minimal acceptance criteria and Solution Documentation
IS 6.01	**Phase objectives:** The acceptance criteria should be revised and agreed with the NBM at the beginning of the initiation stage. The below mentioned criteria are minimal and should not be subject of elimination. 1. The deliverables of each phase should be provided to the NBM as in accordance with the Work Plan which will also take into account the time needed for the beneficiary and Bidder to review and coordinate the deliverables. 2. Deliverables meet the NBM expectations and requirements in terms of clarity, level of detail, structure, content etc. 3. Deliverables are aligned with internal standards of the Bidder and best practices. 4. Deliverables are easy to use and understandable to the intended beneficiaries. 5. Deliverables are aligned with quality standards agreed between the NBM and the Bidder. 6. Acceptance documentations for each phase are formally approved by the Parties.
IS 6.02	**Main activities:** For the testing phase, additional minimal acceptance criteria to be included are: 1. All tests should be completed without severity levels 1 or 2. The severity of the problems found should be defined according to the criteria below:

<table>
<tr><th>ID</th><th>Requirements</th></tr>
<tr><td></td><td>
<table>
<tr><th>No.</th><th>Severity</th><th>Description</th></tr>
<tr><td>1</td><td>Critical (fatal problem)</td><td>Core functions fail completely and constantly or are missing. Complete and continuous central system failure.</td></tr>
<tr><td>2</td><td>High (serious problem)</td><td>Vital or critical functionality for the intended use is missing or failing continuously or repeatedly. Vital or critical functionality for the intended use cannot be activated or fails continuously.</td></tr>
<tr><td>3</td><td>Medium (general problem)</td><td>Important but non-critical or vital for the intended use system functionality is completely missing or failing continuously or repeatedly.</td></tr>
<tr><td>4</td><td>Low (minor problem)</td><td>Certain functions are missing or failing. System works correct but esthetical problems occur. Certain functions work but not completely correct.</td></tr>
</table>
2. Issues with severity level 1 and 2 should require immediate bug fixing, and it should be mandatory for testing process to be continued.
3. Testing process should consist of as many test cycles as necessary until all severity 1 and 2 is-sues will be eliminated. After a Severity 1 or 2 problems will be fixed, it is for the NBM testing team to decide whether test cycle will be restarted or continued.
4. The number of outstanding defects is below an acceptable upper limit (to be agreed before the acceptance phase) or the faults are minor.</td></tr>
<tr><td>IS 6.03</td><td>Deliverables:
As deliverables of the project, the Bidder should provide at a minimum the following documentation:
1. User instructions and users guide: this document should provide sufficient details, understandable by end users regarding functionalities, operations. The document should describe the steps and actions to be performed in application and also print screens should be included, tips & trick, FAQ etc. The purpose of the document is to represent a basis for learning process and also a reference point for users in case information about operating applications is needed. The user guide should be provided in Romanian or English.
2. System operating instructions – work instructions:
a. Maintenance instructions/service management troubleshooting guide: this document should include all known errors and solutions associated and should provide sufficient technical details in order to correct potential errors.
b. Installation manuals, including system modifications at the level of application and database. The document should cover installation requirements, installation steps and parameters setup for the NBM, post installation tasks, tips & trick, FAQ.
c. Documentation relating to application administrators should cover roles, tasks (e.g., back-up, tuning, patching), utilities, logging, tools for developers etc.
d. Documentation relating to application customization/development (conditions and methodology for solution customization by the NBM).
e. Archive & retrieval processes and related documentation.
f. Documentation relating to security, covering access control, user management, auditing and monitoring, security reports.
g. Documentation relating to system configuration – customized installation guide (if this information is not covered by item 2.b above).
3. Commented source code for all developments and customizations carried out during the project period (e.g., for scripts).</td></tr>
</table>

ID	Requirements
	4. Documentation relating to end users and technical trainings - support materials for end user and technical trainings.

4. Project Management Requirements

4.1. A detailed list of project management requirements is in *Table 6*. This section is only for informational purposes, please refer to Section 10 which provides the full template that will need to be completed as part of the Technical Proposal.

