Co-funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of Europe

EU/CoE Horizontal Facility for Western Balkans and Türkiye – Phase III

Action against Economic Crime in Montenegro

APPENDIX I OF THE CONTRACT

Technical Specifications of the extension of the Case Management System of the Montenegrin Police Directorate – Department for Prevention of Money Laundering and Terrorist Financing

TABLE OF CONTENTS

ABBREVIATIONS

DPMLTF	Department for the prevention of money laundering and terrorism financing.
FIU	Financial intelligence unit
CoE	Council of Europe
HW	Hardware
Xml	Extended mark-up language
CAS	Case administration system
ERS	Electronic Reporting System
HA	High availability
STR	Suspicious Transactions Reports
GG Core	Government Gateway Core
CTR	Cash Transactions
CMS	Case Management System

1 Executive Summary

This technical paper aims to review and evaluate the terms of reference and the technical specifications prepared by the Department for the prevention of money laundering and terrorism financing (DPMLTF) regarding the establishment and maintenance of the institutional software system and hosting infrastructure upgrade.

The Department for the prevention of money laundering and terrorism financing (DPMLTF) serves as Financial Intelligence Unit of Montenegro. It generates quality operational and strategic analyses, which are widely used by the competent authorities to investigate money laundering and associated predicate offences, as well as for preliminary investigation of financing of terrorism. The results of the DPMLTF's operational and strategic analysis support the law enforcement operational needs. Financial intelligence disseminated by the DPMLTF triggers and facilitates investigation of money laundering and associated predicate offences.

After conducting a series of face-to-face meetings with the institution and gathering all the necessary information and data, as well as a thorough desk work, this Technical Paper concludes that the requirements document is well-written and includes most of the important issues that DPMLTF faces.

DPMLTF staff has properly identified the project's scope, objectives and mapping user and organization needs in the requirements. Implementing the new system and its necessary infrastructure with complex information system allows DPMLTF to:

- Analyse large amounts of data, including transaction patterns, behaviour, and other risk factors, to identify suspicious activity and investigate potential cases of money laundering or terrorist financing;
- Monitor compliance with regulations, detect and report suspicious activity, and facilitate information sharing between regulatory agencies and financial institutions;
- Stay up to date with evolving risks and threats, as well as changes to regulations and best practices;
- Through introduction of advanced analytics, the system can help to identify patterns and trends that may indicate emerging risks and provide early warning of potential threats.

Overall, a complex information system is a critical tool for DPMLTF to effectively monitor and regulate financial transactions, identify and investigate suspicious activity, and mitigate the risks associated with money laundering and terrorist financing.

2 Analysis

2.1 Project scope and objectives

The Action against Economic Crime in Montenegro (AEC-MNE) aims to support the Department for the prevention of money laundering and terrorism financing. (DPMLTF) to enhance its new information systems to address the challenges that the Montenegro FIU's staff face in their daily work on analysing increasing information streams and needs for data.

The DPMLTF needs an enhanced information system to effectively monitor and regulate financial transactions to prevent money laundering and terrorist financing activities. New additional developments in the existing Case Management System will server to DPMLTF to:

- Enhancement in the existing information system allows the DPMLTF to analyse larger amounts of data, including other perspectives for more transaction patterns, subject behaviour, and other risk factors, to identify suspicious activity and investigate potential cases of money laundering or terrorist financing.
- Improving existing information system can lead to increased efficiency in operations. By streamlining new processes, automating tasks, and reducing manual data entry, employees can complete their tasks more quickly and accurately and Increasing the Institution Productivity.
- Data Accuracy: Improving data quality and accuracy is crucial. Inaccurate information can lead to costly errors and poor decision-making. Regularly updating and maintaining the system helps ensure data integrity.

Overall, enhancements in the existing information system are required for the DPMLTF to effectively monitor and regulate financial transactions, identify, and investigate suspicious activity, and mitigate the risks associated with money laundering and terrorist financing, by increasing the efficiency of data processing, enhancing the quality of analyses, and adopting a risk-based approach to AML/CFT.

To achieve above mention goals DPMLTF needs to enhance the existing Case management system with the following modules and functionalities:

- Development of the new functionalities in the existing portal that will allow electronic filing of the reports for the following categories of users as requested by the law:
  a. Sector of accounting, bookkeeping, and auditing
  b. Sector of production and trade, which includes reporting entities defined under Article 4 of the Law on Prevention of Money Laundering and Terrorist Financing.
  c. Gambling and betting sector.

The data from these new reporting agencies and users should be integrated in the existing CMS in DPMLTF and should allow generation of requested reports.

- New module aimed at enabling the verification of data from specific data tables consolidating data from several linked data sources. Such functionality should be available through the CMS and should generate the necessary reviews, reports, alarms, and notifications.

- Reporting module for generating monthly reports on the work of the financial intelligence unit.

2.2 Presentation of the relevant directorates / departments

2.2.1 Description of the Agency and the processes

The Department for Prevention of Money Laundering and Terrorism Financing (the “Financial Intelligence Unit”) is the organizational unit in the Police Administration working on the prevention of money laundering and terrorism financing.

FIU’s activities consist in receiving, collecting, analysing data, information, documents, and results of analysis on the cases of suspicious transactions inform and advise the competent state authorities and foreign financial intelligence units with the aim to prevent and detect money laundering and terrorism financing.

The Financial Intelligence Unit can request information from reporting entities, and as well can order the temporary freezing of a transaction and monitor the client, etc. Additionally, suspicious transactions are reported to the Financial Intelligence Unit. Other authorities authorized to monitor compliance with the key obligations under the AML Law in different areas include the Central Bank of Montenegro, the Insurance agency, the National Customs Agency, and the related inspectorates.

