SECTION 5: TERMS OF REFERENCE

Title:	Development of the digital National Farmers Registry (dNFR) and implementation of the pilot phase, as a component of the vision for Integrated Administration and Control System (IACS)
Reference No.:	RFP23/02658
Project:	Human security project: Multidimensional response to emerging human security challenges in Moldova
Beneficiary:	Ministry of Agriculture and Food Industry
Reporting to:	UNDP Moldova Project Manager and assigned responsible officer from the Ministry of Agriculture and Food Industry of the Republic of Moldova
Contract Type:	Contract for goods and services
Duration:	June 2023 - February 2024

Contents

Acronyms

The main acronyms and abbreviations used in the present document are provided in the tables below.

Table 1.1. Abbreviations and acronyms used in the document

No.	Abbreviation/Acronym	Description
1.	AIPA	Agency for Interventions and Payments in Agriculture
2.	ANSA	Food Safety Agency
3.	COTS	Commercial off-the-shelf
4.	DB	Database
5.	DMS	Database management system
6.	dNFR or NFR	digital National Farmers Registry
7.	ICT	Information and Communications Technology
8.	UIN	Unique Identification Number
9.	IS	Information System
10.	IT	Information Technology
11.	ITS	Information Technologies Service
12.	KPI	Key Performance Indicators
13.	GIS	Geospatial Information System
14.	MAFI	Ministry of Agriculture and Food Industry
15.	PSA	Public Services Agency
16.	SDD	Software design document.
17.	LPIS	Land Parcel Identification System
18.	SPOF	Single Point of Failure
19.	SRS	Software Requirements Specification
20.	ICAS	Integrated Administration and Control System
21.	SI ESBS	Information system Evidența Solicitanților și Beneficiarilor de Subvenții (Record of Grant Applicants and Beneficiaries)
22.	RCFI	Register of criminological and forensic information

Table 1.2. Definitions of the frequently used terms in the document

No.	Abbreviation/Acronym	Description
1.	Database	Set of organized data according to a conceptual structure which describes the basic characteristics and the relation between entities
2.	Credentials	Set of attributes which establish the identity and authentication of users and systems within information systems.
3.	Data	Elementary information units about persons, subjects, facts, events, phenomena, processes, objects, situations, etc. presented in a form that would allow their notification, comments and processing.
4.	Personal data	Any information regarding the identified or identifiable natural person (subject of personal data). In this respect, an identifiable person is a person which may be identified, directly or indirectly, especially by referring to an identification number or to one or more specific events related to its physical, physiological, psychological, economic, cultural or social identity
5.	Data integrity	State of data, when they preserve their content and are interpreted univocally in case of random actions. Integrity is considered to be preserved, if data are accurate and reliable.
6.	Logging	A function of registering information about events. The logs about events within information systems include details about date and hour, user, identified personal data, undertaken action.
7.	Metadata	Modality of attributing semantic value to data stored in the database (data about data).
8.	Information object	Virtual representation of existing material and nonmaterial entities.
9.	Information resource	Set of information documented in the information system, maintained in line with the requirements and legislation in force
12.	Computer/ IT system	Set of programs and equipment ensuring automated processing of data (automated component of the information system).
13.	Information system	System for processing information, together with the related organization resources which supply and distribute information.
14.	Software design document	Directory document of the information system, which covers the detailed description of the following vision: data structures and their constraints, information system architecture, which provides all the conceptual sections of the information system, the interface of the information system covering the conceptualization of all components of user interface of the information system, functionalities of the information system,

No.	Abbreviation/Acronym	Description
		which covers the detailed description of all the information system implementation scenarios.
15.	Software Requirements Specification	Document that contains the detailed description of all scenarios of interaction between users and information application.
16.	Information subsystem	Component part (with the possibility of functional decoupling) of a complex information system.
17.	Information and Communications Technology	Common term which includes all the technologies used for exchange and manipulation of information.
18.	Data accuracy	The level of data (which are stored in computer memory or in documents) compliance with the real condition of items in the respective area of the system, reflected by these data.
19.	Register	Complete list of objects belonging to a defined object set
20.	Contractor	Selected company or consortium of companies to implement the services referred additionally throughout the document as Service provider or provider or developer.

Introduction

Agricultural sector plays a critical role for the sustainable development of the country and its food security, by contributing to about 10% (2020, WB data) to Moldova's GDP, and employing about 21% of the active population (2021, ILO estimates). Moldova is at high risk of droughts and extreme weather events, with on average a drought every two years: the agricultural output will drop by an estimated 30% year-on-year, coupled with reduced productivity due to outdated technologies, business processes and equipment used for production.

In the same time, despite swift efforts to recover from COVID-19, the war in Ukraine had disrupted trade and supply routes, blocked value chains, caused loss of markets, and the unprecedented rise in fuel/energy prices and overall inflation have had significantly increased Moldova economic fragility, presenting both a security and an economic threat for Moldova and emerged Food security as a major challenge for the country.

These challenges are addressed through the strategic vision of the National Strategy for Agricultural and Rural Development 2023 – 2030 (hereinafter SNDAR 2030) which envision development of a competitive agri-food sector, centered on value chains with increased potential, environmentally friendly and resilient to climate change, which strengthens food security and safety and provide better welfare and living conditions in rural areas.

In line with objective 4 of the SNDAR on ensuring the transposition of EU Aquis and its progressive implementation in the field of agriculture, rural development and food safety, the Ministry reference development of the Integrated Administration and Control System (IACS), in accordance with the requirements and financing principles of the Common Agricultural Policy (CAP), and the adjustment of the subsidy mechanism based on EU standards.

The government addressed fundamentally food security issues through support, integration and development of the key economic sector. The recently presented Food Security Strategy - requires support for proper implementation and institutionalization but also to measure and monitor food poverty - as an emergent form of poverty in the country. In particular, the Government must develop capability to map, monitor and anticipate shortages of supplies; it must further increase its capacities to plan and target subsidies in a transparent manner to most in need agricultural producers affected not only by the current socio-economic and regional conditions, but also by climate change; finally, it has to support the agricultural sector in fully integrating with EU and global agriculture markets.

The Ministry of Agriculture and Food Industry of Moldova (MAFI) is targeting to promote the modern digital technologies both in administrative layer of the sector (improving policy and decision making in the sector), as well as on the agriculture producers and processors side (simplifying ways of working, promoting efficiency improvement, improving decision making and strengthen resilience to crises. In line with the priorities set above, **MAFI requested UNDP for support in the rapid localization and implementation of digital National Farmers' Registry as the first and the strategic component of IACS.**

The IACS system has been in place in the EU since the 1990s and is an important tool for managing and regulating the agricultural sector in the EU. It is a computerized system used to manage the Common Agricultural Policy (CAP) and to control the distribution of agricultural subsidies to farmers. The IACS system collects and stores data on agricultural land, crop yields, and livestock numbers, which are used

to verify that farmers are complying with EU regulations and eligibility criteria for receiving subsidies. The system also enables the EU authorities to conduct on-the-spot checks and inspections to ensure that farmers are adhering to environmental and animal welfare standards.

As one of the key elements of IACS, the digital Farmers Registry shall cover the following objectives:

1. **Supply reliable data for Moldovan policy makers.** Inaccurate, incomplete or compromised data significantly hamper the capacity of decision makers to get a clear understanding about the current situation in agricultural sector and impact negatively the accuracy and effectiveness of the decisions. The Registry will:
    - Define the legal and regulatory framework to collect the data and maintain up to date records.
    - Provide operational mechanism to collect the data and ensure the compulsory effect of data submission
    - Define tools for data collection and simplification of data collection and access mechanisms.
    - Provide access to real data on the agricultural land situation
2. Serve as one of the reference **resources and starting point for harmonization of Moldovan sectorial legislation and regulations with EU standards in agriculture and implementation of the full-scope IACS**;
3. Serve as the basic **tool for monitoring impact of agricultural subsidies**. In the current context of improving the quality of agricultural subsidies payments in Moldova, the Registry will be considered as an indispensable instrument in the process of **identification and registration of farmers/beneficiaries** as it is used in EU countries, where similar information system is part of the IACS (Integrated Administration and Control System)**.**

1. General information

For this purpose, the UNDP Moldova Project coordinates and provides financing for development and implementation of the digital National Farmers Registry and required basis for further development of the full scope IACS.

The digital National Farm Register is a key requirement for EU accession. Such Farmers Registry are to be serving for achieving the following objectives:

- Compile data related to the national agriculture sector, comparable with international standards, in particular EU member states agricultural statistics;
- Support the development of more coherent statistical agricultural surveys, methodologies and practices, based on EU like norms and standards;
- Serve as one of the bases for the verifying and registering beneficiaries of agricultural subsidies to farmers.

To ensure the effective, efficient and complete development and implementation of a complete and fully operational digital National Farmers Registry, services of a **Consortium of companies** and/or NGOs will be selected, under a single LOT, in a competitive way according to UNDP procedures, to cover the 3 components of this project, namely:

1. **Component 1: Conceptual, legal and regulatory framework**

   Company services for developing, in collaboration with MAFI and the Government, the needed conceptual, legal and regulatory framework for developing and operating a digital National Farmers Registry, as a component part of the prospect national IACS, in line with EU standards.

2. **Component 2: Data collection and community engagement framework**

   Company services for developing dNFR implementation concept and implementation on the concept (in collaboration with MAFI, Local Public Authorities (LPA), Government agencies, farmers). The operational elements include: scenarios for data collection, instruments for collecting, validation and processing data and other activities as needed by the proposed implementation concept.

3. **Component 3: Development of the digital National Farmers Registry platform (software component)**

   Company services for developing the IACS IT architecture and software components for the dNFR, ensuring compliance and inter-operability with EU requirements, government infrastructure, databases and digital platforms.

   The present document provides a conceptual vision for setting up and operation of a digital national farmers registry in the Republic of Moldova, as a prior initiative towards implementation of IACS.

   The registry is targeted to be lunched by 28 February 2024, in phase 1 - for a Geographically limited scope, with further extension for national-wide scope and IACS deployment as phase 3.

   Implementation approach shall be aligned with the goal and objectives, principles, main characteristics and components, functionality and conceptual architecture, functional and non-functional requirements of the information system.

In this regard, a brief description is provided for the basic components of the future solution, pointing out the principles and functionalities to be taken into consideration when developing every component.

2. Component 1: Conceptual, legal and regulatory framework

UNDP Moldova Project aims to improve access to and quality of public services and business conditions through accelerated digital transformation of government processes and business model(s) and additionally, to promote innovation by bringing forward digital components in supporting accelerated delivery of the Sustainable Development Goals.

While there is much emphasis on digital tools and technologies in Moldova, digital transformation areas like policy, institutional coordination, and leadership remain a significant challenge and continue to constrain effective digital transformation and economic growth.

Due to the highly regulated nature of this sector, administrative registers are used extensively in agriculture, including under the EU legislation, which mandates the creation of a large number of registries.

The Integrated Administration and Control System (IACS) is used as reference decision point for payment of subsidies (area-based, animal premiums etc.) under the Common Agricultural Policy as well as (common) market regulation measures and control of animal health and surveillance measures.

The Ministry of Agriculture is the key line ministry of the Government and a central body empowered to promote and implement new information technology to strengthen the local agricultural system and improve productivity, to spur digitalization and innovative technology adoption among Moldova's agribusinesses.

While data collection, analysis, monitoring, and sharing tasks were traditionally paper-based, data processing and storage was heavily hampered and most often de-centralized. Within the current realities, given the volume of data and efficiency standards on the processes, use of digital tools and processes is a mandatory necessity. IT systems shall ensure real-time data collection; validation, modelling and compilation and dissemination, to reduce data processing obstacles faced in the past. The initiative complements and builds on national strategies in the sector and Agenda 2030 for sustainable development of the country. The modernization and digital transformation of the agricultural production is imperative to create a sustainable economy and develop human capital in Moldova. Driven by the expanded usage of digital technologies in high growth potential value chains, this transition will result in innovation and spillover benefits to enhance the performance of one of Moldova's most important economic sectors.

2.1. Objectives

The goal of Component 1 is designing and developing the conceptual, legal and regulatory frameworks necessary for implementation and operations of IACS and a digital National Farmers Registry in the RM. It has to fulfill the following objectives.

- It shall address the objectives and the time-line of the program, defining long-term elements and strategy for full- IACS and any other complementary EU Agriculture regulation implementation.
- The frameworks have to be aligned and validated with the MAFI and the Government.
- dNFR shall be a robust and reliable process and in the same time an information system.
- dNFR will define the guidelines and requirements for any other input or output system/process, which shall be developed within the later phases (IACS deployment)
- be the main entry point for agricultural production including collection, analysis, monitoring, and provision of technical assistance to farmers
- dNFR will utilize at maximum the available digital platforms and elements in the country.

2.2. Framework of references

- the dNFR, shall use as reference the European legal and normative acts.
- the national legislation and regulations need to be assessed and duly amended to accommodate the provisions of EU legislation.
- the national legislation and regulations will also be taken into account for adjacent areas.
- due to the digital nature of the NFR, provisions in Moldova's normative legislative framework regarding information systems set up by the Government will also be considered.

2.2.1. Moldovan legal regulatory framework

Acts regulating the development, production and operation of National Registries

The following acts and regulations may be mentioned in this regard:

- Government Decision No. 945 of 05.09.2005 on public keys' certification centers, Official Gazette No. 123-125 of 16.09.2005.
- Government Decision No. 320 of 28.03.2006 approving the Regulation on how to apply digital signature on electronic documents of public authorities, Official Gazette No. 51-54 of 31.03.2006.
- Government Decision No. 7104 of 20.09.2011 approving the Strategic Program for governance technological modernization (e-Transformation), Official Gazette No. 156-159 of 23.09.2011.
- Government Decision No. 188 of 03.04.2012 on official pages of public administration authorities on Internet, Official Gazette No. 70-71 of 06.04.2012.
- Government Decision No. 656 of 05.09.2012 approving the Program on Interoperability Framework, Official Gazette No. 186-189 of 07.09.2012.
- Government Decision No. 1090 of 31.12.2013 on electronic governmental service of access authentication and control (MPass), Official Gazette No. 4-8 of 10.01.2014.
- Government Decision No. 128 of 20.02.2014 on common governmental technological platform (MCloud), Official Gazette No. 47-48 of 25.02.2014.
- Government Decision No. 405 of 02.06.2014 on integrated electronic governmental service of digital signature (MSign), Official Gazette No. 147-151 of 06.06.2014.
- Law No. 91 of 29.05.2014 on electronic signature and electronic document, Official Gazette No. 174-177 of 04.07.2014.
- Government Decision No. 700 of 25.08.2014 on open governmental data, Official Gazette No. 256-260, of 29.08.2014.