Table 6: Project management requirements

ID	Requirements
1. General project management requirements	
PM 1.01	The goal of project management is to provide the necessary skills for project organizing and management to successfully achieve the set objectives. During the project life cycle there should be assured efficient resource planning and allocation, progress control during each stage, quality monitoring and evaluation of the deliverables etc.
PM 1.02	The Bidder is responsible for implementation project management, as well as for execution of activities and Work Plan mutually agreed with the Beneficiary. The jointly agreed Work Plan will include the necessary activities and deliverables review and coordination process within an agreed timeframe.
PM 1.03	The Bidder is responsible for identifying and mobilizing the adequate resources to execute the Work Plan activities in its responsibility, at the agreed quality level.
PM 1.04	The Beneficiary is responsible for all procedural and administrative matters relating to the launching, contracting and financial management of the project (including payments) related to project implementation activities and for technical implementation.
PM 1.05	A well-known project management methodology or standards (e.g., PRINCE2, PMBOK etc.), or an internal developed methodology, based on these standards or methodologies, should be used for the implementation project and should be appointed specifically.
PM 1.06	The minimum number of key Professional Staff is presented in Section 8 and Section 10. In order to organize the project, the Bidder should appoint a Project Manager, who will be heading the project team.
PM 1.07	A detailed project organizational chart, covering the key roles and the potential additional roles identified by Bidder should be provided as part of the Initial Project Management Plan included in the Technical Proposal.
PM 1.08	The Project Manager of the Bidder has the authority and responsibility to coordinate and implement the project so that the objectives are met. Its primary responsibility is to ensure that all required deliverables are timely presented and meet the established quality standards.
PM 1.09	The Project Manager of the Bidder should ensure a proper management of project risks, quality and progress control of deliverables at every stage of the project. It will also be provided a control of interdependencies between the project components to minimize any risk of project stagnation.
PM 1.10	The Project Manager of the Bidder should ensure an effective communication within the project, through progress reports with a weekly frequency as well as, end phase report toward Project Manager of the Beneficiary and with a monthly frequency/or if necessary, more often, toward Steering Committee of the Beneficiary. Simultaneously, the Bidder should provide an adequate level of transparency in project management through adequate documentation of all project management aspects.

ID	Requirements
PM 1.11	The Bidder's Project Manager has the authority and responsibility to manage the day-to-day activities of the project.
PM 1.12	The Project Manager of the Beneficiary has the role to organize the Beneficiary's resources so that they are useful to the project and available as needed to the Work Plan. The Project Manager of the Beneficiary should provide an official interface of communication of daily issues and of reporting regarding project progress between the Project Manager of the Bidder and Beneficiary.
PM 1.13	Other key proposed staff members may be appointed as Team Leaders by the Bidder, having the role of an intermediary in the communication and control process. The Beneficiary should appoint one or more members of those teams made by the Bidder. This will facilitate communication between the parties and will minimize official contact points between the teams. The primary responsibility of a Team Leader is to ensure the achievement of deliverables under the conditions set by the Project Manager of the Bidder.
PM 1.14	The Bidder should ensure timely resolution of identified issues related to its direct responsibility and should include in its proposal a description of the mechanism of escalation/resolution of identified issues.
2. Activities and deliverables requirements	
PM 2.01	**Main activities:** 1. Provide an initial project management plan covering at least the following initial items: Work Plan (phases, milestones, duration, responsibilities etc.), quality management plan, risk management plan, resource management plan, change management plan, communication plan and samples of reports. 2. Adjust the initial project management plan, based on an agreement with the NBM. 3. Adjust the project management plan on a need base during the project timeframe, based on an agreement with the NBM. 4. Organize the kick-off meeting and the project meetings (e.g., Steering Committee meetings etc.) together with the NBM. 5. Execute and monitor the project and provide weekly, monthly and end phase project related reports in a format agreed by the parties. 6. Close the major project phases and provide the draft of the acceptance documents to the NBM prior to formal acceptance.
PM 2.02	**Deliverables:** 1. Initial project management plan. The detailed requirements for the project management plan are listed below (PM 3.01). 2. Updated project management plan. 3. Support presentation for the kick-off meeting and for other project management meetings, such as Steering Committee presentations. 4. Weekly reporting should comprise a report on the status of the project (including decisions that need to be taken at project management and/ or Steering Committee level), list of issues to be discussed, risk register, changes register. The Bidder should include in its proposal the models for each of these reporting items. The weekly reports should comprise at least the followings: date, reporting period, implementation schedule status, performed activities, completed deliverables, identified issues and risks, deliverables to be completed during the next reporting period, changes and their impact analysis. 5. Monthly reporting should comprise a report to Steering Committee and should contain the following: the overall picture of the project progress over the management period, the overall picture of the Work Plan for the next period, the risk analysis, the state of the problems and their impact etc.