Based on the Under the AML legislation there are several entities that have the obligation of reporting: These include banks, financial institutions, payment services providers, insurance and reinsurance companies and intermediaries, etc. Also following any suspicious activity, the financial intelligence unit must be notified and will carry out an investigation or monitor the subject.

All Financial intelligence organizations need to organize the several processes they operate most and at the same time, keep records of business decisions and transactions to meet the demands of accountability. Digital transformation of society and digitalisation have the potential to bring immense opportunities to FIU workflows and in the quantity of data, data sources and information to be considered. There are increased needs for FIUs to use technology to solve a part of their day-to-day challenges.

Montenegro FIU processes run on information created by a great number of reporting authorities and other stakeholders. This information is created, collected, processed, distributed, stored, managed, retrieved, maintained, and disposed as an integral part of every business process and activity of the organization.

As per October 2021, FIU staff is assisted in their daily activities from a Case Management System with analytic capabilities to process vast volumes of data and information.

The Action aims to support the FIU in their processes and where the continuous improvement of information technology is considered especially important, in order to:

- *Increase efficiency*

FIU needs to streamline the repetitive manual process of collecting large volumes of unstructured data from a vast number of reporting entities. Automation and other digital initiatives allow combining and sorting of large volumes data and information from various sources and differently structured databases for subsequent analysis. As a result, FIUs can process more and better-quality data quickly.

- *Enhance quality*

FIU aims to prioritise Suspicious Transactions Reports (STRs) of higher investigative value for detailed and targeted analysis. FIU aims to make use of unsupervised data and text mining techniques and reporting, to better use the data received in STRs and various reports, to identify patterns, and to draw inferences based on the rules set by FIU. As a result, FIU can prepare analysis of higher quality.

- *Adopt a risk-based approach to AML/CFT*

As part of continuous improvement of their capacities, FIU aims to lay down the essential precondition for the implementation of a dynamic risk-based approach in FIU workflows. Better reporting tools can partially improve the process of risk analysis drawing from large volumes of unstructured data. These tools may enable FIU to identify emerging risks, which do not correspond to already known profiles, and to verify and adjust findings prepared based on traditional risk analysis.

- *Allow for better assignment of limited human resources*

Continuous enhancement of digital systems and tools in use by FIU save time of analysts in their daily tasks and activities such as data verification and sorting of large volumes of data and allow them to focus on more sophisticated analytical tasks. As a result, FIU can maximise the value of analysts’ tasks and improving the performance of the resources.

Based on the legislation for the prevention of money laundering and financing of terrorism in Montenegro, the DPMLTF fulfils the functions of the Financial Intelligence Unit in Montenegro to collect, administer, process, analyse and inform the competent authorities about criminal offenses of money laundering or financing of terrorism. It also works closely with partner Financial Intelligence Units internationally.

The Financial Intelligence Unit, as a central national agency, is responsible for receiving (and as foreseen, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:

- Concerning suspected proceeds of crime and potential financing of terrorism;
- Required by national legislation or regulations, in order to combat money laundering and terrorist financing.

The FIU was established as a connecting institution for the financial institutions, business community and the executive authorities, as well as with the aim to direct and coordinate the fight against money laundering, based on the obligation of the interested subjects and financial institutions, in order to identify the client, register and save the data, to report the (STR) and those going beyond decided thresholds (Cash transactions; CTR). This institution has its structures and the initial infrastructure established.

To fulfil its objectives, the FIU structures the collection of the information that is used to identify the money laundering/terrorist financing and criminal activities. Apart from the subjects identified in the law, the FIU also collects data from other sources such as the law enforcement authorities (police, border control, investigation and prosecution authorities); other regulatory authorities (customs, taxes and duties, banks authorities) and any other units that can provide necessary financial information. The FIU also coordinates the work for registering, analysing, and disseminating data to the competent authorities.

The Department for the Prevention of Money Laundering, acting as Montenegro FIU, is a member of EGMONT Group, which is an international forum that executes the collaboration in information exchange, training and experience sharing.

The FIU objectives in this direction are to concentrate on the reporting subjects who must start submitting the Reports on the Cash Transactions (CTR) and the Reports of the Suspicious Transactions (STR).

DPMLTF also has a supervisory role for the subjects of the law and their level of compliance with the AML/CFT legislation and in this regard, it cooperates with all supervisory authorities, especially with the Bank of Montenegro and the Financial Supervision Authority.

For Financial Intelligence Units, such as the DPMLTF, the submitted reports by reporting entities are essential, as they are followed by analysis, dissemination to law enforcement agencies, identification of ML/TF typologies and categorization of transactions involved. Current situation

Electronic Reporting System is part of the CMS (external portal) application that helps FIU to collect information from the reporting entities.

2.2.2 Details on existing Case management System

The DPMLTF employees as analysts and inspectors use a Case management System for their internal procedures, provided with the capacity to register, store and administer cases and documents.

Case Management Module enables the administration of cases, specifically*:*

- Registration and association of cases.
- Registration of persons/entities involved in the analysis of information.
- Registration of subjects.
- Research in reporting and data management within the practice.
- Administration within the case of requests for information.

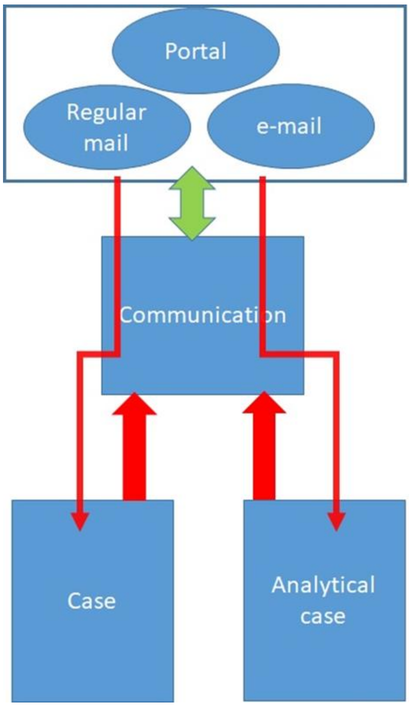

Figure 1:High-level communication flow within FIU CMS

FIU can receive information/documentation via three communication channels:

- Portal
- Regular mail
- E-mail

Information, documentation, or any documents produced by the FIU employees in the case resolution process are herewith referred to as "Communication".