- Government Decision No. 701 of 25.08.2014 approving the methodology for publishing open governmental data No. 256-260 of 29.08.2014.
- Government Decision No. 708 of 28.08.2014 on logging governmental electronic service (MLog), Official Gazette No. 261-267 of 05.09.2014.
- Law No. 142 of 19.07.2018 on exchange of data and interoperability, Official Gazette No. 295-308 of 10.08.2018.
- Government Decision No. 211 of 03.04.2019 on interoperability platform (MConnect), Official Gazette No. 132-138 of 12.04.2019.
- Government Decision No. 375 of 10.06.2020 approving the Concept of Automated Information System “Register of representation powers based on electronic signature” (MPower) and of the Regulation on how to keep the Register of representation powers based on electronic signature, Official Gazette No. 153-158 of 26-06-2020.
- ORDER No. 78 of 01.06.2006 regarding the approval of the technical regulation "Software life cycle processes" RT 38370656 - 002:2006
- Law no. 467/2003 regarding computerization and state information resources (to ensure compliance with the provisions of art. 76 para. (2)
    - a) the concept of the information system [...];
    - b) specifications of the information system [...];
    - c) the regulation of the information resource [...]."
- HG nr. 412/2020 for the approval of the Regulation on the use, administration and development of the entrepreneur's Government Portal for ensuring data exposure related to legal entities in the agro-industrial field;

The construction of the National Farmers registry needs to consider interconnexions with relevant related registers, such as

- the State Animal Register;
- the System of Identification and Traceability of Animals, a basic subsystem and an integral part
- of the process of traceability of animal products;
- Management of Strategic Sanitary-Veterinary Measures, to support the preparation, registration and monitoring of the annual strategic plan drawn up by the National Agency for Food Safety;
- Laboratory Management, to generate the information needed for the complete management of sanitary-veterinary and food safety laboratories;
- the Administration of State Agricultural Heritage;
- the Agricultural Equipment Register, used to provide IT solutions for identifying, recording and managing information about the technical potential of economic agents in the agro-industrial sector;
- Law on the principles of subsidization in the development of agriculture and the rural environment, to automate workflows for managing subsidies while offering the possibility of generating different reports and controlling document circulation;
  Wine Register (includes a series of subsystems and modules that automate and ensure the processes of identification, registration, validation, archiving, deletion or modification of the data, according to the activity of the economic agent, to register wine parcels/wineries);

- Management of the Release of Phytosanitary Certificates (includes management of the export and re-export of products of plant origin, the preparation of reports, producer and exporter records, export directives).

Legal framework on subsidies

- Law No 276/2016 on subsidy principles in the development of agriculture and the countryside;
- Government Decision No 455/2017 on the allocation of the resources of the National Fund for Agricultural and Rural Development;
- Government Decision No 507/2018 approving the Regulation on the conditions and procedure for granting advance grants for start-up projects from the National Agricultural and Rural Development Fund;
- Government Decision No 476/2019 approving the Regulation on the award of subsidies to improve the standard of living and working in rural areas from the National Agricultural and Rural Development Fund;
- Government Decision No 836/2020 approving the Regulation on the granting of direct payments per head of animal;
- Government Decision No 277/2022 approving the

Other acts regulating ICT initiatives of the Republic of Moldova, developing information systems in the Republic of Moldova

2.2.2. European Union legal regulatory framework

The following acts and regulations of the European Union may be mentioned:

- Regulation (EU) 2018/1091 of the European Parliament and of the Council of 18 July 2018 on integrated farm statistics and repealing Regulations (EC) No 1166/2008 and (EU) No 1337/2011.
- Commission Regulation No 1308/2013 of the European Parliament and of the Council of 17 December 2013 establishing a common organisation of the markets in agricultural products and repealing Council Regulations (EEC) No 922/72, (EEC) No 234/79, (EC) No 1037/2001 and (EC) No 1234/2007
- Regulation (EU) 2022/2379 of the European Parliament and of the Council of 23 November 2022 on statistics on agricultural input and output, amending Commission Regulation (EC) No 617/2008 and repealing Regulations (EC) No 1165/2008, (EC) No 543/2009 and (EC) No 1185/2009 of the European Parliament and of the Council and Council Directive 96/16/EC
- Regulation (EU) No 1151/2012 of the European Parliament and of the Council of 21 November 2012 on quality schemes for agricultural products and foodstuffs
- Commission Delegated Regulation (EU) No 1198/2014 of 1 August 2014 supplementing Council Regulation (EC) No 1217/2009 setting up a network for the collection of accountancy data on the incomes and business operation of agricultural holdings in the European Union

EU regulations on agricultural policies and subsidies:

- Regulation (EU) 2021/2115 of the European Parliament and of the Council of 2 December 2021 establishing rules on support for strategic plans to be drawn up by Member States under the

common agricultural policy (CAP Strategic Plans) and financed by the European Agricultural Guarantee Fund (EAGF) and by the European Agricultural Fund for Rural Development (EAFRD) and repealing Regulations (EU) No 1305/2013 and (EU) No 1307/2013

Other acts regulating ICT initiatives in the agricultural field in the European Union.

2.3. Activities

Specific activities are to ensure the:

1. Develop the conceptual, legal and regulatory framework and roadmap necessary for IACS implementation in the Republic of Moldova
2. Develop the conceptual, legal and regulatory framework and roadmap necessary for a digital National Farmers Registry implementation and operation the Republic of Moldova, in line with IACS.
3. Develop detailed dNFR operationalization concepts for the MAFI and its relation to the new Regulations on Subsidies for the Republic of Moldova.
4. Strengthen legal capacities of the Ministry and related agencies and enhancing institutional coordination mechanisms.

2.4. Deliverables

Deliverables #1: Conceptual, legal and regulatory framework development	**Timeline (indicative)**
1. Situational & Gap analysis (tables of compliance) of the national legislation and regulation for implementation of the IACS and dNFR as a first component	June - August 2023
2. Development of the IACS concept and operationalization mechanisms: - Development of the IACS concepts and supporting fact-base - Develop legal recommendations and amendments to the current legislation to ensure the implementation of the IACS; - Description of the operationalization mechanisms for IACS implementation - Development of the IACS implementation roadmap - Development for costing baseline for IACS implementation - Amend the proposed concepts in line with conflicting findings from parallel implementation of components 2 and 3 of the ToR.	June - September 2023
3. Development of the dNFR concept and operationalization mechanisms, as the first component for IACS implementation: - Development of the dNFR concepts and supporting fact-base - Develop legal recommendations and amendments to the current legislation to ensure the implementation of the dNFR - Description of the operationalization mechanisms for dNFR as the first component towards IACS Development of the dNFR implementation roadmap as the first component of IACS - Development for costing baseline for dNFR implementation	June - September 2023

- Amend the proposed concepts in line with conflicting findings from parallel implementation of components 2 and 3 of the ToR.	
4. Development of policy or position briefs on the implementation of the dNFR and transition to IACS. Analysis and development of analytical reports and briefs based on the datasets collected through the dNFR.	June 2023 – February 2024

3. Component 2: Data collection and community engagement

3.1. Objective

This component aims at defining the sources and mechanisms for data collection and community integration into dNFR system, to ensure consistent initial data upload and effective mechanisms for operational support and update of the data.

Feasibility study confirmed that existing registries are mostly non-functional and the accuracy of the data is very doubtful. The component consists of two major sub activities to be carried:

- Identify and ensure functional and effective input data sources and mechanisms for dNRF, which includes
    - define the full scope of input data required for an efficient functioning of the dNFR, based on the concept document defined within Component 1
    - evaluate and assess the availability, integrity and validity of digital data sources and flows for the required data
    - define the requirements for the missing digital data and data flows. Define and support the development of the required normative acts to ensure sustainable functioning of the defined data flows.
- Implement dNFR
    - define and implement the collection approach scenarios, instruments for collecting, verifying, and processing primary data required for dNFR operation.
    - define operational and institutional procedures to ensure sustainable mechanisms for dNFR functioning.
    - Conclude required procedures, contacting or procurement to ensure supply of the required data.
- Test
    - Test the effectiveness and sustainability of the collection approach scenarios, instruments for collecting, verifying, and processing primary data on the pilot phase scope.
    - Compile test reports.
    - Adjust the processes to ensure efficient and effective data supply based on test results, to ensure effective acceptance of the tests by the beneficiary.

3.2. Framework of reference

The implementation of the project during 2023-2024 calendar year will be based on a pilot approach. Nevertheless, its relatively small-scale exposure will allow to test and obtained necessary results to remove any uncertainty about the feasibility of setting up in Moldova of a fully functional Farm Register and IACS during next phases of the program. Thus, for the pilot phase will be gathered a minimum of 10000 [1]declaration/land parcels registration forms in 9-12 communities from 3-4 regions/raions of Moldova.

[1] https://statistica.gov.md/ro/caracteristici-demografice-nationale-lingvistice-culturale-52_3669.html

The implementation of this particular component calls for a tight interaction with Component 1 in order to test and provide feedback during the development process of the dNFR technical concept. This includes inter alia developing and testing

- approaches for registration of primary data at local level:
- instruments for collection of primary data;
- timeframes for the process of primary data collection;
- methods of gathering primary data at local level;
- approaches to verification of primary data at local level;
- initiating data analysis and generating reports.

Beside the above, this Component will conduct activities dedicated to launching of the public awareness campaign in the selected pilot communities. The project will collaborate national and regional and local media outlets to ensure at least 5 special programs about the progress of Farmers registry pilot phase implementation. Elaboration and annual updating of leaflets and posters shall increase the expected results of the information campaign in the selected communities.

3.3. Activities

3.3.1. Information and communication campaign

Project success will largely depend on the level of information and awareness among agriculture producers about the benefits of the Farmers Registry. Within this context, at the initiation stage, the contracted implementer will, in collaboration with UNDP Moldova and other project partners, develop a comprehensive information and communication campaign to advertise the project and disseminate its objectives and benefits at nation-wide scale.

To target agriculture producers at local level a series village promotional events will be conducted jointly with local authorities, and MAFI.

To raise the extent of awareness about Farmers Registry, the project will develop a special set of information materials.

3.3.2. Develop primary data collection instruments

In close coordination with the Component 1 team, the Component 2 team will develop, format and test (within the pilot) digital instruments and their respective instructions to implement a robust, sustainable and efficient process for any dNFR required data collection.

Provides might shall be defining any/all available data collection mechanism and sources and test their effectiveness and efficiency within the pilot phase. Contractor will ensure manual data collection for the pilot phase, in case of failure to define or implement data collection flows/process.

Digital data accuracy may be tested using paper data collecting forms (as back-up process) which is subject to UNDP, MAFI and project stakeholder's validation. The contractor will also be responsible for formatting and development of the digital flows or printing out paper data collection forms, instructions, consent letters, etc., in sufficient capacity / quantities, including consequent digitalization of any paper forms.

Test conclusion shall be user as reference inputs for extrapolation of the data volume and required resources to host the full scope of data within dNFR and IACS full deployment.

The results of the tests should be documented and shared with UNDP and project stakeholders. The Contractor will then suggest revisions to the draft instruments and instructions. Final versions of data collection instruments and instructions must be approved by MAFI.

3.3.3. Selection of project intervention area

Project pilot phase covers 9 to 12 communities from 3 to 4 regions/raions of Moldova. Contractor will contribute to the development of the methodology for selecting pilot-project intervention communities', their evaluation and selection depending on the availability of required data, data collection processes or operational registers in place.

Given the importance of this phase of dNFR establishment in Moldova, it is essential that this sub-activity is conducted in most transparent manner, with clear criteria for selecting intervention areas and potential beneficiaries of the assistance. In order to reduce subjectivity in the process of selecting intervention zones, alternative selection options with diverse criteria and methods might be explored.

3.3.4. Field data validation

Once the project intervention area and selection criteria are defined and validated, the Contractor must commence field data inventory. The term "inventory" is used to describe the process of on-site verification and validation of the data gathered form input sources / registers.

The Contractor is responsible for designing the approach, procedures, instruments and instructions to be used for farm inventory.

Project staff utilized by the Contrctor for farm inventory must have relevant qualifications, be adequately trained and be sufficiently sized prior to start the field work in order to complete the task on expected deliverables and schedule. Data collection will be conducted during at least a three-month period, at the time of day when it is convenient for farm operator and with consideration to hie/her work and farm responsibilities. The collection of primary data shall at least 10,000 farms located in approximately 9-12 communities.

The contractor shall prepare a plan for recruiting, hiring, and training farm inventory staff. UNDP shall approve said plan. It should also address the development and test of such key training materials as the Guidelines/Instructions for the field staff, which later will be institutionalized for in-life support by national authorities.
During the field work, the contractor should submit regular reports documenting the status of the field work in the farms where data collection has been attempted and the completion of forms that were completed. These reports should summarize attempts to locate and survey the farmers, details on reasons for rejecting participation at registration, any logistical or technical issues and challenges, and other relevant data. All forms gathered by Contractor will be submitted on weekly basis to Project office in Chisinau.

The actual output of farm inventory will be a collection of datasets required for operation of the dNFR.

3.3.5. Local staff training

Local level authorities and agencies staff shall be trained on IACS/dNFR concept and all 3 Components of this program, to ensure

- endorsement of the dNFR development project: (i) dNFR overview, objectives and targets; (ii) project governance and project management; (iii) project timeline; (iv) roles, responsibilities and deliverables; (v) reporting requirements and reporting system.
- dNFR/IACS hand-over and in-life management: (i) governance, (ii) purpose and methodology (iii) roles and responsibilities; (iv) data collection techniques and tools; (v) reporting requirements and reporting system.

The Contractor shall develop and validate training plan with the beneficiary, including key training materials as the Guidelines/Instructions, and instruct and equip the team with everything necessary to deliver the trainings.

Training should be an on-going process and at least during the first month of the data collection any lessons learned should be shared with the operators to facilitate further work. To this end regular field staff debriefs should be held to reveal any need for reviewing the data collection approach and feedback should be given to the data collection team.

3.3.6. Support for processing and data quality control

Data entry, cleaning, and verification start alongside the field work and continue toward the end of the project. It is essential that any data entry and review methodology proposed by the Contractor include an effective data quality control approach during the data entry to ensure both timely detection of any problems that can be corrected during the on-going field work and an accurate dataset that can be used for relevant analyses. Illogically missing data should be identified through quality control procedures before data are entered; however, any remaining illogically missing values should also be flagged at the data entry stage and addressed immediately. The Contractor will be responsible for processing the data in a way that can be used for further, more specialized analysis.

In close collaboration with the Component 3 team the Contractor is responsible for contributing to the development of the software used for data entry and storage. Aside from software, the Contractor is encouraged to propose other data entry methods to ensure quality data, such as double key entry. Data quality issues, when identified, should be resolved by the Contractor.