ID	Requirements
	6. End of phase reports should contain the followings: overview of the completed phase, overview of the Work Plan for the next period, risk analysis, state of project issues, project quality register. 7. Exception Reports should contain the following information: description of the causes of deviations, the impact of deviations, proposed problem-solving options and their impact on the general tolerances of the project, recommended option by the Project Manager of the Bidder.
PM 2.03	**Acceptance criteria:** 1. The deliverables are provided to the NBM. 2. NBM has no objections regarding the completeness and correctness of the document in accordance with quality and other agreed criteria.
3. Project management plan requirements	
PM 3.01	The Bidder should submit as part of its proposal the initial version of the Initial Project Management Plan. The Plan should include the following sections: *a. Project Management Approach*: i. General management approach (methodology and tools used, own team or subcontracting etc.); ii. Project deliverables and other expected results; iii. Constraints; and iv. Key success factors *b. Project organizational chart*: organizational chart *c. Major deliverables description* i. The deliverables description should cover: deliverable name and / or code, goal, content, format and presentation, person responsible for delivery, quality criteria for the deliverable and the how the quality will be tested by the responsible person, resources required for testing the quality of the deliverable. ii. The presented quality criteria should not be ambiguous and should be measurable. iii. Criteria for deliverables approval should be as follows - Compliance with requirements set for the deliverable. - The extent to which responds to the objectives of the project. - Performance indicators, as appropriate. *d. Quality management plan* *i.* The quality management plan should include - Responsibilities for quality assurance. - Reference to the standards to be met. - Identifying the key quality criteria to be achieved. - Control and audit methods for certifying the quality of project management deliverables and those technically specialized. - Other tools for quality assurance. *ii.* In order to record the quality controls to be made on deliverables, the Bidder should keep a Quality Register, which should contain the followings: deliverable, quality control method, results of verification, corrective activities, planned date and actual date of approval. *e. Resource management plan* *i.* The resource management plan should include for each proposed activity the resources (expressed in man-days) expected to be allocated by the Bidder, on-site and off-site, and number of persons by categories to be allocated, describing the functions and duties of each team

ID	Requirements
	member of the Bidder and the estimated workload for each task for each staff category. *ii.* The resource management plan should include for each proposed activity the necessary resources to be allotted by the Beneficiary, describing the functions and duties of each team member of the Beneficiary and the estimated workload for each task for each staff category. *f. Change management plan* *i.* Change management plan should treat the situations that might appear due to scope change, including scope extension, using the resources reserved for this purpose, or when the Bidder will propose solutions to individual requirements that NBM does not believe are satisfactory. Any such NBM reservation should be announced to Bidder and be subject to the governance and escalation process, according to the rules of change control. For this purpose: *ii.* The Bidder should provide a change process map and should describe the process - the steps, roles involved and templates to be used, including the mechanism of identifying/ monitoring/ reporting/ approving/ rejecting change requests, responsibilities and escalation procedure. *iii.* The Bidder should also include an impact analysis in the change process. *iv.* The Bidder should provide an example of change requests register. *g. Communication plan* *i.* The communication plan refers to the interactions between the Beneficiary's Project Manager, the Bidder's Project Manager and other project stakeholders. *ii.* The communication plan should comprise: - identifying the project stakeholders - information needed for each group of stakeholders - information source - frequency of communication - content of the communication - persons responsible for the development and transmission of communications *h. Project controlling and monitoring mechanism* *i.* Description of the way the project monitoring & controlling will be performed during the project (e.g., Reporting mechanisms – weekly and monthly, end of phase, in exceptional circumstances. *ii.* Description of weekly/monthly reporting model. *iii.* The procedure for handling project deviations and exceptions. *iv.* Contingency plans. *i. Approval plan:* should present in a condensed form each type of deliverable and the way this deliverable is approved. *j. Project library*: description of how the project documents and deliverables will be stored, found and retrieved. *k. Annexes:* should present models of documents representing each step of project management (minutes, examples of registers, questionnaires, weekly, monthly and end phase reports).