Most of communication with reporting agencies and partners comply in:

- Communication on the basis of which an analysis (case) is opened or an analytical can be formed (i.e. suspicious transactions received from the reporting entity, etc.)
- Communication related to the already opened case or analytical case (FIU requests, responses to FIU requests, etc.)
- Communication on the basis of which an administrative case is opened (budgetary planning, public procurement documents, etc.)
- A communication that represents a notice
- Internal communication

Typical cases handled by FIU are:

- Analyse – On this type of case the information and documentation received is analysed thoroughly to decide whether is necessary an investigation/analytical case. It consist in analysing the available information documentation or documentation in FIU and as well administration of several requests for information and searches on available records of the related local or foreign agencies.
- Administrative Cases

- Information/Notice

2.2.2.1 CMS SOFTWARE ARCHITECTURE

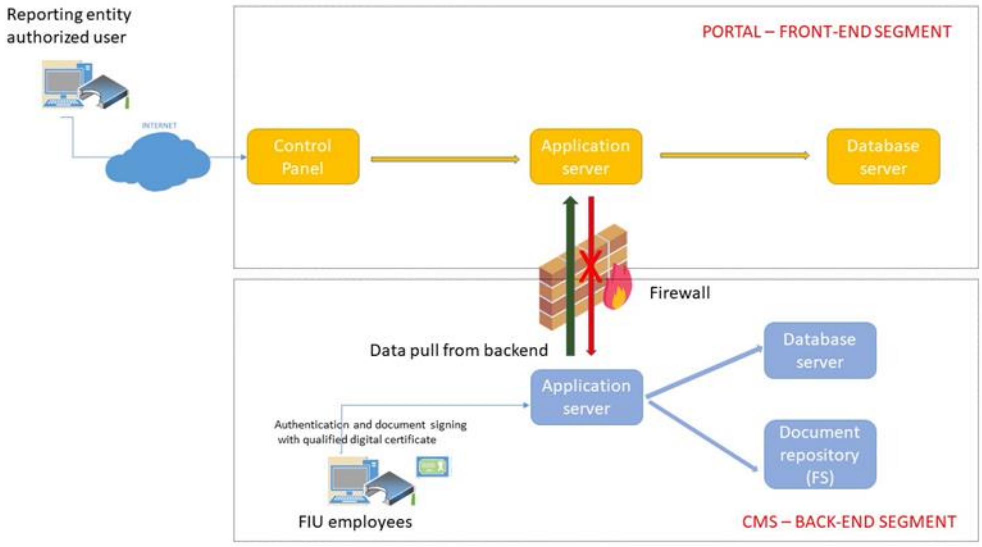

Figure 2:High-level CMS architecture

CMS consists of the front-end and back-end segment.

a. Front-end segment (Portal) is used by the authorized users from the reporting entities to electronically submit data and related documentation as requested by the law and legal framework. These users are authenticated, and they electronically sign submitted documentation via electronic certificated issued by the qualified certificate authorities in Montenegro (new eID). Due to the sensitivity of the information Authorized users from the reporting entities must have classified data security clearance to access the Portal or classified documents that can be received from the FIU in the paper form.

- Application server at the Portal segment processes application and the business logic and stores data in the Database server. Front-end servers are hosted in a DMZ (demilitarized network zone) protected by firewalls. The firewall facing the public allows only specific network protocols and ports that are necessary to access the Portal by authorized users.
- For security reasons the Application server at the DMZ serving to the public Portal, can't initiate connection or push data towards the Application server at the Backend segment. Connection between zones is managed (initiated, and data is pulled from the Application server at the Backend). Such design is intended to protect the inner part of the Case Management System in the case of cyber-attack and possible compromise of server(s) on the front-end segment.

b. Application server at the Backend segment processes application and business logic including internal user actions and stores data in the Database and electronic documents at the Document repository (file system). Authentication and Authorization for FIU employees is managed through electronic certificated issued by the qualified certificate authorities in Montenegro (new eID).

Network traffic between two system segments is protected by the next-generation network firewalls.

2.2.2.2 User roles in CMS:

Operator with the following functions:

- the operator does the necessary data entry and submits in the CMS. The information communications consist in different types as described above.
- forwards communications to the other user roles of the system.

Operator for international cooperation

- Submits in the CMS the communications.
- forwards communications to the other user roles as Head of the FIU or the Head of the Department. Communications consist in official mail, external mail or external communications (Siena, EGMONT, Interpol, FIU.net),

Head of FIU:

- this user role has insight into all communications, assigns communications to the Head of a department or group, has insight in all reviews and reports.

Head of department with the following functions:

- Review of the communications received through the Portal,
- review communications forwarded to him/her, to review
- review all communications related to a division, assign communications to an employee,
- opens a case, opens an analytical case, approves correspondence, adds and changes the officers in charge of a case, has insight into reviews, reports...

Head of Unit –

- review communications received through the Portal,
- Review communications forwarded to him/her, to review all communications related to a group,
- Assign communications to an employee,
- Opens a case,
- Opens an analytical case,
- Approves correspondence,
- Adds and changes the officers in charge of a case,
- Has insight into reviews, reports...

The user role chief of a department differs from and Head of unit user role because the chief of a Department has insight in work of all Department Units and Head of Unit user role can access only the information on his unit.

