ANNEX 1 – SCHEDULE OF REQUIREMENTS

Terms of Reference

RfQ/02488: Company to deliver quality assurance services during the implementation of the Forensic Case Management System of the Republic of Moldova

A. Project Title *"Strengthening Efficiency and Access to Justice in Moldova"*

B. Project Description

The UNDP project "Strengthening Efficiency and Access to Justice in Moldova" (A2J) is a multi-year institutional development project designed to contribute to an increased efficiency of justice services and to improved access to justice of men and women in Moldova, in particular from vulnerable and marginalized groups, through enhanced capacities of forensic institutions to provide qualitative justice services, strengthened capacities of the justice sector actors in the selected pilot areas to provide coordinated response to men's and women's justice needs and strengthened civil society able to claim the respect of rights and engage in a constructive dialogue with the justice chain actors. Project interventions will offer and encourage equal opportunity for the participation of men and women.

Although important efforts have been deployed at national level during the last years to advance the efficiency, transparency, fairness and accessibility of the justice sector, improvement is further required to ensure coherent coordination among law enforcement, security and justice institutions for effective administration of justice, so that men and women, particularly from marginalized or minority groups, are able to claim their rights and access justice effectively.

The system of forensic institutions[1] is an integral part of the justice system. The expert opinions provided by these institutions are critical for the objective and evidence-based delivery of justice. The quality and accuracy of forensic investigations and examinations have an extensive impact on the quality of justice and affect the overall perception of users about the justice system.

Despite the importance of forensic examination for the act of justice, the institutional system of judicial expertise has not enjoyed the same attention, assistance and support in its modernization and e-transformation efforts, as in the case of other actors of the justice sector.

For example, the judicial system has enjoyed consistent support for the development, implementation and sustainability of the PIGD information system, and the Prosecutor's Office, with the support of development partners, has initiated and continues to implement the 'e-File' information system.

Although significant efforts have been made nationally in the recent years to promote the efficiency, transparency, fairness and accessibility of the justice sector, further improvement is required to provide consistent coordination between institutions for a more efficient management

[1] The system of judicial expertise institutions includes public institutions of judicial expertise and private forensic experts' bureaus. In line with the art.65 para.(2) Law no. 68/2016 on the Judicial Expertise and the Status of Judicial Expert, the system of public institutions of judicial expertise includes the specialized institutions of the Ministry of Justice and the Ministry of Health, Labor and Social Protection, the operative technical-forensic subdivisions or judicial expertise of the Ministry of Internal Affairs and the National Anticorruption Center. The state can also create other public institutions of judicial expertise.

of the justice sector, so that both men and women, especially those of vulnerable groups, are able to claim their rights and access justice equally and effectively.
Thus, the UNDP Project 'Strengthening efficiency and access to justice in Moldova' (A2J Project), provides support for institutional development, as it is designed to support achieving a higher efficiency of services the justice sector and to increase access to justice for everyone. As result of the conducted international tender procedure, an IT company has been selected which is currently involved in the process of development of the FCMS.

In this context, UNDP is looking to contract a company to deliver quality assurance services in the context of implementation of the FCMS. The company will have to assess whether the offered FCMS IT solution is in line with the announced Technical Requirements and ToR, assisting in software and security testing of FCMS, as well as advising on acceptance of implemented FCMS IT solution. The selected company is also supposed to carry out a technical security audit of application software systems developed/procured.

C. Scope of Services and Expected Outputs

The overall objective of the assignment is to assess if the offered FCMS IT solution is in line with the announced Technical Requirements, monitor the implementation process, as well as to assist in software and security testing of FCMS.

The primary objectives of this assignment are to ensure that:

a. FCMS IT solution is developed according to the FCMS non-functional technical requirements;
b. Performance requirements of the newly developed FCMS software are met;
c. The FCMS software solution is tested according to international QA standards and are free of major issues.
d. The newly developed FCMS is developed according to security standards and are free of security vulnerabilities.