5. Conditions for warranty, maintenance and post-implementation support

5.1. The scope of post-implementation maintenance and support services is to ensure for the NBM the following objectives:

a. The functionality provided by the application should be timely aligned with the NBM changing business needs;
b. The incidents and the problems occurred during the use of solution should be addressed and resolved in a timely manner with minimal impact on the NBM activity;
c. The difficulties in using the solution should be properly and timely solved, as agreed between parties.

5.2. To achieve these objectives, the post-implementation maintenance and support services are going to be provided by the Bidder in compliance with the requirements from *Table 7*. This section is only for informational purposes, please refer to Section 10 which provides the full template that will need to be completed as part of the Technical Proposal.

Table 7: Post-implementation requirements

<table>
<tr><th>ID</th><th>Requirements</th></tr>
<tr><td>MnS 1</td><td>As part of the initial contract for the delivery and implementation of the solution, the Bidder should provide a warranty period, which involves the provision of support services and maintenance services for a period of 12 months from the date of final acceptance of the solution, including 500 man-hours for change requests.</td></tr>
<tr><td>MnS 2</td><td>Maintenance and support services should be provided on basis of a Service Level Agreement, which should be attached to the contract signed between the Parties. The agreement should establish the post-implementation maintenance and support services level, based on the following minimal requirements:
a. Support days: 5 business days per week
b. Support hours: 09:30-15:00, UTC+2 (Chisinau local time)
c. Response Time (RT) and Solving time:
<table>
<tr><th>Classification of the NBM request*</th><th>Response Time (RT)</th><th>Solving Time (ST)</th></tr>
<tr><td>Critical</td><td>3h</td><td>6 h</td></tr>
<tr><td>High</td><td>5 h</td><td>1.5 days</td></tr>
<tr><td>Ordinary</td><td>1 day</td><td>4 days</td></tr>
<tr><td>Low</td><td>3 days</td><td>The best effort</td></tr>
</table>
* NBM requests for post-implementation maintenance and support services are classified in terms of their importance for the NBM. The importance for the NBM is estimated by the impact (inflicted or potential) of the event that has created the need for the request on the quality parameters of the solution operation.</td></tr>
<tr><td>MnS 3</td><td>The Bidder should have a customer support center where all requests from the NBM will be directed to. The work program and organization of the Support Center should ensure post-implementation maintenance and support services at the level established in this RFP.</td></tr>
<tr><td>MnS 4</td><td>The Support Center should be contacted at least by the following means: e-mail, phone, web etc.</td></tr>
<tr><td>MnS 5</td><td>Maintenance and support services should be provided remotely.</td></tr>
<tr><td>MnS 6</td><td>For the provision of post-implementation maintenance and support services, the Bidder should provide NBM with access to a ticketing solution, available through the Internet. The ticketing system should be properly secured. All interactions between the Bidder and the NBM while</td></tr>
</table>

ID	Requirements
	providing post-implementation maintenance and support services should all be carried out by means of the respective platform.
MnS 7	NBM expects the proposal for post-implementation maintenance and support services will be based on best practices for Project Management and IT Service Management (e.g. ISO 20000, ITIL).

Section 5. Milestones

The following table provides the major milestones for the AML Software Solution, which correspond to the phases described in Project Implementation Requirements (*Section 4, Table 5*).

Output	Estimated Due Date*
1. Completion of analysis and design phases as outlined in IS 1.03	TBD
2. Completion of implementation/construction phase as outlined in IS 2.03	TBD
3. Completion of training and testing phases as outlined in IS 3.03 and IS 4.03	TBD
4. Completion of go-live phase as outlined in IS 5.04 and IS 5.07	TBD
5. Final acceptance including a six-month run during the warranty period	TBD

**Actual dates will be identified during contract negotiations with IDG.*