Analyst/inspector user role

- Can access information and insight into communications received through the Portal, insight into cases that are allocated to him/her;
- Access into all communications related to the cases assigned to him/her
- works on a case, has insight into reviews, reports.

- After analysing the information can suggest opening analytical report, or not following the case.

Administrator- This user role is used mainly by IT Unit and enables a centralized control of the administration functionalities as managing users, granting users rights, managing categorise of the information and other system parameters.

With implementation of CMS through two distinct zones (public and internal) the work of the FIU staff has been improved and the users, such as analysts, inspectors, and other employees can access a big part of the information in digital form and also manage their cases through the system.

2.2.2.3 Workflow

The workflow in the DPMLTF financial investigation unit typically involves several key stages, which are in general the same for such organizations and may vary slightly depending on the specific organization and their investigative procedures.

- *Identification of suspicious activity*: This stage involves the identification of transactions or patterns of behaviour that may be indicative of money laundering or other financial crimes. This may be done through the use of automated transaction monitoring systems, due diligence procedures, or other means of identifying potentially suspicious activity.
- *Investigation*: Once a suspicious activity has been identified, an investigation is typically launched to determine the nature and scope of the activity, as well as to gather evidence and identify any individuals or entities involved. This may involve conducting interviews, reviewing transaction records, analysing financial statements, and gathering information from external sources.
- *Analysis*: The information gathered during the investigation is then analysed to determine the extent of the suspected money laundering activity, as well as to identify any potential risks to the organization or the wider financial system.
- *Reporting*: If the investigation confirms that money laundering or other financial crimes have taken place, the AMLTF financial investigation unit will typically file a report with the relevant regulatory authorities, law enforcement agencies, or other stakeholders. The report will outline the details of the suspected activity, along with any evidence gathered during the investigation.

Finally, the AML financial investigation unit may take steps to remediate any issues identified during the investigation, such as improving internal controls, enhancing due diligence procedures, or taking other measures to mitigate the risk of financial crime in the future.

Throughout the entire workflow, AML financial investigation units must adhere to strict legal and regulatory requirements.

The implementation of the new systems has improved the quality of work for DPMLTF staff which is benefiting form:

- Decreases in paperwork because of digital record-keeping.
- Centralized data management.
- Close to Real-time updates and better access to information.
- More efficient resolution of cases.

- More effective collaboration.
- Increased transparency and clear audit trails.

2.2.2.4 Technology in use for the CMS components

In summary, the technology stack used for the CMS and Portal includes Microsoft SQL Server for the database layer, C# and .NET Framework for the middle layer, and a mix of web technologies for the Portal's user interface. Both components make use of CSLA.NET for their respective frameworks, and the CMS includes a desktop application with DevExpress controls. The Portal also provides a Web API for data download services. Below is a detailed list of technologies to be used in this procurement.

Case management System elements:

1. *Database Layer:*

Database Management System: Microsoft SQL Server.

Components: Stored procedures, User-Defined Functions (UDF), and Jobs

2. *Middle Layer:*

Programming Language: C#

Framework: .NET Framework 4.7

Communication Protocol: Services using Windows Communication Foundation (WCF)

3. *Client Libraries for External Client Services:*

Programming Language: C#

Framework: .NET Framework 4.7

Communication Protocols: SOAP client, REST services client, WCF service client

Framework: CSLA.NET

Application (CMS):

Type: Desktop Windows Forms Application

Programming Language: C#

User Interface Components: DevExpress v21.1 controls

Framework: CSLA.NET

4. *Portal:*

Database Layer:

Database Management System: Microsoft SQL Server.

Components: Stored procedures, User-Defined Functions (UDF)

5. *Middle Layer and Web Application:*

Programming Language: C#

Framework: .NET Framework 4.7

Web Application Framework: ASP.NET MVC 5

Framework: CSLA.NET

6. *User Interface on Web Pages:*

Technologies: JavaScript, KnockoutJS, jQuery JavaScript Libraries, HTML, and CSS

7. *Service for Downloading Data from the Portal:*

Programming Language: C#

Framework: .NET Framework 4.7

Web API: ASP.NET Web API

2.2.2.5 *Existing hardware infrastructure*

All systems in use by DPMLTF are hosted their [premises in a server infrastructure that has at least the following equipment:

Lenovo Blade chassis with 3 Lenovo Flex blade servers/virtualization hosts, redundant LAN and SAN FC modules and power supplies

- IBM Storwize V7000 storage system
- Backup LTO tape device
- 2 x data centre Juniper switches
- 2 x firewall Juniper devices

DPMLTF has a server room that respect the parameters in relation with security, physical security, temperature, and other specifications.

2.3 Future processes

2.4 Software new functions

The DPMLTF IT staff has done a comprehensive analyse of functions in the organization and comparing the ability of the existing solutions that are being used in the organization. To improve the effectiveness and efficiency of work, the DPMLTF staff has several needs that are not matched by the existing system. Introduction of such new features and development will decrease the manual work done and will save precious time.

More specifically there are needs for improvement in all components, such as:

- In reporting from new reporting users as requested by law.
- In enhancement in the Case management and administration system to accommodate and process the new information.
- Enhancement of data synchronisation.
- In Automated reporting and analytics for the usage of the system.

Such new development might need interoperability with the external systems (business and civil register). External registers are administered by different agencies, but interoperability is already in use for other existing functionalities in the system.

Due to the necessary enhancement and improvements in several functionalities, the EU/CoE Horizontal Facility for Western Balkans and Türkiye – Phase III, Action against Economic Crime in Montenegro Project will help DPMLTF with a procurement procedure considering development of additional functionalities mentioned in more details below.

2.5 New development details

DPMLTF needs additional functionalities in their existing CMS to be compliant with the law an as well to improve work processes within the agency.