The Contractor will provide a summary of the data collection methodology and any deviations from the proposed methodology that occurred during data collection. The Contractor will provide a User's Guide for the dataset. The Contractor shall be responsible for keeping the forms and data files for the duration of the Project for internal control.

All datasets and other data collected shall be the property of UNDP, and completed data collection instruments should be transferred to designated authority at the conclusion of each survey. The Contractor cannot release the data or present any reports using these data without the prior consent of UNDP.

3.4. Deliverables

Deliverables #2: Data collection and community engagement	Timeline (indicative)
1. Development of communication strategy, define information campaign and communication events at national and local levels (minimum 10 events).	June - July 2023
2. Development of required informative materials for the campaign (including but not limited to posters, leaflets etc., in Romanian and Russian languages	June - August 2023
3. Development and deliver training for national and local level staff (estimated at 1000 beneficiaries)	June - August 2023
4. Development of data collection instruments and mechanisms (forms, guidelines, criteria).	June - July 2023
5. Collect and develop/operationalize datasets of farm operators in intervention area (minimum 10,000 farms from 9 to 12 regions)	August – October 2023
6. Interim field work data collection progress report	October 2023
7. Final field work data collection report and final dataset	December 2023

4. Component 3: Development of the digital National Farmers Registry software, as a as component of the IACS

4.1. Objectives

This component aims at defining the requirements for development of required architecture, IT and DATA infrastructure to enable the deployment and operation of the dNFR. In the relation with Component 1 and Component 2, the Contractor - a team of experts, shall define, design, develop, deploy and operationalize the digital National Farmers Registry platform (software), as an element of the future IACS.

The Contractor will be defining the functional requirements and platform architecture alongside with definition of Component 1 and 2. In the same time, Component 1 and 2 teams will be assisting component 3 team in order to define and design the system which will be fulfilling the following goals:

1. Design the concept and architecture of IACS platform and dNFR integration within other elements of the IACS.
2. Development of the baseline for the Land Parcel Identification System (LPIS) and perform current mapping using high precision satellite imagery that are digitally rendered using AI tools for to identify agricultural lands, including overlaying with existing cadastral maps and soil maps. Available resources and databases of the e-Cadaster agency will be provided.
3. Standardize sector data: unify and centralize the farmers data and records, their agricultural activities or outputs and cadastral data. Align national standards with EU references.
4. Increase the traceability: ensure the authenticity of the records and their integrity through implementation of Farmers' Unique Identification Number. Each farmer shall receive one unique identification number and record within the register
5. Eliminate manual or paper-based data collection, management processes or registers.
6. Ensure and supply accurate and consistent real time data and information regarding the agricultural sector in Moldova.
7. Elimination of direct human factor in defining the size of Moldova's agricultural sector, agricultural production, agricultural subsidies for farmers in the Republic of Moldova, and other data related to Moldova's agricultural sector
8. Increase transparency, monitoring in the activity and quality of decision-making processes in the agricultural system of Moldova
9. Improve traceability of Moldovan agricultural products
10. Development of a secure, complete and fully operational digital National Registry for Moldova
11. Develop data management functionalities (input data loading or retrieval; data processing and storage; data export, exposure and reporting)
12. Increase inter-operability and data exchange with other information systems of the MAFI (ANSA, AIPA, etc.) and the Government

Short term objectives:

- Analysis and assessment of the existing datasets related to farms registries, including their integrity or accuracy.
- Develop an IACS compliant/ ready architecture. Leverage on the existing data sources and other platforms to be integrated:

    - The FaST or similar (Farm Sustainability Tool - digital service platform for agriculture based on space data)
    - Official agricultural registers.
    - Official statistical surveys.
    - Smart farming applications.
- Develop the grounds for Land Parcel Identification System (LPIS). Validate the available geospatial data from e-Cadaster and other available local registries
- Deploy a multi-actor approach. Clear/defined responsibilities and sources for data collection, processing, reporting (Bureau of statistics, e-agency, MAFI/AIPA, ANSA, etc.) and in the same time, ensure integration and validation of data in case of multi-sources inputs.
- Definition of access rights, information and data security (ISO 27001).
- Validate and deploy dNFR data model.

From the analysis of the existing data sets, we have concluded that a Farm Registry must contain the following information:

- Basic information about Business/legal entity or natural person, that will allow to identify and contact.
- Farm and agricultural plots (land parcels geo-location) of establishments.
- Type of farming and employees' handwork type of a production unit.
- Tenure regime of a crop parcel.
- Existing specialization and degree of commercialization
- Cultivation system and cultivation detail.
- Seed type and organic farming certification.
- Labor type, irrigation type and actions carried on the crop.
- Use of fertilizers and phytosanitary products: product, dose and application dates.

The approach to the registry shall:

- Focus on the land parcel's geo-location.
- Develop a unique farm identification code for the farms, in line with Government initiative.
- The agricultural plot would be the minimum work unit: defined as farmer + crop + cultivation system.

Tentative, the information can be organized in three levels, unless different proposed as per IACS best practices:

- Land parcel geo-location and data about the soil
- Farm location: farm base and establishments, geospatial delimitation(s) and basic use (Agricultural Land, Permanent Pastures, and Permanent Crops).
- Crop versus animal production: Category/type of livestock farm (type of animals, number/category).

- Methods of production: seedtime or date of the specific labour carried out on the crop, agricultural activity, fertilizers, plant-protection products.

4.2. Framework of references

For the purpose of ensuring the objectives set for the IS „dNFR", the following general principles should be considered when designing, producing and implementing it:

- ***Principle of legality****: implies setting up and operating the information system in line with the national legislation and international norms and standards recognized in the area.*
- ***Principe of focusing on stakeholders' needs*** *which implies that the information solution will supply complete functional capabilities to meet the needs of all stakeholders interested in human resources' evaluation processes.*
- ***Principle of decoupling the technological platform*** *which ensures that IS „NFR" will not be conditioned by selection of the technological platform based on which it will be implemented. The independence of the technological platform implies that the IS „NFR" will be able to be implemented and operated on a variety of technologies accessible for Ministry of Agriculture and Food Industry (MAFI), selecting the best technological option. Thus ensuring the rational use of available ICT resources and intelligent investments in ICT.*
- ***Principle of dividing the architecture by levels****: implies designing and implementing the functional components of the IS „NFR" in line with the interface standards between levels;*
- ***Principle of service oriented architecture (SOA)*** *which implies distribution of functional components of the information system into smaller, distinct components – called services – which may be distributed into a network and may be used together to create applications meant to implement the business functions of the information system. These components will be able to be implemented without rigid mutual dependencies and will interact through external interfaces implemented based on open and independent standards of technology. This fact provides flexibility to choosing technologies and independent life cycles for components of the IS „NFR". It will also allow the stakeholders to select alternative technological options for capabilities to introduce and access data.*
- ***Principle of reusing existing capabilities*** *which implies that the IS „NFR" will be implemented by reusing at the level of its components the current ICT capabilities to which MAFI has access. The development of new capabilities specific for the IS „NFR" will be performed only in case when they are missing in the current ICT architecture of MAFI (preserving the SOA architecture and ensuring the possibility of reusing these capabilities by other systems, where possible). This fact implies the use of governmental platform services or of platform solutions implemented within MAFI, for developing the components which are setting the IS „NFR".*
- ***Principle of aligning to the wide-scale of ICT architecture of MAFI*** *which implies that the place of the IS „NFR" in wide-scale ICT architecture is explicitly delimited from other systems. The IS „NFR" should be implemented applying the principle of ICT architecture established by MAFI and should be able to interact with other components of the ICT architecture. At their turn, the ICT architecture principles are aligned to the principles of governmental architecture.*

- ***Principle of open and interoperable data model*** *which implies that the data model supported by the IS „NFR" is documented and communicated to all stakeholders. The IS „NFR" should be developed based on the good standards in the area and aligned to the governmental and departmental data model (adoption of already existing taxonomy and semantics at the national and departmental levels and their enrichment to meet the specific needs in the area).*
- ***Principle of security through design*** *which implies the design of the IS „NFR" with knowledge regarding the information security risks that may impact the good functional of the information system. The legal requirements applicable for personal data protection shall be considered when designing the IS „NFR' and implemented at the development stage. The IS „NFR" will ensure the controlled, transparent and responsible access to information.*
- ***Principle of integrity, completeness and accuracy of data****: implies the implementation of mechanisms which would allow preserving the content and the univocal interpretation of data in conditions of accidental influences and elimination of phenomena that would distort or liquidate them accidentally, supply of a volume of sufficient data for carrying out business functions of the information system and ensuring a high level of data compliance with the real condition of objects they represent and which are part of the Integrated Management System.*
- ***Principle of accessibility of public information and data security****: which implies the implementation of procedures to ensure access of applicants to public information provided by the information solution.*
- ***Principle of expansibility****: stipulates the possibility of extending and completing the information system with new functions or improving the existing ones;*
- ***Principle of the first persons/single center priority****: implies the existence of a responsible person of high level, with sufficient rights to take decisions and coordinate activities for setting up and operating the information system;*
- ***Principle of scalability****: implies ensuring constant performance of the information solution when the volume of data increases and the demand for the information system goes up;*
- ***Principle of simplicity and convenience in use****: implies the design and implementation of all applications, technical means and program means accessible to users of the IS „NFR", based on exclusive visual, ergonomic and logical principles of conception.*

4.3. Activities

The activities of design, development, testing and implementation of IS „dNFR" must be performed by teams with sufficient necessary experience to perform the appropriate work and will include the following stages and element to be undertaken by Component 3 Provider:

4.3.1. Functional design stage (2 months)

- performs the business analysis and define functional requirements of the system, considering the output of work on Component 1 and 2. Validate the requirements with all stakeholders, through a Technical Project (SRS and SDD) developed within 0.5 calendar months;

- define the architecture of the IACS and dNFR. Validate the architecture with project stakeholders and other public entities concerned (eGOV, STISC)
- define the development and integration pre-requisites and requirements.

4.3.2. Development (3 months)

- deploys and integrates platform environment: Development, Test/ Training and Production
- delivers required software and components development, in accordance with the validated functional requirements.
- caries unitary, integration, functional and user acceptance test. Performs application demo.
- refines developed software until UAT is passed and the final acceptance is signed.
- performs the integration with external data sources. Performs initial data migration.

4.3.3. Documentation & Training

- hand over up-to-date system architecture and documentation, including operational manuals.
- training of System Administrator roles. Minimum of 2 admins.
- training of trainers (ToTs) on system operation and user layer. up to 30 authorized users with all configured roles will be trained.

4.3.4. Stabilization stage of IS „dNFR"

- will begin with the approval of the minutes of acceptance by the MAFI in the presented version and the signing of the act of putting into production of the IT system. This stage will last 3 months during which the Provider will assist the MAFI in the operation of IS „NFR" and will perform activities to eliminate errors / deficiencies, detected as well as optimizations in the operating parameters of IS „NFR".

4.3.5. Commissioning of the system

- Transfer of the system to operations. Hand over of the administration.

4.3.6. Warranty period

- Regardless if the Provider is or not contracted for support and maintenance services delivery during the first year of system operation, the period in which the Provider assumes the obligation towards the MAFI to assist it in maintaining the capacity of the IT system to provide services, as well as the modification of the product (elimination of errors and optimization of operating parameters), preserving its integrity. In the case of IS „NFR", 12 calendar months of warranty, maintenance and technical support are required.

4.4. Deliverables

The final product (IS „dNFR") deliverables are specified in table 7.1.

Deliverable#3: Development of the digital National Farmers Registry software	**Timeline**
1. Development of the dFNR in line with Law no. 467/2003 regarding computerization and state information resources, including baseline for implementing Land Parcel Identification System (LPIS) and perform current mapping using high precision satellite imagery that are digitally rendered using AI tools for to identify agricultural lands, including overlaying with existing cadastral maps and soil maps.	June - December 2023
2. Transfer of knowledge and software to the owner, holder and administrator of the software solution, as per sub-deliverables below	
3. Warranty, maintenance and technical support - 12 calendar months	12 months from the date of signing the act of commissioning the software

* The solution shall consider capacity for integration or absorption of current subsidy disbursement mechanism (SI ESBS), LEADER IT software, and shall be passible for integration in the vision for IACS implementation.

List of component sub-deliverables:

Nr.	**Requirement**	**Timeline**
DEL 001	Complete documentation as per Law no. 467/2003 regarding computerization and state information resources o the concept of the information system o specifications of the information system o the regulation of the information resource	
DEL 002	Technical Project (SRS+SDD).	
DEL 003	Documents and reports related to the project management processes for the design, development and implementation of IS „NFR".	
DEL 004	Functional environment of the platform with 3 instances.	
DEL 005	The complete source code of the modules and components required to compile the delivered program product.	
DEL 006	Test plan and test reports (functional, integration, performance, loading, security).	

DEL 007	Software solution of the primary data migration and population in IS „NFR”.	
DEL 008	The final product packaged for easy installation into the proposed technological environment (including automated deployment scripts).	
DEL 009	Document on the deployment and configuration of IS „NFR”.	
DEL 010	User Manual	
DEL 011	Administrator's Manual (including contingency plan).	
DEL 012	Administrator's Training and training materials	
DEL 013	Trouble shooting and current maintenance activities guide	
DEL 014	The Provider will develop and deliver training programs for all relevant categories of users, deliver users training and submit training materials.	
DEL 015	Data migration/ Data integration tests results	
DEL 016	ToT	
DEL 016	Technical specifications for interfaces consumed and published/exposed by IS „NFR” .	
DEL 017	SLA agreement signed with the MAFI for the period of maintenance, warranty and support.	
DEL 018	All artifacts are to be delivered electronically (DVD + -R).	
DEL021	The Provider is to provide technical assistance services during the pilot period of IS „NFR” (period of stabilization of the IT system).	
DEL 022	The Provider will assist the MAFI in the acceptance testing activities of IS „NFR”.	
DEL 023	The Provider is to provide services to assist the MAFI in the processes of putting IS „NFR” into production.	
DEL 024	The Provider is to eliminate all deficiencies and errors of the IS „NFR” identified during the stabilization period and in the acceptance test.	
DEL 025	The Provider is to provide post-implementation technical support (after putting the system into production) for a period of 12 months, including corrective, adaptive and preventive maintenance, in accordance with MS ISO / IEC 14764: 2015 - Software engineering. Software life cycle processes.	