In order to achieve the stated objectives, the company will have the following responsibilities:

(i) Analyse the Information system requirements

The purpose of this analysis is to understand the information system requirements. The company shall review the following documents for preparation of test strategy and test plans:

a) Technical Requirements for Supply and Installation of the FCMS;
b) Detailed software specification documentation (SDS and SRS) – a document that will be prepared and submitted by the Supplier of the FCMS software solution and will contain:
    - Analysis Models, including:
        - requirements model and/or use cases
        - domain model, fully specifying the entities and the relations between them.
    - Component model, including a narrative description of all components, the links between them and integration interfaces with other systems/external components
    - Logical model

- Deployment model, including a narrative description of all nodes and the links between them. This model will also contain the precise requirements of the equipment and operation environments for the operation of the system at normal parameters, as well as Requirements for a minimal configuration
- Dynamic model including diagrams and a narrative description of the states and transitions of the key entities

c) Hardware specification for the virtual servers and other needed cloud infrastructure (submitted by the Supplier of the FCMS);
d) System installation and configuration guidelines, that must include at least how to install the application, what the hardware and software requirements are, platform description and configuration, application configuration and disaster recovery procedures (submitted by the Supplier of the FCMS);
e) Documentation of APIs (if any) used for integration with other IT systems, such as e-Governance services, PIGD, e-File of the Prosecutor Office (submitted by the Supplier of the FCMS);
f) Testing plan and testing scenarios (to be submitted by the Supplier of the FCMS);

(ii) Performing of testing activities for FCMS

The purpose of this activity is to ensure that the FCMS software is being developed free of major defects and its builds are ready to be promoted to the production environment.

Should any deficiencies be identified as result of testing, the FCMS Supplier will be required to fix them in reasonable time and once the software is adjusted the company shall conduct re-testing of the system. **It is expected that up to three iterations of such re-testing activities can take place. Re-testing activities may refer to all type of tests: load, stress and security testing.**

The selected company will provide testing documentation and activities for the platform's testing, including:

(a) Baseline the software test plan document (i.e. get it reviewed and approved/ signed-off by the Beneficiary)
(b) Design the required test strategy in line with the scope and organization standards
(c) Define the test automation approach and evaluate test automation ROI
(d) Evaluate and identify the required test automation and test management tools
(e) Estimate the test effort and test resources (team size, skills, attitude and schedule)
(f) Review the test cases and test data generated by Supplier of the FCMS solution
(g) Track the new/ updated requirements in the project and manage the testing artefacts update accordingly
(h) Collect and analyse metrics on test progress and product quality
(i) Report the testing progress/results to the UNDP, including the identified issues and recommendations.
(j) Ensure the resolved defects are re-tested

(iii) Ensure the smooth execution of System Performance Testing Process

The purpose of this activity is to assist the FCMS owner[2] in the System Performance Testing process for developed information system and perform the following activities:

Conduct and validate the following tests for end product and provide a sign off:

(a) Assess the technology used, architecture, performance and security aspects assuring information is protected, reliable, quickly available;
(b) Performance Testing: Load and Stress testing;
(c) Analyse both the results of load testing carried out on STISC servers and those performed separately by the FCMS Supplier;
(d) Provide sign off as the Independent Testing provider for System Performance Testing together with the UNDP, STISC and Ministry of Justice.

(iv) Execution of application software security audit

The purpose of this audit is to perform security code review, penetration testing and other security audit activities to evaluate the following area:

(e) **Validation and Encoding.** The rules for validating and encoding each input to the Information system, whether from users, file systems, databases, directories, or external systems;
(f) **Authentication and Session Management.** The authentication credentials and session identifiers protection throughout their lifecycle;
(g) **Access Control.** The roles (groups, privileges, authorizations) used in the Information system and the access rights to each asset and function for each role;
(h) **Error Handling.** The handling mechanism of errors occurring during data processing.
(i) **Logging.** The information, useful in forensic investigation, logged for each security-relevant event.
(j) **Connections to External Systems.** The authentication and encryption mechanism handled for all external systems, such as databases, directories, and web services.
(k) **Encryption.** The mechanism of data encryption, certificates and other credentials handling.
(l) **Availability.** The mechanism of protect against denial of service attacks such as authentication lockout, connection exhaustion, and other resource exhaustion attacks.
(m) **Secure Configuration.** The mechanism of securing the default values for all security relevant configuration options.