New development will consist in:

1. Additional E-filing capacities

Additional functionality in the portal aimed to assist e-filing of the data forms and electronic questionnaire for data created by authorities and agencies supervising:

- Sector of accounting, bookkeeping, and auditing
- Sector of production and trade, which includes reporting entities defined under Article 4 of the Law on Prevention of Money Laundering and Terrorist Financing.
- Gambling and betting sector.

It is necessary to expand the existing Portal's e-filing functionalities in implementing data validation and control elements. The data forms are and will be implemented based on well-defined questionnaires prepared by DPMLTF. For each new reporting unit will be used specific data forms and questionnaires.

The e-filing module should be provided with the necessary control instruments for the data entry forms and fields to assist the process, users and validating the information before submission. E-filing module should exchange (receive) data using the existing web services for Central Business Registry (CBR) and Central Population Registry. Such web services are already used in another functionalities within CMS.

Based on the reporting user type, the e-filing module should redirect the user to the specific questionnaire (data form) for the sector to which the user belongs.

The module shall enable temporary storage of data entered in the questionnaire, as well as their review and modification. On the process of the completion of the forms, users shall have the possibility to save as draft submission. On the submission of the data by the reporting user and confirmation of receiving it, further changes on the information should be disallowed. Based on the permission from DPMLTF the system can allow in the users in a later phase to review and correct data on the questionnaire and/or to enter a new questionnaire.

The module and the forms shall be provided with the internal risk calculation logic based on the data entered. The details of the risk calculation process will be provided to the contractor by DPMLTF.

The reporting supervisory authorities should have the possibility to access (view) the data gathered from the questionnaires, grouped by the companies or the reporting sector to which it belongs, including the parameters related to the risk categories (these categories are recognized in the questionnaire).

The portal should also enable a specific group of users to log in based on username and password. This group refers to REs that are outside of Montenegro and cannot use the legal Montenegrin authorization and authentication method.

All functionalities of the existing Portal should be also applied onto the new development.

2. Data analytics and reporting (for the new development)

An additional module in CMS, to analyse the received information and generation of necessary reports. The data collected through the e-filing module (data forms and questionnaires) should be processed in CMS. Processing of the information received should consider weighting and the method of risk calculation for each question of the questionnaire and for each group of questions related to a certain type of risk. Based on weight and calculation methods of entered data, the new development for processing and generating reports should be implemented to achieve the following:

- To enable the visualisation in CMS of all entered data (legal entity, sector of the legal entity, risk group, risk parameters, all entered elements from the questionnaire concerning risk (for example countries with which tit cooperates, risky countries, number of employees, size of the legal entity in comparison to profit, etc.).
- To enable the generation of reports and their export in .xlsx, .pdf. formats.

The supervisory authorities should also have possibility to access (view) the reports for the data and information related to their scope.

3. Enhanced Data Synchronization

For this new development the contractor shall develop or configure connectors for each external data source in function to sync with. These connectors should be capable of connecting to and retrieving data from various types of sources, such as APIs, databases, web services, or flat files. It should implement a mapping system that associates subjects or data categories in the database with their corresponding counterparts in external data sources. This mapping should define how data is retrieved and integrated into the database.

The contractor should create a scheduling mechanism to automate the synchronization process considering that can be used cron job, task scheduler, or a built-in scheduler within the system to specify when and how often updates should occur (e.g., daily, weekly, or custom intervals). Also new developments should be carried to apply data transformation and validation rules to ensure that the incoming data aligns with existing database's schema and quality standards. This step may include data cleansing, transformation scripts, and data visualisation within the structure of the existing CMS.

A notification mechanism should be developed to alert administrators or relevant users when synchronization processes fail or when critical issues arise during the data update. Also, this module should be provided with the necessary means for Logging and Auditing to maintain comprehensive logs and audit trails of the synchronization processes. This shall allow for troubleshooting, historical data tracking, and compliance purposes.

4. A module for FIU’s activities Reports

DPMLTF needs to improve reporting over internal and external activities. It is necessary to create a module in which the entered parameters will be the period for which the report is requested (date from and date to), and the result is a generated report on the FIU’s work for the selected period.

The report should include at least but not limited to the following:

- Number of open cases by initiators
- Reported STR, SAR and CTR by reporting entities
- Data on cooperation with other state authorities and foreign FIUs (number of cases opened on the initiative of other authorities or foreign FIUs, number of data delivery requests, number of additional data requests, number of requests received, number of responses sent onto requests received...)

- key indicators of FIU's work

- Number of open cases,
- Number analytical reports forwarded,
- Number of additional analytical information forwarded,
- Number of requests for ongoing monitoring of the client's financial operations,
- Number of orders for temporary suspension of transactions,
- Number of natural/legal persons in orders for temporary suspension of transactions, Total value of suspended funds)

- Case description for cases which analytical reports are disseminated
- Performance volume for individual FIU officers.

2.6 Business requirements

2.6.1 List of main Requirements

Requirements have been grouped into the following tables.

- Table 1: shows the general business requirements for this procurement.

The Bidder shall commit to every function/requirement in the given tables of this document and enclose the completed tables in their Bid. The required functions/requirements marked with the letter „R" must be met. The requirements/functions that are optional, but desirable, are marked wih the letter „O" . Depending on whether the required or optional functions/requirements are met, the Bidder shall circle the appropriate mark „R" or „O". In addition, in the column „Bidder response" the Bidder must state how the function/requirement will be met, by using the following marking system:

Bidder response	Description of how the requirements shall be met
A	Exists as a function and is already implemented with at least one client – may be presented on the client's premises
B	Exists as a function, but not implemented with any client – may be presented on the Bidder's premises
C	Function requires little modification /programming and may be realized in a set time limit
D	Function cannot be met

All the functions marked by the Bidder with A, B and C are the subjects of delivery and the Bidder must deliver these within the bid-price.