	Maintenance, and ORDER No. 78 of 01.06.2006 regarding the approval of the technical regulation "Software life cycle processes" RT 38370656 - 002:2006	

5. Stakeholders involved

In line with the scope of the Project and the objectives of the dNFR development and implementation, the preliminary list of the key stakeholders for this project is listed below:

- Ministry of Agriculture and Rural Development (MAFI)
- Agency for Payments and Interventions in Agriculture (AIPA)
- National Food Safety Agency (ANSA)
- The National Office for Wine and Vine (ONVV)
- The Agency for Land relations and Cadaster
- Electronic Governance Agency (eGov)
- Information Technology and Cyber Security Service (STISC)
- National Anticorruption Center (CNA)
- Public Services Agency (ASP)

Among other stakeholders may be mentioned:

- Local public authorities;
- NGOs, Associations
- Economic operators/ famers;
- Citizens;

The list of the stakeholder might be extended during the detailed Analysis and Design Phase of the Project. The implementation will rely on the so-called partnership approach.

6. Stages of implementing the digital National Farmers Registry

The activities of all 3 components for the design, development, implementation and operationalization of the digital National Farmers Registry, as delineated in this document, must be performed by companies with the necessary experience to perform the appropriate work, within the allocated time of 9 months (June 2023 - Febuary-2024), and will include the following key deliverables:

1. **Concept, legal and regulatory framework.** The Contractor shall develop, validate and test with all stakeholders the IACS concept, vision and framework, with the dNFR as the first implementation phase.
2. **Development and transfer to operations of the digital National Farmers Registry platform (software component developed based on the vision for IACS architecture).** The Contractor shall develop the software for the digital National Farmers Registry (dNFR) of Moldova, ensuring inter-operability with EU requirements for IACS, and local government databases, aligned with general principles as delineated in this document, and according to the existing and new regulatory framework proposed.

3. **Operationalize the digital National Farmers Registry.** The Contractor shall ensure functional coverage and data migration for the Pilot phase scope of farmers.

A timetable which defines the activities implementation shall be submitted as part of the technical proposal.

7. Requirements for completing offers

The competition is open for companies specialized in providing complex services in legal frameworks, data collection and analysis and IT software development services, with at least 5 years of experience in the field. The companies should be legally registered entities and can ensure rapid local response (including presence of staff) to any of the contract related requests (whether though a local branch or office, through a local consortium partner or a local subcontracted consultant or company or other – all relationships to be documented through official documents and valid contracts submitted with the Proposal).

Given the fact that this is a pilot phase of creation of the IACS system in Moldova, it is expected that a lot of interventions will have a testing function to guide further preparation for the national scale implementation. Therefore, it is expected from the bidder a maximum level of agility and flexibility connected to new learnings during the pilot phase implementation of the Registry. Moreover, the bidder should present the possibility of involving a knowledgeable expert with EU IACS to consult the implementation of the registry in accordance with EU requirements.

In the technical offer, the Provider will present the data regarding the personnel involved in the project and their qualification. The involvement of qualified personnel with experience in the development and implementation of digital National Farmers Registries systems of similar complexity within the CPA of the Republic of Moldova is welcome. Requirements for the key personnel are presented in the Request for Proposal, Section 4.

7.1. Description of the Proposed ICT Solution

The Bidder must provide detailed descriptions of the essential technical, performance, or other relevant characteristics of all key Information Technologies, Materials and Services offered in the tender (e.g., version, release, and model numbers). Without providing sufficient clear detail, Bidders run the risk of their tenders to accumulate the minimum technical score.

To assist in the tender evaluation, the detailed descriptions shall be organized and cross referenced in the same manner as the Bidder ’s item-by-item commentary on the Technical Requirements described in Section below. All information provided by cross reference must, at a minimum, include clear titles and page numbers.

7.2. Item-by-Item Commentaries on Components Requirements

The Bidder must provide an item-by-item commentary on Components Requirements, demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to the Requirements.

Failure to do so, increases significantly the risk that the Bidder ’s Technical Tender will result in a lower technical score.

7.3. Preliminary Implementation Plan

The Bidder must prepare a Preliminary Implementation Project Plan describing, among other things, the methods and human and material resources that the Bidder proposes to employ in the design, management, coordination, and execution of all its responsibilities, if awarded the Contract, as well as the estimated duration and completion date for each major activity. The Preliminary Implementation Plan must also address the topics and points of emphasis specified in this document. The Preliminary Implementation Plan shall also state the Bidder ’s assessment of the major responsibilities of the Beneficiary and any other involved third parties in System supply and installation, as well as the Bidder’s proposed means for coordinating activities by each of the involved parties to avoid delays or interference.

In addition to the topics and points of emphasis, the Preliminary Implementation Plan must address all activities listed in the Implementation Schedule.

Confirmation of Responsibility for Integration and Interoperability of Information Technologies.

8. Institutional arrangements

The Service Provider will work under the guidance of the UNDP Project Manager for substantive aspects of the assignment and under the direct supervision of the UNDP Project Officer for administrative aspects.

The Service Provider is expected to cooperate closely with the representative of the Ministry of Agriculture, management, and delegated staffers from the ANSA and AIPA under the Ministry of Agriculture, eGov, STISC and other related Agencies.

All the deliverables shall be submitted in English and Romanian language, in hard copy and electronic format.

Before submission of final deliverables, the Service Provider will discuss the draft documents with the parties involved, so that the final products reflect their comments. All the deliverables of the Service Provider shall be coordinated with the UNDP Moldova Project.

COVID-19 implications

As of 11 March 2020, the World Health Organization (WHO) declared COVID-19 a global pandemic as the new coronavirus rapidly spread to all regions of the world. Travel to and in the country has been also subjected to restrictions of different duration and scope, since March 2020.

The selected Service Provider shall abide by the latest recommendations of WHO and National Commission for Emergency Situations of the Republic of Moldova pertaining to safety measures in the COVID-19 context.

Please note that the Project Team envisages as most the efficient approach for carrying out the assignment the on-site working, in particular when it comes to conducting of activities related to the Analysis and Design phase, as well as when conducting of users’ trainings. When planning and conducting

workshops/meetings with physical presence of participants, the Contractor shall abide by the safety rules and regulations set by the Moldovan authorities in regard to gatherings/meetings at that particular time, ensuring the safety of its staff and those they shall interact with. Hence, no stakeholders, consultants or UNDP staff should be put in harm's way and safety is the key priority.

It is also expected the Contractor to ensure a fast response during the technical support period especially for the most critical issues signaled by the dNFR users. Therefore, it is desirable for the Bidder to have local office or a local consortium partner or a local subcontracted consultant or local subcontracted company in Republic of Moldova which will serve as a local contact point in order to ensure the fastest reaction of the Contractor when so required.

However, in case of limited possibilities to travel or on-site working restrictions due to COVID-19 epidemiologic situation within the country, the Service Provider should develop a methodology to conduct the assignment virtually and remotely, using teleconferencing equipment and tools, including the use of remote interview methods and extended desk reviews, data analysis, surveys and evaluation questionnaires.

In this context while preparing and undertaking interviews, meetings, presentations and briefings through telephone or online (skype, zoom etc.) the Contractor shall work remotely in close coordination with the Project team.

The above noted aspects shall be detailed in the inception report and agreed with the UNDP Project. The limitations like stakeholder availability, ability or willingness to be interviewed remotely, accessibility to the internet/ computer and working from home arrangements must be reflected in the final report.

The Offeror's proposal shall be clear on the activities, costs entailed, and approach proposed to ensure the delivery of the assignment in the current pandemic context whereby objectives of the assignment are met, while enforced safety standards are adhered to.

In line with the UNDP's financial regulations, when determined by the UNDP Moldova Country Office and/or the Service Provider that a deliverable or service cannot be satisfactorily completed due to the impact of COVID-19 and limitations to the assignment, that deliverable or service will not be paid.

However, due to the current COVID-19 situation in the country and its implications, a partial payment may be considered if the Service Provider invested time towards the deliverable but was unable to complete to circumstances beyond his/her control.

Language requirements

All documentation related to the assignment shall be in English and Romanian. All documents submitted, in English and Romanian, will be subject to proofreading and editing to ensure compliance with the language and terminology in the national legislation regulating the subject matter of the assignment.

The Service Provider shall ensure, if necessary, interpretation during interviews, meetings, presentations, and briefings organized through telephone or online, during the missions, to the Republic of Moldova, should these be organized, as well as translation of assignment related documentation and deliverables. All collaborators involved in the project who are deployed directly in the field must have a perfect command of the Romanian language.

Any translation, interpretation and proof-reading costs shall be listed separately in the financial proposal.

9. Minimum technical requirements for dNFR

The functional and technical requirements defined in the current version of the document, represents a minimum / reference requirement for a prospect dNFR system.

These requirements were identified based on the preliminary data gathered during the feasibility study phase and reference experience of other countries developments.

Final requirements document will be developed by the provider, alongside with Providers of Components 1 and 2, upon the development and validation of the deliverables within the related components worksteams, which Provider will be part of.

9.1. Architecture of the National Farmers Registry system

The Registry's architecture can be divided into the following blocks, all of which shall be developed as part of Component 2:

1. Homepage: supply a user-friendly web interface, accessible through an Internet explorer of wide use (*MS Internet Explorer/MS Edge*, *Mozila FireFox*, *Opera*, *Google Chrome* or *Safari*). From a functional point of view, a reliable solution will be developed to be scalable both, in case of increasing number of concurrent users, or in case of increasing volume of information managed by the system.
2. Statistics: display of basic statistical data useful for farmers, local public authorities, the MAFI, etc. Access rights to data for each group shall be designed based on the basis of their defined roles and rights. Data access and management should include functions such as
    a. search tools, to enable search for data within the database
    b. Creation, editing and printing of data. Access rights to data for each group shall be granted based on their defined roles and rights.
    c. Possibility of connecting with other databases within the Government, as well as available GIS databases.
3. Administration: management of the system

Because the IS „dNFR" is not an isolated computing solution, but will interact with other information systems within MAFI and of different public authorities of the Republic of Moldova, the development information system should provide support for integration with third-parties' information systems.

The basis of the IS „dNFR" will be a client-server architecture of minimum 3 levels (which excludes direct interaction of the application with the database) based on adequate WEB technologies from time point of view. To ensure an adequate level of information security, the respective information system should allow a secured connection between the client spaces and application server to ensure a safety level for sent information (through VPN channels and TLS/SSL sessions).

The IS „dNFR" will be installed and will function within the governmental service MCloud.

The solution of cooperating the resources for ensuring the functionality of the IS „dNFR" covers 4 categories of distinct nodes:

1. **MCloud** – ICT infrastructure of the common governmental technological platform, which sets up the governmental cloud (*MCloud*), which is usually hosting all the information systems of the PA in the Republic of Moldova, and where the *IS „NFR"* will be hosted. It should be mentioned that the *IS „NFR"* will consume *MCloud* governmental service. All the connections with external information systems will be mainly carried out through *MConnect* governmental interoperability platform.
2. **MAFI ICT Infrastructure** – - the ICT infrastructure of the *Ministry of Agriculture and Food Industry* (located outside *MCloud*), where the*, IS „NFR" is* hosted*. The IS „NFR"* will not interact directly with these information systems. The interaction will be carried out through *MConnect* interoperability platform/ governmental service.
3. **ICT infrastructure of PSA** – the ICT infrastructure of the *Public Services Agency* hosting the *State Register of Population. The IS „NFR"* will not interact directly with this information system. The interaction will be carried out through *MConnect* interoperability governmental service.
4. **Client computers** – computers from which the authorized and anonymous users (depending on their rights and roles) will access the functionalities of the *IS „NFR".*

To implement a number of functionalities, the IS „NFR" will consume a number of governmental services and APIs provided by governmental and external information systems, as follows:

1. **Authenticate** provided by *MPass* governmental service for authenticating users through electronic or mobile signature.
2. **Sign** provided by *MSign* governmental service for applying the electronic or mobile signature on documents and forms concluded within business processes of cases.
3. **Notify** provided by *MNotify* governmental service for implementing an universal and centralized system for notifying the users of the *IS „NFR"*.
4. **Log** provided by *MLog* governmental service to log sensitive business events produced after the operation of the IS *„NFR"*.
5. **Send open data** which interacts with *Open Data Portal* (https://date.gov.md) for the purpose of publishing the sets of public data produced in business processes of the *IS „NFR"*.
6. **Extract identity data** provided by the *PSR* to complete the human resources profile with official identification and documentation data.
7. **Extract criminal record data** provided by *RCFI* for extracting data regarding the previous criminal record of the person.
8. **Extract integrity record data** provided by the *IS „PAPIR"* for extracting data related to person's integrity record.

9.2. Data model of the information system

To ensure good operation of the *NFR,* it is necessary to implement the functionalities necessary for managing the following groups of information items:

Parcel:	1. Each parcel (as defined as a continuous area of land, where one single crop group is farmed) shall receive a **unique geographical identification number** 2. Region/raion / code of the territory

	3. Land tenure type (property, lease, communal land, ….) 4. Agricultural activity
Farmer	1. each farmer shall be matched to a unique identification number 2. Contact information (address; email; phone, …) shall be included 3. Farmer type shall be included (natural person, legal person; group of natural persons, group of legal persons; …) *4. Machinery owned?*
Agricultural activity (for each parcel unit) Pre-loaded values aligned with Moldovan and EU regulations	1. crop type 2. irrigation method (surface; localised; drip; sprinkler; center pivot; manual,..) 3. water origin (?) 4. fertilisation method (broadcasting, foliar, placement, fertigation, no fertilisation) 5. fertiliser type a. see Regulation (EU) 2019/1009, Annex 1. 6. labour type (regular unpaid; regular paid; casual unpaid; casual paid) 7. Organic farming – type of organic certification (certified, non-certified, in transition, …) 8. Certification related to management of livestock and animals a. ó livestock identification system (for EU imports, phytosanitary requirements) 9. Other type of farming certification 10. Other information relevant to agricultural activity 11. start and end date (ó to support when / until when to provide subsidies)
Production unit	1. All parcels used for agricultural activities by the same farmer

Analyzing the modelled area, it is possible to delimit the totality of information items to be taken into account when developing the *IS NFR"*.

To ensure good operation of the *IS „NFR",* it is necessary to implement the functionalities necessary for managing the following groups of information items:

A. ***Contest application form***. Represents an information item through which the data related to contest application forms are stored. These applications are concluded based on some specialized forms which cover the following categories of data:
   a. Application identifier;
   b. Date the application was sent;
   c. Content of the application questionnaire;
   d. Documents annexed to the application;
   e. Testing/evaluating forms related to the application;

B. ***Receipt***. Represents an information item through which the data related to the receipts delivered to contest participants - confirming receipt of the request to participate in the competition.