D. Deliverables and Indicative Timeframe

No.	Deliverable	Deadline*

[2] https://gov.md/sites/default/files/document/attachments/subiect-06-nu-514-mj-2021.pdf The Ministry of Justice of the Republic of Moldova is the Owner of the System according to the approved Governmental Decision on the technical concept of the Forensic Case Management System.

1.	**Inception Report which shall reflect the project plan, company's working approach, communication methods, tentative structures of the testing reports developed and submitted.** It is expected that the company will provide brief comments that reflect its understanding about FCMS based on reviewed FCMS Technical Analysis and Design documentation which is submitted by the software development company (FCMS Supplier).		*By August 25, 2022*
2.	**Testing documentation for the FCMS developed and submitted.** The documentation should include: • Test plan; • Test strategy; Test reports.		*By September 23, 2022*
3.	**Report on each System performance testing conducted and retesting after the system improvement, if any** The report should include: • System readiness report; • Improvement proposals.	**It is expected that up to three iterations of re-testing activities can take place. Re-testing activities may refer to all type of tests: load, stress and security testing.**	*By October 17, 2022*
4.	**Report on application software security audit and retesting after the system improvement**. The report should include: • System security test report; • Improvement proposals; • Activity Progress Reports.		
5.	Monthly reports detailing activities performed and progress achieved during the reported period developed and submitted.		*First week of every month following the reporting period*

Note: *According to contract provisions, the unit prices are fixed and are not subject to any variation whatsoever (currency fluctuation, increase of market prices, increase of any taxes etc.), that is why Bidders are encouraged to include all costs associated with the completion of up to three iterations of re-testing activities in their financial proposal.*

****A specific date for each of the testing activities and related interventions shall be proposed by the Service Provider at the beginning of the assignment and coordinated with the Project Team and Ministry of Justice.***

The software and security testing reports shall include the following information:

- Identified deficiencies observed during test and security audit process;
- Recommendations for remediation of identified deficiencies. All recommendations should reflect latest industry trends and standards

The test report will be submitted after each testing cycle and technical security audit of the Information system, won't take longer than 1 week.

<u>Confidentiality statement</u>*: All data and information offered by the UNDP A2J Project and other involved parties for the purpose of this assignment must be treated with confidentiality and must be used only for the purpose of activities stipulated by these Terms of Reference. The contents of written materials obtained and used in this assignment may not be disclosed to any third parties without the expressed advance written authorization of the UNDP. All intellectual property rights that arise from the implementation of these Terms of Reference are attributed to UNDP.*

E. INSTITUTIONAL ARRANGEMENTS

The company will work in close collaboration with UNDP A2J team and National ICT Consultant for the substantive aspects of the assignment, and the UNDP Project Officer – with regards to administrative aspects.

All the deliverables should be cleared by UNDP. The above-listed deliverables will be finalised based on inputs from UNDP A2J Project Team and will be adjusted to the needs of the end beneficiary.

Language requirements

All communications and documentation related to the assignment will be in English and Romanian. The deliverables should be submitted in an electronic format that beneficiaries can further edit and use in their work. If needed, the company shall ensure the interpretation required in the context of performance of the expected tasks.

Timeframe and Location

The expected period of implementation of the assignment is during August - October 2022. The quality assurance services will be carried out in Republic of Moldova.