The Bidder must enclose a functional specification in their Bid, i.e. a description of the bid software solution, and other relevant accompanying documentation that describes the bid solution.

The total number of functional requirements is 33, of which 33 are required.

Table 1: General business requirements

No.	Category	Requirement	R/O	Bidder's Response
1	User Registration	User registration with personal and professional information.	R	

	and Authentication			
2	User Registration and Authentication	User authentication through secure login credentials (username and password).	R	
3	User Roles and Permissions	Define different user roles (e.g., accountant, AML compliance officer, administrator).	R	
4	User Roles and Permissions	Assign role-based permissions to control access to specific features and data.	R	
5	Dashboard	A user-friendly dashboard that displays relevant notifications, task lists, and recent reports	R	
6	Dashboard	Quick access to commonly used features and actions.	R	
7	Report Submission	Capability to create and submit both periodic and ad hoc AML reports.	R	
8	Report Submission	Input forms with fields for required AML information, such as suspicious transaction details, customer data, and transaction history.	R	
9	Report Submission	Ability to attach supporting documents, evidence, or files to the reports.	R	
10	Report Review and Approval	Workflow for report review, where designated personnel can review and approve reports.	R	
11	Report Review and Approval	Option to include comments or annotations during the review process.	R	
12	Report Review and Approval	Notification system to alert accountants when a report has been reviewed.	R	
13	Compliance Checks	Integration with AML compliance databases and watchlists for real-time subject screening	R	
14	Compliance Checks	Automated checks for suspicious transactions, customer profiles, and risk assessment.	R	
15	Report Tracking and Management	A central repository to store and organize submitted reports using DPMLTF standards.	R	

16	Report Tracking and Management	Search and filter options to quickly locate specific reports based on criteria like date, subject name or status	R	
17	Report Tracking and Management	Archive and historical access for auditing purposes.	R	
18	Notifications and Alerts	Automated notifications for deadlines, pending approvals, and compliance alerts.	R	
19	Notifications and Alerts	Alerts for any suspicious activity or potential AML violations.	R	
20	Data Security and Encryption	Secure data transmission and storage using encryption protocols.	R	
21	Data Security and Encryption	Role-based data access control to protect sensitive information.	R	
22	Audit Trail	Comprehensive audit trail to log all user actions and system activities.	R	
23	Audit Trail	Exportable logs for compliance and audit purposes.	R	
24	Reporting and Analytics	Generate and export summary reports on AML activities and compliance status.	R	
25	Reporting and Analytics	Analytical tools to identify trends and patterns in submitted reports.	R	
26	Integration	Integration with financial systems and databases for streamlined data retrieval.	R	
27	Integration	API support for data sharing with regulatory authorities.	R	
28	Training and Support	User training resources and documentation.	R	
29	Training and Support	Helpdesk or support ticket system for user assistance.	R	
30	Compliance Documentation	A repository for storing compliance policies, regulations, and reference materials.	R	
31	Mobile Accessibility	Responsive design to ensure usability on various devices, including smartphones and tablets	R	
32	Scalability	The system should be able to handle a growing number of users and reports.	R	
33	Backup and Disaster Recovery	Regular data backups and a disaster recovery plan to ensure data	R	

		integrity as per existing DMPLTF rules on the issue.		

2.7 Project implementation and realization requirements

Due to the sensitivity of the data and information processed by FIU, the Supplier needs to adhere to the following main conditions:

- The Supplier shall conduct software development only in the DPMLTF's premises and on the development environment that is installed on the equipment owned by DPMLTF, between the following working hours: 7.30 AM - 3PM.
- Thoroughly test Software, including, but not limited to, all its subsequent releases/editions, subsequent upgrades, enhancements and subsequent versions. This must be documented in written form and it should include detailed description of tests, the manner of conducting tests, test results and List of program errors and important issues. Plans for testing must be reviewed by DPMLTF in order to ensure that quality standards are maintained. transfer its entire right, title, and interest in anything created or developed under this Contract including all patents, copyrights, trade secrets, and other proprietary rights.
- Execute and aid in the preparation of any papers necessary or helpful to obtain or maintain any patents, copyrights, trade secrets, and other proprietary rights under this Contract.
- Handover the source code for an unlimited use without copyright restriction and Installation of development and testing environment to DPMLTF on optical medium. The Source Code is ownership of DPMLTF.
- The Supplier’s obligation is to submit a proposal for Functional acceptance tests for each phase.
- The format of the Functional acceptance tests should be as follows:

The obligation of the Supplier is to guarantee that no part of the Software or documentation, covered by this Contract, shall contain the protection feature designed to prevent the use of the Software. This includes, but not limited to, any computer virus, worm, software lock, drop dead device, Trojan-horse program, trap door, time bomb or any other code or instruction that can be used for assessing, modifying, deleting, damaging or disabling the User Software or computer system. The Contractor is obliged to transfer ownership of the Source Code for the Application as well as physically deliver the source code to the Police Department

The Supplier shall compensate and enable integrity to the DPMLTF from complaints or activities of any or all third parties, including losses, expenses, responsibilities, real compensations for a lawyer and other expenses that may occur form such complaints and activities, where the reason is that the Software infringes or violates the copyright, brand, patent or business secret of a third party, on the condition that:

- DPMLTF immediately informs the Supplier in written on any complaints;
- The Supplier has a sole role of defending from any such complaint and all to carry out all the negotiations for reaching an agreement or compromise;
- DPMLTF shall ensure reasonable cooperation with the Contractor.

In any activity based on the complaint for violation, the Supplier has, at his own expense, (i) obtain for the DPMLTF the right to continue using the Software, or (ii) replace or modify the Software with the Software that does not cause violations but it ensures the same functionality.