C. ***Document attached to evaluation case file***. Represents an information item through which the data related to the electronic copies of the documents attached to the human resource evaluation case file are stored. The following categories of data are characterizing this information item:

a. Document identifier;
b. Document name;
c. Document type;
d. Evaluation case file;
e. Document loading date;
f. Document location route;
g. Document related file.

D. ***evaluation form***. Represents an information item through which the data related to the electronic forms are evaluated The following data categories are characterizing this information item:

a. Form identifier;
b. Evaluation type;
c. Evaluation modality;
d. Evaluated person/entity data;
e. Evaluation case file;
f. Form category (according to the classifier of electronic forms set up in the *IS „NFR"*);
g. Evaluation questionnaire content data;
h. Timetable envisaged for evaluation;
i. Evaluation start date, hour, minute;
j. Evaluation end date, hour, minute;
k. Form sending date, hour, minute;
l. Electronic signature (if it is the case).

E. ***Evaluation report form / endorsement***. Represents an information item through which the data related to the electronic forms of Evaluation Reports/Endorsements concluded. The following data categories are characterizing this information item:

a. Form identifier;
b. Period planned for conclusion:
c. Form type;
d. Form category (according to the classifier of electronic forms set up in the *IS „NFR"*);
e. Form data;
f. Electronic evaluation form related to the Evaluation Report/Endorsement;
g. Form sending date, our, minute;
h. Electronic signature (if it is the case).

F. ***Approval/rejection form***. Represents an information item through which the approval/rejection events are registered. The following data categories characterize this information item:

a. Event identifier;
b. Sending date, hour, minute;
c. Qualifier (approval/rejection; fit/not fit; promoted/not promoted, etc.);
d. Informative note;

e. Relevant electronic form draft;
f. Electronic signature.

9.2.1. Profiles

Complex information item, which defines the totality of profile information which is necessary for operating the *IS „NFR".* The profiles of the information system are defined by the following categories of information items:

Individual person's/legal entity's profile. Represents registration data of any individual/legal entity which is the object of an evaluation case (case authorized users). As a rule, the completeness level of an individual's profile depends on his/her role and contains the following categories of data:

a. IDNP/fiscal code;
b. Name;
c. Surname;
d. Patronymic;
e. Sex;
f. Post address (domicile/residence);
g. Telephone contacts;
h. Email contacts;
i. Held identity acts' data;
j. Family composition data;
k. Biometrical data;
l. Biographic data;
m. Person's private data;
n. Religious peculiarities' data;
o. Education data;
p. Employment data;
q. Criminal record data;
r. Administrative record data;
s. Integrity record data, etc.

Authorized person profile. Represents profiles of authorized users of the information system, who will be involved in the business processes of the *IS „NFR"* or will need access to evaluation case file details (represents case authorized persons). The following data should be able to be managed for the profile of the authorized person:

a. Access credentials;
b. Reference to individual person's/legal entity's profile (personal and contact data);
c. Authentication strategy/restriction (user + password, electronic/mobile signature, PI access address, etc.);
d. Access validity period;
e. Held roles;
f. Profile status.

9.3. Business roles of the information system

In line with the legislation in force, the following entities of the Republic of Moldova are interested or should be involved in the development and good functioning of the *IS „NFR"*:

1. **Ministry of Agriculture and Food Industry (MAFI)** – as the entity responsible for implementing and ensuring the good operation of the *IS „NFR". MAFI* is the direct beneficiary of the *IS „NFR",* and the MAFI together with UNDP is the co-financer of the project which will take an active part at all the stages of design, development, production and operation of the information system.
    a. **The Agency for Intervention and Payments in Agriculture (AIPA)** - administrative authority under the MAFI tasked to manage financial resources to support agricultural producers, monitoring of funds' distribution, quantitative and qualitative evaluation of the impact of support measures to farmers by the state.
    b. **The National Agency for Food Safety (ANSA)** - administrative authority under the MAFI tasked to ensure the monitoring the state of health of domestic and wild animals/birds that is very important for knowing the state of health at the national level and for preparing analyzes regarding the risk of passing certain diseases from wild animals to domestic ones.
    c. **The National Office for Wine and Vine (ONVV)** - administrative authority formed as a public-private partnership tasked to manage the Moldovan wine sector, which contributes to the regulation and sectors' development acting as a platform for joint action of all those involved in increasing the competitiveness of wine products, capitalizing on authenticity and consumer orientation and those engaged in promoting Moldovan wines through the program and the national wine brand "Wine of Moldova – A legend alive".
2. **The Agency for Land relations and Cadaster** – overall responsibility of the Agency is to ensure the quality and transparency of land management in the Republic of Moldova via the registration of immovable public and private property, and the valuation of real estate.
3. **National Anticorruption Center** – as the public authority responsible for evaluation of institution integrity, evaluation of public agents' integrity and issuance of integrity records requested during the subsidy process.
4. **Public Services Agency** – as provider of data related to identity, identity acts and biometric data related to the candidates/citizens to benefit from agriculture subsidy program stored in the *State Register of Population*.
5. **Electronic Governance Agency** – as the body empowered with *e-Transformation* activities. *The Electronic Governance Agency* will ensure access to the interoperability governmental service *MConnect* and access to governmental service of *MCloud (MPass, MSign, MLog, MNotify)* and *Open Data Portal.* As well, the *Electronic Governance Agency* will provide the infrastructure for hosting the *IS „NFR"* within the common governmental technological governmental service *MCloud.*
6. **Information Technology and Cyber Security Service** as an entity which manages the common governmental service *MCloud* hosting the *IS „NFR",* as well as hosting the platform services with which the *IS „NFR"* will have to get integrated.
7. Other relevant institutions, if identified.

9.3.1. Owner of the information system

The owner of the *IS „NFR"* is the MAFI. As the owner of the *IS „NFR", the MAFI* will be able to attribute roles and rights to authorized persons, to operate the information system depending on their service duties. As well, the MAFI through the *IT Service of the MAFI*will ensure the totality of support activities, maintenance and continuous development of the *IS „NFR"*.

9.3.2. Holder of the information system

The holder of the *IS „NFR"* is the *Information Technology and Cyber Security Service,* because it holds the common governmental technological governmental service *MCloud* which will host the information system. The *ITCSS* will be responsible, as well, for solving the totality of technical problems related to operation of the *IS „NFR"*.

9.3.3. Administrator of the information system

The administrator of the *IS „NFR"* is one or more persons appointed by the MAFI (as a rule, employees of the *ITS*). The whole administration of the content in the IS *„NFR"* will be carried out by specialists from the MAFI. As well, at the level of the technical infrastructure of hosting the *IS „NFR",* the administration functions will be exercised by the *ITCSS.*

9.3.4. Registrar of the information system

The registrars of the *IS „NFR"* shall be the MAFI.

9.3.5. Purchaser of the information system

The purchaser of the information system *IS „dNFR"* is the UNDP Moldova and the Ministry of Agriculture and Food Industry.

9.4. User interface of the information system

The *SI „NFR"* should provide an ergonomic and intuitive user interface, accessible to all types of users. The user interface of the information system will be accessed through an Internet browser. The *IS „NFR"* should have an intuitive, acceptable, balanced, distinct and optimized graphic design for the minimum work resolution 1360x468 for PC type computers. As well, the user interface should be responsive to resolutions for such devices as smartphones and tablets, and optimized for tactile screens.

For users' easiness, the information solution will have a system of online contextual assistance, at the level of every user interface.

Depending on the users' categories (their rights and roles), the information system will provide a personalized interface for every user category.

The *SI „NFR"* will provide a user interface in Romanian language. The procedures for finding information and entries will be carried out through a simple search (specifying search ranges) or some higher complexity searches, through which a more accurate filtering of information may be carried out (QBE forms). Regardless of the nature of searched for information, the user will use the same method of interrogation and finding information for any compartment of the information product.

Additionally, to the search module based on QBE principle, which will give the possibility to define visually sophisticated interrogations, the interface should provide the possibility to deepen the search results by ensuring the possibility of filtering the data in the list with search results.

The user interface of the information system should ensure the filtering of entries which meet the search criteria presented to users depending on their access rights.

There should be a possibility to filter indexed measures (classifier values, nomenclatures), by choosing the value from predefined lists. For numerical or calendar date type fields, there should be a possibility to filter by exact value of the searcher for characteristic or by search mask.

The content of any table with results or electronic form, depending in the nature of the contained information, there should be a possibility to export them in the following formats CSV, XLS/XSLX and PDF. The data export should be strictly delimited by roles. All the data export actions will be logged.

9.5. Functional requirements

9.5.1. Requirements of the interoperability framework of the National Farmers Registry

Interoperability with the following databases shall be ensured, namely:

1. e-ANSA for phytosanitary licenses
2. Animals Registry – this Registry will be interconnected with the National Farmers Registry
3. Businesses Registry
4. National Wine Registry – this Registry will be interconnected with the National Farmers Registry
5. National Cadaster
6. State Hydrometeorological Service
7. State Fiscal Service
8. Other relevant existing databases (AIPA subsidies register, ODA registries, Council of Competition registries, etc.)

Agreements on formulation of functional**, non-functional and other requirements**

The requirements set in this document are marked using the following conventions:

- all the requirements are indexed with 3 values **C.X.Y**, where **C** represents the category of the requirement (as per table below) **X** represents the use case for which the functional requirement is formulated, and **Y** is the single identifier of the requirement in the use case of which it is a part.
- the binding nature is mentioned for every functional requirement: M – mandatory requirement, D – desirable to be implemented, optional requirement.

	Meaning	Interpretation
CF	Functional requirement	Functional requirements of IS „NFR" implementation
CNF	Non-functional requirement	General requirements of IS „NFR" implementation.

PERF	Performance requirement	Requirement refers to operation performance of the IS „NFR".
SR	Scalability requirement	Requirement refers to the scalability properties of the IS „NFR" to increase the number of users, transactions or volume of processed data.
SHC	Platform requirement	Requirements for the software platform, hardware and communication channels necessary for the operation of the IS „NFR".
LIPR	Licensing and intellectual property requirements	Requirements refer to intellectual property rights related to the IS „NFR" and soft components necessary for the operation of the SI „NFR".
INT	Interoperability requirement	Requirement refers to the interoperability framework of the IS „NFR".
MIG	Data migration	Requirement refers to the data migration within of the IS „NFR".
SEC	Security requirement	Requirement refers to aspects of ensuring information security to be met by the IS „NFR".
DEP	Deployment requirement	Requirement refers to deployment of the IS „NFR".
DOC	Documentation requirements	Requirement refers to documentation of the IS „NFR".
GMS	Guarantee, maintenance and post-implementation support requirement	Requirement refers to characteristics of the services for operational maintenance and post-implementation development of the *IS „NFR"*, requested within the procurement.

The proposal submitted by the *Provider* should meet on binding basis all the requirements indicated as mandatory.

The informative requirements are meant to provide more information, for a better understanding of the context of other requirements.

Functions available within the NFR

Function	**Local public authority**	**Ministry official / MAFI**	**Farmer**	**System administrator**
Search	Search for all data	Search for all data	Only data ***	Search for all data
Create	Editing rights for farmers of its own municipality/mayoralty	Available for all data	Only creation of profile, and input for own	Available for all

			**; one user is related to one unique identification number	
Edit	Editing rights for farmers of its own municipality/mayoralty	Available for all data	To be defined	Available for all data, including deletion of users and entries
Print	Only available for data related to own municipality/ raion	Available for all data	Only available for data related to own unique identification number	Available for all data
Statistics	Only available for data related to own municipality/ raion	Available for all data	Only available for data related to oneself, based on unique identification number.	Available for all data

9.5.2. Functionalities of the information system

CF 1: Receive notifications

Use case through which the users of the *IS „NFR"*, regardless of their role, will receive the notifications sent by the *IS „NFR"* in relation to the business events in which they are involved.

The functional minimum requirements of the mechanism meant to receive notification sent by the *IS „NFR"* to authorized users are presented below.

Identifier	Binding nature	Description of functional requirements
CF 1.1	M	IS „NFR" will notify automatically any authorized user in case of registering a business event which implies any actions from the user or which modifies the status of processes which are managed, monitored by him/her or refer to him/her.
CF 1.2	M	Authorized users will receive notifications at the email address indicated in their profile in the IS „NFR".
CF 1.3	M	A copy of the notification will be displayed in the Dashboard of the authorized user in the IS „NFR" (if applicable).
CF 1.4	M	The authorized user IS „NFR" will have the functionality to set up preferences for receiving notifications (on email or in Dashboard).

CF 1.5	M	IS „NFR" will send the entire range of notifications meant for authorized users.
CF 1.6	M	A notification sent through Email may contain an attached file (*example: receipt.*).
CF 1.7	M	Users of the IS „NFR" will receive notifications through Email in HTML format or enriched Text Format.

CF 2: Use Dashboard

Use case which providing all the functionalities which are necessary for the setup of the use dashboad. *The IS „NFR"* will provide facilities to set up the dashboad, taking as basis the primary data provided.

The functional minimum requirements meant for the operation of the Dashboard meant for authorized users of the IS „NFR" are presented below.

Identifier	Binding nature	Description of functional requirement
CF 2.8	M	IS „NFR" will provide the authorized users a Dashboard through which they will be notified about important business events and will provide rapid access to their details.
CF 2.9	M	The following business events displayed on the Dashboard may be listed: ● system notifications; ● notifications regarding the need to involve the user in the activities of the work flows of the IS „NFR" (including delay alerts); ● notification regarding the forms or documents waiting to be approved by decision-making roles (including delay alerts); ● notification about filling in the evaluation case file with new documents or electronic forms; ● notifications on acceptance/rejection of electronic forms' drafts; ● other relevant events.
CF 2.10	M	The dashboard of the US „NFR" user will display only business events relevant for the roles and data available for the authorized user.
CF 2.11	M	The dashboard of the user with the role of System Administrator will display all business events related to the functionalities of the IS „NFR" (totality of notifications displayed in the Dashboard of all the users of the IS „NFR" and notifications dedicated exclusively to the user with role of System Administrator).

CF 2.12	M	The dashboard will group business events displaying them in the form of indicators with aggregated values (*example: Unread system notifications -20; Open evaluation cases – 20, Forms under work – 10; Forms sent for approval – 2; etc.*) which will content hypertext reference to access details.
CF 2.13	M	IS „NFR" will display detailed entries of the Dashboard in specialized windows or fields on the main page of the user's interface, which will have hypertext reference for accessing details (example: opening the form which has generated the notification).
CF 2.14	M	When accessing the hypertext reference related to the aggregated value or detailed entry of the Dashboard, the IS „NFR" will ensure access to detail information related to it or requested functionality (*example: content of the psychological evaluation test, direct approval/rejection of the forms sent for review and approval, etc.*).
CF 2.15	M	The dashboard of the IS „NFR" will have a specialized field (favorite) where the user will place references to the content information on which he/she works. They can be of 3 types: ● open/closed evaluation cases; ● performed electronic forms (business events related to currently performed evaluation cases); ● reviewed electronic forms (agenda or business events related to reviewed evaluation cases).
CF 2.16	M	IS „NFR" will provide to every user the functionality of individual setup of the Dashboard aspect and content.