F. Qualifications of the proposed team:

The bidder shall provide sound argumentation of the proposal by demonstrating compliance with the ToR and the environment in which it will provide the services. The bidder shall include information on the volume of allocated resources to carry out the assignment. A breakdown per working days allocated for each deliverable shall be submitted, clearly explaining the role of the team members involved in producing the deliverable. In this context, the Service Provider shall ensure a clear presentation of distribution of tasks and allocation of working days deemed necessary for engagement. The proposed team should consist of but not be limited to the following members: 1 (one) Team Leader, and 1 (one) Security Testing Consultant, 1 (one) Testing consultant and 1 (one) Business Analyst.

The successful bidder must meet the following minimum qualification requirements for the assignment:

<u>Criteria for the evaluation of the Bidder:</u>

- Legally registered entity or consortium of firms. If the applicant is a foreign entity, it should have a local legal subsidiary/ consortium partner/subcontracted consultant or have at least one core auditor that is a resident of the Republic of Moldova;
- At least 5 years of experience in Software Testing and Quality Assurance and security testing/audit (during the last 5 years)
- At least two successful executed contracts in the last two years, as outsourced project in testing and security testing/audit;
- Certification related to quality and security management (ISO 9001, ISO 27001)
- Proposed key personnel with the required academic and professional qualifications, proven by CVs and valid certificates, if any.

Bidders agree that proposed personnel will provide high quality outputs and expertise and participate in the project at the level and duration specified. Should any changes be necessary in this regard, a formal request for the agreement of the A2J Project team to allow substitutions, shall be submitted.

UNDP may at any time request the withdrawal or replacement of any of the Service Provider personnel. Replacement will be at the Service Provider expense.

Bidders shall enclose a CV for each team members anticipated to be engaged in activities specified at Section C of the ToR - Scope of Services and Expected Outputs.

CVs of the team must be included in the offer. The CVs submitted for proposed personnel should be detailed and comprehensive and prove that the team members are fit to provide the tasks assigned to conduct.

The CVs should include for each of the team members listed bellow:

Team Leader

- University degree in areas such as computer sciences, engineering, and telecommunications or other ICT related;
- Minimum 5 years of experience in area of software development;
- Minimum 3 years of software application security audit;
- Proven experience in applying internationally recognized standards and best practices (e.g. OWASP, ITIL, ISO/IEC 270002, etc.).
- At least 3 years of experience in Project Management in public or private sectors. Internationally recognized certificates such as PMP, PRINCE2, AGILE are considered an advantage;
- Certifications in security qualifications such as CISSP and/or CEH are considered an advantage.

Security Testing Team Member

- University degree in areas such as computer sciences, engineering, and telecommunications or related;
- Minimum 5 years of experience in area of software testing;
- Minimum 3 years of experience in security auditing (code review and penetration testing) of application software;

- Proven experience in applying of internationally best practices regarding application software security developed by OWASP (code review and pen testing).

Testing Team Member

- University degree in areas such as computer sciences, engineering, and telecommunications or related;
- Minimum 3 years of in-depth software testing and Quality Assurance.
- Certifications in testing (such as ISEB, ISTQB or other) are considered an advantage.

Business Analyst

- University degree in areas such as computer sciences, engineering, and telecommunications or related;
- Minimum 5 years of experience in area of IT Business/System Analysis;
- Solid knowledge of UML and BPMN;
- Proven experience in business processes modelling in the content of IT systems.

All team members are expected to have the ability to effectively communicate and write in English. Knowledge of Romanian and/or Russian is an advantage.

Proven commitment to the core values of the United Nations, in particular, respecting differences of culture, gender, religion, ethnicity, nationality, language, age, HIV status, disability, and sexual orientation, or other status.

UNDP Moldova is committed to workforce diversity. Women, persons with disabilities, Roma and other ethnic or religious minorities, persons living with HIV, as well as refugees and other non-citizens legally entitled to work in the Republic of Moldova, are particularly encouraged to apply.