2.8 Project Schedule

The period of project implementation and realization must not be longer than 180 calendar days.

The Bidder shall give details of their suggested methodology of implementation, as well as the most detailed plan of project realization possible with all its relevant activities, performers of activities, deadlines, and potential bottlenecks and key points. It is expected that the Supplier offers a plan of the implementation realization of the software solution in phases:

- Inception report;
- Analysis;
- Design;
- Software solution development;
- Implementation of production environment
- Implementation of testing environment;
- Testing of software solution;
- Producing the as-built documentation, project documentation and user instructions;
- Completed training of administrators and system users;
- Establishment of production environment;
- Production.

The Bidder shall also compile a list of potential risks that can jeopardize the project realization, as well as suggestions for their minimization/elimination.

Upon signing the contract, the Ordering Party will send the Supplier the following set of documents:

- System architecture
- Description of workflows (including the existing documentation and forms that are currently being used),
- Printed glossary of data – containing exact data sets regarding the equipment from the subject of the bid to be conducted in the new system.

It is expected that this set of documents will contribute to a faster and more effective phase of Software Solution Development Analysis.

In accordance with the characteristics, available functionalities, and options for expanding the chosen software solution, and all this in agreement and collaboration with the Supplier, the Ordering party will also define in detail the new processes that will be the basis for the complete realization of the software solution.

In establishing the system environment and necessary infrastructure, FIU's appropriate technical service will play a significant role.

Below, the graphic of the project implementation is shown, according to the respective phases:

No.	Phase Description	M1	M2	M3	M4	M5	M6
1	Analysis/ Requirements gathering	■					
2	Delivery of detailed requirements document.	■	■				
3	Development and deployment			■	■		
4	Integration and testing					■	
5	Acceptance and closure						■

2.9 Out of Scope

The hardware necessary for the extension of the existing CMS is not part of this procurement.

This document is a requirements document prepared for Montenegro FIU. Due to the high sensitivity of the information in this document the functions are mentioned in high level without many details.

2.10 Project Risks

The purpose of risk identification and assessment is to enable avoidance or mitigation and it is essential that unacceptable risks are mitigated by senior management prior to project commencement. Beyond this, risks and threats should be continually evaluated throughout the life of the work. List here the risks identified during the business requirements phase. For each risk, indicate its probability, impact and possible mitigation measures.

Probability reflects how likely a risk is to materialize and Impact indicates the magnitude of exposure represented by the risk (from 1=Low to 4=High). Overall rating reflects the combination of probability and impact. By definition, unacceptable risks are almost certain to occur and will severely impact, if not prevent, completion of the initiative.

Category	**RISK**	**Impact**	**Probability**	**Overall gravity**	**Proximity**	**Current Mitigation**	**Assigned to**
What type of risk is this risk is?	RISK TITLE in capitals followed by the risk description (Risk is a specific situation in the future which is undesirable, can be	Severity of the risk occurring (from	Likelihood of the risk occurring (from	Overall rating reflects the combination of	When is the risk likely to occur	Specific measures in place to counter the risk	The person appointed to keep an

	avoided or mitigated and is measurable)	1=Low to 4=High)	1=Low to 4=High)	Probability and Impact	(in X months)		eye on the risk
Infrastructure	Server infrastructure not ready to	4	2	8	2	Coordinate the projects to synchronize the timeline Or FIU should consider cloud	Project Manager
Infrastructure	SERVER ROOM CONDITIONS In case of transferring the platform in FIU premises - Lack of the appropriate environment and conditions of the Server Room where the hardware equipment will be located.	3	2	6	1	A site survey is necessary to be done in the very beginning of the inception phase, after the contract signing between Contractor Authority and Bidder.	Project Manager, IT Staff
Participation	DISENGAGEMENT OF KEY ACTORS - such as the availability of the FIU staff, the availability of the staff of the Bidder developing the FIU software that this infrastructure will host and the availability of the Bidder staff that will implement the hardware infrastructure.	4	2	8	1-4	Organize frequent meetings, keep Minutes of Meetings for documentation reasons. Follow best practices in software development.	Project Managers form company and from FIU

Stakeholders	STAKEHOLDER CONFLICTS - Disagreement between stakeholders over project issues.	4	2	8	1-4	Identify issues as soon as possible, in the very beginning when they may be identified. Discuss issues immediately with all the stakeholders involved and document minutes of meetings.	Project Manager, Project Team from FIU and Bidder.
Communication	MISUNDERSTANDING - Project team misunderstands requirements.	4	2	8	1	Organize and keep track of the project initiation meeting with all the necessary stakeholders. Organize periodical meetings for the status of each phase of the project. Organize meetings for requirements gathering and discussion between stakeholders. Require the Inception	Project Manager (from FIU and Bidder)

						Report from the Bidder after the gathering of the requirements.	
Resources	INEXPERIENCED RESOURCES - Resources who are just out of school or who are new to your industry or profession tend to make more mistakes and be less productive.	4	1	4	1-4	Careful Evaluation of the team resources qualifications and experience.	Procurement Team

2.11 Verification/Acceptance

Verifying the success of the completed phases of implementation and testing of the software solution shall be carried out by a professional commission consisting of a Supplier's consultant, and a person to be appointed by FIU.

The exact list of team members that will monitor the implementation of the PLATFORM, manner of testing and reporting will be defined in the inception report.

The elements of delivery which the Bidder must complete are:

- Software solution which meets all the agreed functional requirements on the required technological platform
- Training of internal users
- Launching the new solution into production work
- Production work of the new solution with good, acceptable performances
- Project and user documentation and instructions

The software solution that fulfils all the agreed functional requirements on the required technological platform will be verified as follows: the Supplier will carry out a presentation in a testing environment to the relevant representatives of the Ordering party, their advisors (the supplier of the study) and representatives of CoE where they will directly see and confirm that all agreed (functionality and content), has been executed and completed by the Supplier. A written protocol shall be made, serving as proof of the completion of the contractual obligations by the Supplier.