CF 3: Search/view data

Use case provided by the *IS „NFR"* through which the authorized users will be able to explore the stock of data to which they have access based on the role held in the information system and service duties.

In this respect, the *IS „NFR"* will provide a mechanism for searching evaluation case files and their content, using different criteria, such as:

1. Person's/legal entity's identification data;
2. data related to the users authorized for the case;
3. data for identifying the evaluation case;
4. calendar data related to the evaluation case files;
5. calendar data related to the business events' forms of evaluation case files;
6. data related to business events related to the evaluation case;
7. Person/legal entity status;
8. evaluation case status;
9. etc.

SI „NFR” will display as found results:

10. Persons/legal entitys;
11. evaluation plans;
12. evaluation case files;
13. business events of evaluation cases;
14. documents attached to evaluation cases.

For every result category, the *IS „NFR”* will allow performing the following manipulations:

15. for found persons: viewing person's profile, viewing evaluation cases related to the person, viewing business events' documents which are related to the evaluation case;
16. for evaluation cases' files: accessing the content of the evaluation case file, generation of case file;
17. for business events of evaluation cases: viewing the document related to the event, accessing the electronic form of concluding a business event, approving/rejecting the form, generating the document related to the business event;
18. for evaluation plans: viewing plan, approving/rejecting the plan, generating the document related to the plan.

It is appropriate for the *IS „NFR”* to provide a mechanism for indexed search of data and presentation of results depending on the relevance of the results of the formulated query.

The functional minimum requirements related to the mechanism of searching for data stored in the database of the IS „NFR” are presented below.

Identifier	Binding nature	Description of functional requirement
CF 3.17	M	IS „NFR” will provide a mechanism to search for data and documents in the stored data content.
CF 3.18	M	IS „NFR” will provide a mechanism for indexed search of data. The search mechanism will use morphological means.
CF 3.19	M	IS „NFR” will allow defining the following search targets (the search result will display the list of): ● evaluation case files; ● documents contained in the evaluation case files; ● concluded electronic forms concluded and contained in the evaluation case files.
CF 3.20	M	IS NFR” will provide a flexible and efficient mechanism to define search criteria.
CF 3.21	M	In case of formulating too wide search criteria, or criteria which need too much time and resources for execution, the IS „NFR” will not execute these queries, but will request the user the narrow the area of searched for values.

CF 3.22	M	The search results will be ordered depending in the relevance of the search query result, alphabetically or creation date/last update.
CF 3.23	M	The user will be able to define criteria for ordering or grouping the content of the list with search results.
CF 3.24	M	IS „NFR" will provide a mechanism for paging the search results meant to avoid the overloading of web explorer and data transportation channels.
CF 3.25	M	The search results' entries will be marked (specific color or icon) depending in the nature or status of found informational item.
CF 3.26	M	IS „NFR" will provide the functionality of refining the search in found results.
CF 3.27	M	IS „NFR" will allow initiating some processes regarding the found results or a group of found and marked results, such as: ● selecting the entries of search results; ● initiating the creation of business event form including the results in the form or in the base of selected entries (*example: including a group of human resources' profiled in an evaluation plan*); ● changing the entry's status; ● multiple deletion; ● multiple electronic signing; ● other relevant actions.
CF 3.28	M	IS „NFR" will restrict the access to found results' details when the use who has initiated the search process does not have access to the information items requested to be accessed.
CF 3.29	M	IS „NFR" will allow exporting the table with the search results in CSV or PDF formats.

CF 4: Generate documents and reports

Functionality accessible for authorized users of the *IS „NFR"* which allows generating pre-established and ad-hoc reports regarding the information content of the information system and activity of authorized users.

These reports are useful for producing documents and reports specific for the REC activity, analysis of the information basis of the information system, performance of authorized users' activity, in particular, and of the entities they represent, in general, hence allowing extracting some performance indicators meant to analyze business processes.

It is appropriate for the information system to integrate a solution dedicated to setup and generation of reports (reports' generator), which would be reused, as well, for setting up and extracting the standardized documents specific for business processes of the *IS „NFR"*. The documents may be generated, as well, based on some configurable templates.

The functional minimum requirements of the mechanism to extract documents and reports to be presented in a user-convenient form or for assisting the work flows and the decision-making process are presented below.

Identifier	Binding nature	Description of functional requirement
CF 4.30	M	IS „NFR" should be able to provide a number of statistical and ad-hoc reports, for the decision-makers.
CF 4.31	M	It is appropriate for the basis to generate reports to be a dedicated platform meant to set up dynamic generation of reports (*example: JasperReport*).
CF 4.32	M	IS „NFR" should provide to MAFI decision-makers a predefined number of documents/reports which may be configurable and upon request, so as to ensure the production of ad-hoc reports, if needed.
CF 4.33	M	IS „NFR" will provide a set of documents to be generated based on data stored in the database of the information system, as follows: ● application for participation in the contest; ● evaluation report; ● own responsibility declaration; ● criminal record; ● integrity record; ● system notification; ● other relevant documents.
CF 4.34	M	IS „NFR" will have predefined (editable) templates for every type of generated document necessary for the eventual update of generation rules.
CF 4.35	M	IS „NFR" will allow drafting documents in electronic format, applying the digital signature of REC or MAFI.
CF 4.36	M	Developer will implement up to 25 documents to be generated by the IS „NFR". The complete list of documents will be identified during business analysis.
CF 4.37	M	IS „NFR" will provide a set of reports to be generated based on the data stored in the database of the information system, as follows:

		● Performance report of the IS „NFR” (statistical data regarding the current content of IS „NFR”) with different principles of aggregation (according to the MAFI subdivision, etc.); ● The performance report of the authorized user, containing statistical data and details regarding newly-opened evaluation cases, under operation cases and closed cases for a determined period of time with a different level of aggregation; ● Form of evaluation case file (a synthesis of data from all business events' forms of the evaluation case file); ● Report on evaluation cases (according to subdivisions, according to time periods, according to type of evaluation, according to evaluation result); ● Evaluation tally sheet; ● Evaluation report/endorsement; ● Extract from the Evaluation Register; ● Other relevant reports.
CF 4.38	M	IS „NFR” will have a mechanism for defining the set of reports and data available for every category of users, depending on their roles and rights.
CF 4.39	M	A user viewing a report in the system, should be able to export it to an external editable file (XLS/XLSX și DOCX).
CF 4.40	M	Implicitly, the reports will be extracted in PDF format.
CF 4.41	M	The developer should implement up to 25 categories of predefined reports requested by the beneficiary, including the ones specified in CF 11.08.
CF 4.42	M	IS „NFR” will log all the events for generating and printing out reports and documents.

CF 5: Approve/reject forms

Use case available to users with decision-making role in the *IS „NFR”* through which he/she will be able to approve or reject draft electronic forms and documents specific for business cases.

The approval or rejection of the electronic form implies the conclusion of an endorsement/comment, selection of approving/rejection options and applying electronic signature of the user with decision-making role.

The functional requirements of the component meant for decision-making roles to approve or reject the electronic forms concluded through the *IS „NFR”* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 5.43	M	IS „NFR" will provide the authorized stakeholders (REC decision-makers) a mechanism to approve or reject the drafts concluded by REC Specialists which need approval before being saved or processed.
CF 5.44	M	Preventively, the following draft documents (electronic forms concluded by REC Specialists) shall be approved by decision-making roles in IS „NFR": ● new/modified test to be launched in production; ● test to be extracted from production.
CF 5.45	M	The complete list of electronic forms needing approvals from the decision-making roles will be identified in the business analysis process.
CF 5.46	M	Approval or rejection implies providing a grade, selecting a status (approved or rejected), its conformation and applying the electronic signature by the user with decision-making role.
CF 5.47	M	Access to the functionality for approving/rejecting the draft will be possible if the user with REC decision-making role also has empowerment (verification is done through MPower).
CF 5.48	M	IS „NFR" will use the MSign governmental service for applying the electronic signature for approving/rejecting the electronic form.
CF 5.49	M	If the electronic form is approved, the IS „NFR" will notify all relevant users regarding the approval/rejection event.
CF 5.50	M	If the electronic form is rejected, the work flow will switch automatically to the previous stage (will return to concluding the form of the user who has sent it for approval) and will notify all the relevant users.
CF 5.51	M	When a form is sent for approval, it can be modified only by the decision-maker who has to approve it, by repeated application of the electronic signature.
CF 5.52	M	IS „NFR" will log all the events for approving/rejecting the draft electronic forms.

CF 6: Generate statistics and system reports

It is a use case providing functionalities which are necessary for users at the level of *System Administrator* to generate predefined and ad-hoc statistical reports regarding the events for operating the *IS „NFR"*.

These reports are useful for analyzing the carried out processes, information basis of the information system, performance of authorized users' activities, allowing to anticipate information security problems.

The functional minimum requirements for the component of extracting reports for the purpose of IT audit of the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 6.53	M	*IS „NFR"* should provide a number of management, statistical, and ad-hoc reports for the administrative roles to have the possibility to monitor the activity and the status of the system.
CF 6.54	M	The reports managed are meant for IT audit functions and do not include reports related to business event related to human resources' evaluation cases.
CF 6.55	M	This reporting is necessary within the entire system, including: ● nomenclatures and classifiers; ● database entries; ● user's activity; ● access and security permissions.
CF 6.56	M	Reports will be generated based on the following categories of logged events: ● successful login of users; ● unsuccessful login of users; ● sent notifications; ● actions on data (accessing, adding, modifying, eliminating).
CF 6.57	M	*IS „NFR"* will allow extracting reports in an aggregate way or detailing them per specific user, central or territorial subdivision of MAFI or some groups of users.
CF 6.58	M	A user who views a report within the system, should be able to export it in PDF format or external editable file (XLS/XLSX, CSV, DOC/DOCX).
CF 6.59	M	The developer will implement up to 10 predefined reports got IT audit, requested by MAFI. The audit reports that may be generated through system means will not be implemented in the user interface of the IS „NFR".
CF 6.60	M	To extract reports and statistics from the system, which are relevant for UC16, it is welcome to use platform dedicated to setting up and generating reports.

CF 7: Manage users, roles, rights

Use case providing functionalities for managing users and their credentials (including specification of users' authentication strategy). As well, the *IS „NFR"* will allow the authentication and authorization of users through the *MPass* governmental service.

The information system will provide functionalities, through which the roles and rights associated to them are managed, and which subsequently will be attributed to the authorized users of the *IS „NFR".* The access rights to the user interface and database entries will be defined depending on the user-related role or explicitly for every separate user.

For specific roles, the access rights to human resources evaluation case files will be attributed explicitly through business events' forms or by users with administrator role.

The functional minimum requirements of the component related to managing users and setting up access to user interface and database content of the *IS „dNFR" whch* shall be administered through MPass, are provided below.

Identifier	Binding nature	Description of functional requirement
CF 7.61	M	IS „dNFR" will have a mechanism to define and manage dynamically the users, their roles and rights.
CF 7.62	M	IS „dNFR" will include a default category of users created by the developer and the credentials will be provided upon delivery for the category of **super-administrator**.
CF 7.63	M	IS „dNFR" will allow blocking/unblocking the user's access.
CF 7.64	M	IS „dNFR" will provide authentication in 2 levels (2FA) and will use primarily the MPass governmental service for authentication of users through electronic or mobile signature.
CF 7.65	M	IS „NFR" will allow specifying the modality for user to get connected to the system (electronic/mobile signature, user name + password, IP address or a combination of these).
CF 7.66	M	The following categories of data will be able to be managed within users' profiles: ● user name; ● user surname; ● email of contact; ● telephone of contact; ● access login; ● access password; ● authentication strategy (user + password, electronic signature /mobile signature, authentication in 2 levels (2FA), LDAP etc.); ● activated/inactivated account; ● access validity period;

		● users' roles; ● users whom I temporarily replace; ● users who temporarily replace me; ● other relevant data.
CF 7.67	M	IS „NFR" will provide a mechanism to define the users' rights to access data depending in the categories or types of concluded electronic forms and cases in which the authorized user is involved.
CF 7.68	M	A profile of authorized user may be deleted physically from the IS „NFR" only if there are no logged events or entries related to it.
CF 7.69	M	The mechanism of managing users' rights and roles will allow formulating the principles of access to the components of the user interface and the information content of the information system for every user, separately, or group of users.
CF 7.70	M	IS „NFR" will provide user interface and information content only based on the rights and roles held by users.
CF 7.71	M	The information system will allow setting up an unlimited number of roles.
CF 7.72	M	One role is defined through generic name, brief description and active/inactive status. Inactivated roles will not be displayed when setting up the access rights to the application resource or users' rights.
CF 7.73	M	After being introduced and activated, the role will be available to be used in the modules for users' management (attributing users' roles) and components' management in IS „NFR" (attributing roles that have access to components of user's interface and setting up their access modalities).
CF 7.74	M	It will not be possible to delete a role, it if is attributed at least to one user or to one component of the user interface of IS „NFR".
CF 7.75	M	IS „NFR" will provide a mechanism for registering the components of user interface (resources) for the purpose of ensuring a mechanism to define users' access rights to user interface. A component means any modular entity of the application (form, menu, menu option, field, etc.), whose detail level is enough to set up the access rights, transition of workflows or actions accessible to users.
CF 7.76	M	IS „NFR" will allow setting up the hierarchy of user interface components, having at the root level the basic modules of the application, and the subordinated levels will not be limited in depth, with the hierarchy determined by their architecture.

CF 7.77	M	Any component of the user interface in IS „NFR" will contain data regarding the generic name, brief description, actions available to users (business events they can generate), roles that have access to the user interface or actions that may be undertaken.
CF 7.78	M	Any component of the user interface in IS „NFR" will contain data regarding the status through which the data pass when managed through the component, transitions for going through the component status (setting up workflows).
CF 7.79	M	IS „NFR" will allow defining permissions related to actions a (business events) available to users with access to user interface components. The following categories of actions available to users will be set up: ● viewing the entry; ● adding an entry; ● changing an entry; ● deleting an entry; ● workflow transition; ● other relevant actions.
CF 7.80	M	IS „NFR" will allow setting up the log strategy for business events generated by each component of user interface.

CF 8: Configure flows and document templates /reports

Represents a use case meant for *System Administrator* that provides the totality of functionalities available for configuring work flows, and models of standardized documents/ statistical reports necessary for printing out entry or exit documents (setting the area letterhead, footnotes, static and dynamic content, formatting, graphic aspect, etc.) and of statistical reports.

The functional minimum requirements of the component for setting up workflows, electronic forms meant to insert data and templates of documents, which will be populated with data and generated in the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 8.81	M	IS „NFR" will have a mechanism to manage program resources (modules, electronic forms, menu options, buttons, etc.) to set up workflows and define processing rules for all scenarios related to processes of concluding and processing electronic forms related to human resources' evaluation cases.

CF 8.82	M	It should be possible to manage the workflows using the graphic interface of the information system in which the user works in a usual way.
CF 8.83	M	The workflows will be defined by specifying the statuses through which an electronic file can pass through and the processing steps (development stages or transitions of the workflow which may be carried out in a specific status of the form) carried out by users with specific roles.
CF 8.84	M	A workflow will be implemented as a collection of activities through which would pass an electronic form concluded within business processes which are carried out sequentially.
CF 8.85	M	The number of steps that may be include in a flow should not be limited. In this way, the computing solution will be adjustable to the changes in the working methodology with the documents processed within the human resource evaluation case file's procedures.
CF 8.86	M	A workflow should be able to have an associated coordinator (supervisor). The coordinator should be able to receive warning messages (notifications) generated by the respecting flow rolling. The user who launches a processing form for a workflow should be able to specify who the flow supervisor is.
CF 8.87	M	The developer will set up the processing flows of the electronic forms meant for concluding all the business events related to' evaluation cases.
CF 8.88	M	IS „NFR" will provide mechanisms for configuring the document templates (and reports) related to the generated documents, based on the completed electronic forms (the templates will have a well-defined structure that will allow changing the appearance and content of the extracted document).
CF 8.89	M	Document templates are welcome to be configured through a reporting and configuration platform (Example: JasperReports).
CF 8.90	D	All the templates of documents set up through CF 15.09 - CF 15.10 will be used when generating documents through CU11.
CF 8.91	M	Upon the request of the Beneficiary, the developer will set up to 20 templates of documents to be generated by the IS „NFR".

CF 9: Manage metadata

Use case that provides to users with the role of *System Administrator* access to functionalities which are meant to manage metadata which are necessary to set up the functioning parameters of the *IS „NFR"* (classifiers, nomenclatures, constants, parameters for setting and operating the information system). The developer will use on priority basis the official classifiers of the Republic of Moldova, when necessary.

The functional minimum requirements necessary for managing the metadata of the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 9.92	M	IS „NFR" will have a mechanism for managing the nomenclatures, classifiers which contain the totality of metadata meant for setting up the system and managing the processes events.
CF 9.93	M	IS „NFR" will not allow eliminating a category of metadata, if it is used at least in one entry of the database.
CF 9.94	M	IS „NFR" will provide a mechanism for having versions for the metadata values and establishing the time interval related to validity of metadata values.
CF 9.95	M	The developer will ensure the update of the classifiers in automated regime, if such facilities are provided by the information systems with which the IS „NFR" is getting integrated *(example: State Register of Population*).
CF 9.96	M	IS „NFR" will allow setting up linear and hierarchical classifiers (in which some values may have parent categories).
CF 9.97	M	IS „NFR" will provide a mechanism to export and import classifiers from the user interface in XML or CSV format. The import and export rights will be attributed to users with the role of System Administrator.
CF 9.98	M	IS „NFR" will provide a mechanism from the user interface with the role of System Administrator to set up variables of general configuration of the system

CF 10: Other administration activities

Represents a use case meant for the *System Administrator,* which describes the totality of functionalities meant to manage and audit the *IS „NFR"*: configuration of operating parameters of the *IS „NFR",* configuration of parameters to integrate with the APIs exposed by third information systems, exploration of logged events, extraction of reports from system registers to analyze and identify eventual logical or physical security problems in the *IS „NFR"* etc.

The use case for administration of the *IS „NFR"* will implement the totality of functionalities to ensure the viability and integrity of the information system.

The functional minimum requirements regarding other categories of activities to manage the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 10.99	M	IS „NFR" should allow administrative roles to take over, display and reconfigure the operational parameters and the general system settings.
CF 10.100	M	IS „NFR" will allow the users with System Administrator role to set up access to APIs provided by external information systems with which IS „NFR" interacts.
CF 10.101	M	System Administrator will have a specialized interface to access and analyze systems logs of the IS „NFR".
CF 10.102	M	IS „NFR" will provide an interface meant to monitor the current functioning of the information system and analyze the loading level or identify the possible operational problems.
CF 10.103	M	System Administrator will be able to generate, upon request, backup copies of the IS „NFR" and to establish the functionality of the information system based on the backup copies generated manually or automatically.
CF 10.104	M	IS „NFR" will provide the functionality of archiving and excluding historical data to be deleted according to the legislation in force.
CF 10.105	M	IS „NFR" will provide the System Administrator with all functional facilities necessary to ensure the functionality of the information solution in good conditions.

CF 11: Execute automated procedures

Represents a use case through which the *IS „NFR"* will execute automated procedures with a certain periodicity or upon occurrence of a business event. *System Administrators* will have facilities to set up parameters for initiating and operating automated procedures.

The following can be mentioned under these procedures:

1. generation of backup copies;
2. data archiving;
3. initiation of evaluation cases;
4. erasing forms which exceeded the deadline of being under the status „Draft";
5. calculation of complex KPI necessary for generating complex statistical reports;
6. other categories of automated procedures.

The functional minimum requirements of the mechanism for executing the automated tasks necessary for operation of the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 11.106	M	IS „NFR" will have a component of executing automated procedures (jobs) launched with a certain periodicity and at a certain point in time.
CF 11.107	M	IS „NFR" will have the functionality of setting up the automated procedures (performed action, periodicity and the moment of launching the automated procedure etc.).
CF 11.108	M	IS „NFR" will provide the mechanism for automated generation of backup copies (according to some pre-established rules) based on which it will be possible to re-establish the functionality of the information system if any security incidents occur.
CF 11.109	M	IS „NFR" will provide the mechanism for archiving old data, which are useless for current business processes of the REC and removing them from the production platform.
CF 11.110	M	IS „NFR" will automatically trigger, if necessary, the procedures of mutual data exchange with external information systems defined through CU22.
CF 11.111	M	IS „NFR" will delete automatically the electronic forms in „Draft" status, which have exceeded the deadline of being in this status set up through CU15.
CF 11.112	M	IS „NFR" will be able to perform periodically and in a planned manner (in hours of minimum demand for the IS „NFR") the preliminary calculation of the indicators which are necessary to generate in useful time complex statistical reports.
CF 11.113	M	IS „NFR" will publish periodically within the Data Portal public reports and KPI produced during the implemented business processes.

CF 12: Log events

Use case through which the logging of business events generated by the functional components of the *IS „NFR"* will be performed. Any event generated within the business processes implemented in the *IS „NFR"* will be logged and saved in the corresponding tables of the Database.

The logging mechanism will be developed based on standards and good practices implemented in the industry. The information system will provide functionalities to set up the strategy to log business events, including: business events' categories subject to logging, calendar period (determined or undetermined) for logging) etc.

For critical or sensitive business events, the logging will be carried out in parallel using the governmental service *MLog* (*example: import of data from the SRP, accessing data in the profile of Candidate/ receiving the candidate's file, etc.*).

The functional minimum requirements of logging the business events produced during the operation of the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 12.114	M	IS „NFR" will contain a mechanism to log all the business events related to its use.
CF 12.115	M	*System Administrator* will be able to set the totality of log strategies related to the business events through the use case *CU14*.
CF 12.116	M	*SI „NFR"* will provide to System Administrators a mechanism to search, filter and view the details of logged events
CF 12.117	M	The following categories of events will be logged: ● user login; ● user logout; ● adding/changing/removing/accessing the entry; ● business events specific to workflows of the *IS „NFR"*; ● synchronization with external information systems; ● generating/accessing report; ● queries to database; ● other specific business events.
CF 12.118	M	The logged events will save the following categories of data (depending on the nature of logged events): ● identifier of the user who has generated the event; ● category of the logged event; ● moment of logging the event; ● module of IS „NFR" which has generated the business event; ● entry related to the business event; ● action performed by the user.
CF 12.119	M	IS „NFR" will log exhaustively all the produced business events.
CF 12.120	M	IS „NFR" will log in parallel the critical business events through the logging governmental service MLog.
CF 12.121	M	IS „NFR" will provide the functionality of defining the critical business events to be logged in parallel through the MLog government service.

CF 13: Send notifications

Use case which provides functionalities for notifying the authorized users of the *IS „NFR"*. Notifications will be stored in the Dashboard of authorized users, ensuring direct access to the electronic form, whose business event has generated the notification.

The *IS „NFR"* will generate and send automatically the notifications related to any business event generated by the evaluation case of the Candidate. As well, the *IS „NFR"* will generate and send automatically to users notifications about any business event which needs their involvement.

The systems will provide both, mechanisms of internal notification (integrated in the *IS „NFR"*), and integration of mechanisms for external notifications through the governmental service *MNotify*, as needed.

The functional minimum requirements of the component related to notifying the stakeholders of the *IS „NFR"* are provided below.

Identifier	Binding nature	Description of functional requirement
CF 13.122	M	Depending on the user (the data for setting its profile), the functionality for notifying the users will apply one of the 3 notification strategies: ● notification via Email; ● notification via Dashboard of the authorized user; ● both categories from above.
CF 13.123	M	Depending on the configurations of the resources in the IS „NFR", the functional component for notification will send notifications to the relevant users upon occurrence of a business event specific for the program resource.
CF 13.124	M	Notification will contain reference of accessing the resource/form relevant to the business event which has generated the notification (valid for notifications stored in the user's Dashboard).
CF 13.125	M	Authorized users (regardless of the roles that they have) will be able to set up the preferences of the notification means.
CF 13.126	M	*The System Administrator* will have the functionality of concluding and sending notifications to explicit users or groups of users.
CF 13.127	M	IS „NFR" will notify the System Administrator about any problems related to the performance and availability of the information system.
CF 13.128	M	IS „NFR" will notify the external users through the governmental system of notification MNotify.

CF 14: Data exchange between computer systems

Use case which provides the necessary functionalities IS „NFR" for the exchange of data with external computer systems.

This synchronization refers to the exposure or consumption of interfaces designed for the reciprocal exchange of data (reception of data from external sources, sending of data to external computer systems and bidirectional exchange of data).

Part of the integrations with external IT systems are to be implemented through the *MConnect* interoperability governmental service. Governmental services (*MPass, MSign, MLog, MNotify, MPower, PDD)* are to be integrated directly through the APIs exposed by them.

The integration of IS „NFR" with the internal IT systems of the MAFI is to be carried out largely through a microservices infrastructure.

The functional requirements of the procedures for synchronizing the data processed by the *IS „NFR"* with the databases of external information systems are provided below.

Identifier	Binding nature	Description of functional requirement
CF 14.129	M	IS „NFR" will interact with external information systems to receive/supply data through APIs exposed by them (in case of nongovernmental information systems) and the interoperability governmental service MConnect (in case of information systems of PA).
CF 14.130	M	The interactions among MAFI internal information systems in case when the data supply/reception services are not requested by the information systems of other PA from the Republic of Moldova will be implemented through micro-services.
CF 14.131	M	IS „NFR" will have a mechanism meant for mutual exchange of data between the public interface and the BackEnd component so as to provide electronic services through the public interface of IS „NFR" and to send to the public interface/announcements and public reports.
CF 14.132	M	IS „NFR" will get integrated with the RCFI so as to extract criminal record of the Candidate
CF 14.133	M	IS „NFR" will get integrated through the interoperability governmental service MConnect with the State Register of Population to receive specific metadata, data about persons' identity, held identity documents, specific biometrical data, photos and specimen of handwritten signature in the process of managing the profiles of Candidates.

CF 14.134	M	IS „NFR” will get integrated through the interoperability governmental service MConnect with the IS „PAPIR” to send request for getting integrity records and to receive the integrity records of the Candidates.
CF 14.135	M	IS „NFR” will get integrated with the governmental service MPass for the purpose of implementing the user authentication procedures through the electronic signature and mobile signature.
CF 14.136	M	IS „NFR” will get integrated with the governmental service MSign to implement the procedure of electronic signature of electronic forms/documents.
CF 14.137	M	IS „NFR” will get integrated with the governmental service MLog to log critical business events.
CF 14.138	M	IS „NFR” will get integrated with the governmental service MNotify to implement the mechanism of users' notification.
CF 14.139	M	IS „NFR” will get integrated with the governmental service MPower to verify the empowerments of authorized users.
CF 14.140	M	IS „NFR” will get integrated with the Open Data Portal to publish public statistical data produced in the implemented workflows.
CF 14.141	M	All synchronization events and in particular access to personal data through the procedures described by the functional requirements CF 23.03 - CF 23.14 will be logged through the internal logging mechanism of IS „NFR” and the MLog governmental service.

9.6. Nonfunctional requirements

This compartment of the Terms of Reference sets forth the requirements regarding the nonfunctional characteristics that should be held by the *IS „NFR”*. The computing solution which is the object of the respective procurement should meet the set nonfunctional requirements mentioned below.

The general system requirements are defined by the policies and strategies developed and adopted in the Republic of Moldova. It is important to mention that these acts are based on good industry practices and include many organizational measures but also a series of technical measures. The general system minimum requirements specific to IS „NFR” are presented below.

CNF 15: General requirements

ID	Binding nature	Requirement
CNF 15.142	M	IS „NFR” must be developed based on the Agile methodology.

CNF 15.143	M	All user interfaces and the content of the database will be configured in Romanian language, with the use of Romanian diacritics.
CNF 15.144	M	The information system must be able to configure the Russian version of the user interface.
CNF 15.145	M	IS „NFR" database data is to be stored in unicode format (example: using UTF-8).
CNF 15.146	M	User interface elements must comply with Level A with the requirements of Web Content Accessibility Guidelines (WCAG) 2.0.
CNF 15.147	M	The user interface for authorized users of IS „NFR" will be optimized to 1360x768 resolution by avoiding the appearance of scroll bars for user interfaces presented by the IT solution.
CNF 15.148	M	IS „NFR" will provide adaptive user interface (will deliver responsive interface) depending on the device used by it (notebook, netbook, desktop computer, smartphone, tablet, etc.) optimized for touch screens.
CNF 15.149	M	Data search procedures will be implemented through simple searches (specifying search strings) or more complex searches, through which more accurate filtering of information can be performed (QBE forms). Regardless of the nature of the information sought, the user will use the same method of querying and retrieving data for any compartment of the user interface of the IT product.
CNF 15.150	M	The user interface of the computer system must ensure the search, filtering and viewing of records that correspond to the search criteria presented to users according to their access rights.
CNF 15.151	M	The contents of any search results table must be able to be exported in either XLS, CSV and PDF format.
CNF 15.152	M	The IS „NFR" architecture will be designed in an integrated way, developed with the application of the best practices in the field (example: architectural principles and reference architectures aligned TOGAF 9.1).
CNF 15.153	M	The IS „NFR" architecture must have a high level of resistance to falls, not contain single points of fall (SPOF).
CNF 15.154	M	The IS „NFR" architecture must ensure the rational and balanced use of processing resources.
CNF 15.155	M	The IS „NFR" will be developed based on a multilevel SOA architecture (at least 3 architectural levels (example: presentation level, business logic level and data level).