2.12 Training verification

For the training verification it is necessary that the Bidder:

- Develops the training program based on the requirements listed in this Technical specification,

- Completes the training of all the course trainees,
- Devises tests for the trainees which all the trainees must pass,
- Performs the testing of trainees (in the conditions which the Ordering Party must establish), supervised by the consultant.

Training is verified when all the requested trainings are completed and the testing of all the trainees is carried out. The obligatory condition is that all the trainees pass the test with a minimum of 85% of completed tasks predefined by the minimum percentage of solved tasks. The minimal percentage of solved tasks is defined by the project coordinator from FIU, in collaboration with a consultant. A written protocol will be made, serving as proof of the completion of contractual obligations by the Supplier.

2.13 Verification of launching the solution into production work

Verification of launching the new solution into production work is ascertained by performing Functional Testing and User Acceptance Testing (UAT). A written protocol will be made thereof and it will be used as proof of the completion of contractual obligations by the Supplier.

The verification of the production work of the new solution with good, i.e. acceptable performances is ascertained by measuring the response of the application solution on an application sample chosen by the Ordering Party (Performance and Stress Testing). The measuring of the response will be performed in production conditions and in the period chosen by the Ordering party and in the presence of the Supplier and consultant. The measuring of the application solution response will also be performed in the intranet, at a minimal throughput of 10 Mbps, at a given workstation. A written protocol shall be made thereof, serving as proof of the completion of the Supplier's contractual obligations.

All the project and user documentation must be in **the Montenegrin and English language**.

2.13.1 Project documentation

Project documentation shall include:

- Logic data model;
- Physical data model, i.e. a complete database scheme (which includes all the objects in the database);
- Functional model of the system, with a description of each function;
- Model of roles, as a method of controlling data access;

2.13.2 User documentation

User documentation shall include:

- General instructions for using the application, i.e. user interface;
- User instructions (manual) for each of the installed and used modules, i.e. functions;

Verification of project and user documentation and instructions is ascertained by the delivery/availability of their electronic versions (*Word, HTML and*/or *pdf* files). A written protocol will be made thereof, which will serve as proof of the completion of the Supplier's contractual obligations.

2.14 Warranty and system maintenance

The Bidder must include in the price the maintenance of the information system with a warranty period of at least 6 months, which will secure the normal operation of the application and database. The warranty period begins with the date of acquisition (delivery and acceptance) of the information system.

Note: Bids with a warranty period shorter than 12 months will not be accepted.

As security for enabling the normal functioning of the information system within the

If the Bidder fails to meet their obligations and deadlines stipulated in the technical specification, the Ordering Party has the right to activate the promissory note submitted as a guarantee of the completion of their obligations within the guaranteed period.

The Bidder must specify the price for the annual maintenance of the offered solution for every year following the offered warranty period for 1 year.

Upon the completion of the project, the Bidder is expected to continue to perform the following:

1. After receiving a written notification from the Client regarding the irregular functioning of the software solution, they must identify the problem, fix the problem/make an intervention so the programs can function correctly, or recommend how the problems can be overcome.

2. All the irregularities in the functioning of the software that impact FIU's capacity to use the system productively must be eradicated within 7 (seven) calendar days; more serious irregularities must be eradicated within 2 (two) working days.

3. The Bidder must expand or enhance their smaller solutions, as requested by the Client and which are the subject of this procurement, which includes alterations of the existing and the creation of new reports, minor changes in the data entry application, modifications and viewing, and change in the data access policy. "Minor changes" are defined as engaging the supplier up to 2 (two) days per month, with no additional charge.

4. To expand and enhance their solution at the Client's request (major intervention) which are the subject of this public procurement, and to create/modify the user documentation and to offer training to all the relevant users, with additional payment.

5. To perform additional training of users (whether new or current) regarding issues and areas which are specified and particularly requested by the Ordering Party, with additional payment.

Annex 1: Table of Fees

Below list specifies the expected deliverables and their corresponding deadlines. Prices are indicated in Euros **without VAT**, payable in local currency. ***Tenders proposing a total fee above the exclusion level will be entirely and automatically excluded from the tender procedure.***

Table 2. Table of Fees

Deliverables ▼	Deadline for delivery ▼	Fees ▼	Exclusion level ▼
1. Clarify and refine the functional requirements of the application based on the Technical Specifications indicated in the Appendix 1 of the Contract, which includes: i. A module for completing an electronic questionnaire prepared by the supervisory authority for: a) Sector of accounting, bookkeeping, and auditing activities; b) Sector of production and trade, encompassing entities under Article 4 of the Law on Prevention of Money Laundering and Financing of Terrorism; c) Sector of gambling and betting. ii. A module for analysis and report generation based on the collected data from the requirements outlined in the first module. iii. A module for cross-referencing data entered into dedicated tables with information from all sources available through the Case Management System, and generating essential overviews, reports, alerts, and notifications; iv. A module for generating monthly reports on the activities of the Financial Intelligence Unit (FIU)	20 October 2024		
2. Develop and upgrade the software solutions, including the testing of the software solution.	1 December 2024		
3. Finalise the development of the new modules and upgrade, following the feedback received from FIU and the findings of the testing phase.	15 January 2025		
4. Establish the production environment, integration, testing and production to the FIU.	15 February 2025		
5. Deliver one training for the responsible FIU staff and key users of the platform and revise accordingly the operations' manuals for the online platform.	1 March 2025		
6. Putting the software solution into production use.	20 April 2025		
	TOTAL ►		**50000**