CNF 15.155	M	The IS „NFR" must provide web interfaces for interaction with computer systems of the MAFI and other public authorities of the Republic of Moldova through microservices and MCloud.
CNF 15.156	M	The IS „NFR" will be optimized in the minimum data transfer between the client and server computer, focusing on avoiding unnecessary requests as much as possible, implementing AJAX with JSON, minimizing the server resources required for authentication, authorization and logging procedures.
CNF 15.157	M	The potentially variable information (example: different parameters, data storage paths, connection paths with external services, classifiers, etc.) will be configurable and will NOT require the recompilation of the solution or direct interventions in the database.

PERF 16: Performance requirements

IS „NFR" should have the capacity to process in useful time the transactions performed by the users of the information system, according to the volumetric analysis of the results from the activity of the MAFI and its territorial services. Table 6.3 provides the performance requirements to be met by the *IS „NFR"*.

Table 6.2. Performance requirements of the information system

ID	Binding nature	Requirement
PERF 16.158	M	The response time to a transactional query of the externa user/service should not exceed 3 seconds (it does not refer to generation of reports).
PERF 16.159	M	IS „NFR" should be able to manage up to 300 concurrent sessions (connections of authorized users and external systems) with the possibility of scalability up to 1000 concurrent sessions during the extension of the information system.
PERF 16.160	M	The Provider will include in the guideline for administration and operation of the IS „NFR" information regarding the processes that may decrease the performance of the IS „NFR" and its recommendations regarding the concurrent carrying out of these processes (example: it is not recommended to roll out the process X of generating daily reports, simultaneously with the process Y of generating the backup copies).
PERF 16.161	M	Generation of reports and accessing information for the purpose of business analyses should not influence the operational performance of the information system at the level of transactions' processing. In the documentation of the information system, there will be identified the reports with significant impact on performance and Provider will

		formulate recommendations for generation of the respective reports, so as not to influence the performance indicators of the IS „NFR".
PERF 16.162	M	The Provider will indicate in its bid the minimum values guaranteed for performance characteristics of the IS „NFR", referring to the recommended technological platform.
PERF 16.163	M	IS „NFR" should have the capacity to process at least 50 000 transactions per day.

During the use of *IS „NFR"*, it is possible that the number of processed transactions and competing users will increase or decrease significantly from one period to another. In order to have a rational use of processing resources, the information system must be easily scalable (up and down). Table 6.4 contains requirements on the scalability characteristics related to *IS „NFR".*

SR 17: Scalability requirements

ID	Binding nature	Requirement
SR 17.164	M	IS „NFR" will allow the processing capacity to be increased without interrupting its operation. To this end, the system will support the horizontal expansion of processing capacity (example: adding new server nodes and balancing the load).
SR 17.165	M	IS „NFR" can be configured for automatic scaling of key components (lag sensitive). The scaling of the system will be done both up and down.
SR 17.166	M	IS „NFR" must be able to serve an unlimited number of transactions, with the condition that the appropriate allocation of data processing and storage resources is provided. Resources will be allocated horizontally (allocation of new servers, without increasing performance on existing servers).

SHC 18: Software, hardware and communication (SHC) requirements

Table 6.5 contains the software, hardware and communication technology insurance requirements for the implementation of IS "NFR".

Table 6.5. Categories of specification requirements

ID	Binding nature	Requirement
SHC 18.167	M	IS "NFR" must be able to be installed on both dedicated servers and virtualization solutions (IS "NFR" must be in accordance with the requirements for the deployment of information systems on the common government technology governmental service MCloud).

SHC 18.168	M	It is necessary to demonstrate the virtualization capability by delivering to MAFI an image of the system that can be uploaded and becomes functional with minimal configurations on one of the existing virtualization solutions available on the market.
SHC 18.169	M	The provider will demonstrate the possibility of installing and operating IS "NFR" within the MCloud infrastructure.
SHC 18.170	M	IS "NFR" must be accessible on communication channels of at least 512Kbps.
SHC 18.171	D	For the development and operation of IS "dNFR" it is welcome to use portable FOSS (free open source software) platforms on UNIX and WINDOWS operating systems, prioritizing technologies that have demonstrated continuous development. As an example, we reproduce the technological stack adopted by AGE in the development of government platforms: a) C# programming language; b) Web framework ASP.NET MVC Core; c) RDBMS - SQL Server; d) Container engine - Docker; e) Container orchestration - Kubernetes; f) Cache server, session store-SQL Server or Redis.
SHC 18.172	M	The Provider will explicitly indicate in the offer the software platform on the basis of which IS "NFR" is to be developed and the software platform necessary for its operation.
SHC 18.173	M	The technologies proposed by the Provider must be accessible for at least 3 companies specialized in the development of software solutions operating on the local market of the Republic of Moldova.
SHC 18.174	M	If the software platform for the development and operation of IS "NFR" is based on commercial IT solutions that require licensing, the Provider will include in the price offer the cost of all licenses necessary for the development and operation of IS "NFR" (the Provider must purchase on behalf of MAFI all the licenses necessary for the development and operation of the IT system).
SHC 18.175	M	If the software platform for the development and operation of IS "NFR" is based on commercial IT solutions that require licensing, the Provider will include in the price offer the delta of licensing costs in case of: ● doubling the number of users; ● doubling the number of processing units (CPU or CPU cores); ● doubling the number of application server nodes/ database.

SHC 18.176	M	IS "NFR" will use open standards for formats and communication protocols.
SHC 18.177	M	The services exposed to the public by IS "NFR" will be technologically neutral (Operating System, Internet explorer, etc.).
SHC 18.178	M	The recommended generic program product for operation and interaction with IS "NFR" is the WEB explorer.
SHC 18.179	M	The system will be compatible with at least 2 of the latest versions of the following web browsers: MS Internet Explorer / MS Edge, Mozilla Firefox, Google Chrome, Safari and Opera.
SHC 18.180	M	Compatibility with MS Internet Explorer / MS Edge WEB Explorer is compulsory.
SHC 18.180	D	IS "NFR" will incorporate a Heart-beat service that will periodically communicate the normal working state of the system.
SHC 18.181	M	IS "NFR" will include configurable means of technical logging.
SHC 18.182	M	The system must be able to produce at least the following levels of technical logging: info; warning; critical; error.
SHC 18.183	M	The Provider will enumerate the means that will be used for the technical troubleshooting of the system.
SHC 18.184	M	The Provider will prepare means to facilitate the administration of the system: ● starting of the system components; ● stopping of the system components; ● restarting the system components; ● creating the database backup copy; ● restore the data from the indicated backup copy; ● refreshing the operational memory of the system.
SHC 18.185	M	IS "NFR" will operate in TCP / IP networks and especially HTTPS.
SHC 18.186	M	Communication between all IS "NFR" components will be secured, using the internal interfaces of the system components for this purpose.
SHC 18.187	M	The Provider will suggest other network services and utilities required to operate the system.

LIPR 19: Licensing and intellectual property requirements

MAFI will hold all the necessary rights for using for undetermined period of time the information system *IS „NFR"* and of all soft components necessary for the good functioning of the *IS „NFR"*.

The specification of minimum requirements related to licensing and intellectual property rights related to the *IS „NFR"* and soft components necessary for the system operation are presented below.

ID	Binding nature	Requirement
LIPR 19.188	M	MAFI ensures the following operation environments for the *IS „NFR"*: ● Production environment; ● Testing/training environment; ● Development environment.
LIPR 19.189	M	*The Provider* will include in its financial offer the licenses for all soft products of COTS type, which are necessary for implementation and use of the *IS „NFR"* in those three environments provided to MAFI. The following are included here: operation systems, database management systems, software libraries, utilities and other system soft.
LIPR 19.190	M	The quantity of provided licenses should allow accessing and using *IS „NFR"* (in any environment in which it operates) of at least 20000 nominal users, as well as unlimited by external systems. There will be no restrictions regarding the number of documents, transactions or accessing modality for the *IS „NFR"* (*e.g. limitations in concurrent accessing*).
LIPR 19.191	M	Quantity of provided licenses should allow accessing the APIs exposed by *SI „NFR"* by any application and external system.
LIPR 19.192	M	*The Provider* will transfer to MAFI all the rights for developments, adjustments, setups and customizations carried out for implementing the *IS „NFR"* according to requirements. They may refer to third licensed soft products or may be components developed within the project.
LIPR 19.193	M	Any data stored in the database related to the *IS „NFR"* represent the property of the MAFI. Access to these data over the entire provider's contacting period, as well as afterwards, is subject to information confidentiality requirements and clauses.
LIPR 19.194	M	*The Provider* will present its licensing model suggested for the *IS „NFR"* which should be in line with the requirements LIPR 001 – LIPR 006. The *Provider* will describe the suggested licensing model, reasoning why it is the most optimal one for the MAFI. Will present a comparative analysis with other licensing models provided usually for the tendered solution.

INT 20: Interoperability requirements

The interoperability of the *IS „NFR"* represents the characteristic of the information system to communicate with other information applications. The system architecture sets interfaces which should exist between the *IS „NFR"* and other systems of the *MAFI* or of public authorities from the Republic of Moldova. The requirements regarding the minimum interoperability characteristics of the *IS „NFR"* requested by *MAFI* are presented below.

ID	Binding nature	Requirement
INT 20.195	M	All the interfaces exposed by the *IS „NFR"* should be based on open standards. All the flows of messages between the *IS „NFR"* and external entities shall be carried out using open standards.
INT 20.196	M	*IS „NFR"* will have the capabilities to implement the interfaces through *MConnect*.
INT 20.197	M	*IS „NFR"* will be integrated at the implementation with the following external systems: ● MPass; ● MSign; ● MNotify; ● MLog; ● MPower; ● Open Data Portal; ● State Register of Population; ● IS „PAPIR".
INT 20.198	M	All the interfaces provided by the *IS „NFR"* will interact with external applications instantly or in a programmed way through specialized jobs.
INT 20.199	M	IS „NFR" will have the capability to define new standard interfaces to access all the key business functions of the system (example: generation of documents, generation of transactions, accessing information about business entities stored in the IS „NFR"). The respective interfaces should allow managing business entities by applying all the relevant business rules and using all the characteristics related to business entities.
INT 20.200	M	*IS „NFR"* will have capabilities to define new interfaces to access external systems with use of open standards. These interfaces will be accessible under the functions of the system, when implementing the functionalities of the *IS „NFR"*.
INT 20.201	D	*IS „NFR"* will have standard interfaces to export data within the tools of *Data Warehouse* type.

INT 20.202	M	All the interfaces of the system should be adequately documented (*example: applying model Web Services Description Language*).

MIG 21: Data migration and popular requirements

The data migration minimum requirements are presented below.

ID	Binding nature	Requirement
MIG 21.203	M	MAFI will prepare and deliver the necessary data and metadata sets to the population with primary data of IS „NFR". The format of the migrated data will be agreed with the Provider.
MIG 21.204	M	The Provider will need to convert specific values of the metadata related to the external data sets according to the MAFI metadata system.
MIG 21.205	M	The Provider will include in the technical offer its approach on the procedure for implementing the initial migration and popular procedure of the database.
MIG 21.206	M	The Provider must provide a mechanism that will ensure the automated population of the IS „NFR" database with relevant metadata (nomenclatures, classifiers, variables of various kinds, etc.) and the primary data sets provided by the MAFI in order to consolidate the initial data stock of IS „NFR".
MIG 21.207	M	During the implementation of the migration and popular data procedure the Provider is responsible for: ● defining the methodology used in the migration and popular data process; ● elaboration of detailed migration and popular data plans; ● providing software mechanisms for data migration and population; ● defining the quality requirements for the migration / population data sets and processing them through the developed migration and population mechanisms; ● mapping the value of metadata received from external sources (in case of divergences); ● defining the criteria for reconciling migrated and populated data; ● participation in the process of data cleansing and enrichment; ● checking and validating the quality of the data sets to be migrated and populated;

		● the primary population of the IS „NFR" database based on the data sets provided by the MAFI; ● identifying and resolving exceptions / errors during the migration and popular data process.
MIG 21.208	M	The Provider must propose to the MAFI the data migration and population methodology. The methodology must contain the following elements: ● methodology for preparing of the data to be migrated and populated; ● methodology for mapping of the migrated and populated data; ● methodology for cleansing and enriching migrated / populated data and ensuring their quality; ● methodology for completing the value of the data required by IS „NFR" but which are missing in the data sets provided; ● automated migration and population data procedure; ● principles of reconciling migrated and populated data; ● recovery plan in case of failure (for each stage of the migration and popular data process); ● delivery plan of the data migration and population mechanism.
MIG 21.209	M	The Provider must prepare and deliver the detailed migration plan and initial population with data of IS „NFR" (migration and data conversion strategy). This plan must be aligned with the IS „NFR" implementation plan.
MIG 21.210	M	The Provider must deliver to the MAFI a software solution designed to automate the initial migration and population processes with IS „NFR" data.
MIG 21.211	M	All migration and initial population activities of IS „NFR" with primary data must be performed in the operating environment controlled by the MAFI. The data will never leave the MAFI's ICT infrastructure.
MIG 21.212	M	In the migration process, the Provider will conform the security policy of the MAFI.
MIG 21.213	M	The Provider will demonstrate the correctness of the initial migration and population instrumentation with IS „NFR" data to the MAFI specialists (an act of acceptance of the migration and initial population with IS „NFR" data is to be signed between the Provider and the MAFI).

SEC 22: Security Requirements

IS „NFR" should allow adequate control over the security risks of the information to be used. The implemented security measures should be aligned to security policies approved in the *MAFI* and shall ensure the prevention, identification, and adequate reaction to security incidents.

IS „NFR" should implement an approach of „*Multi-layered security*" type at the level of the system and to have the capacity to get integrated in the institutional model of the *MAFI* for information security management (based on standard family ISO 27000).

The table provides the minimum requirements for the security characteristics related to the *IS „NFR* system.

- **Requirements for security architecture**

ID	Binding nature	Requirement
SEC 22.214	M	The architecture of the IS „NFR" should be established by applying an approach of the type „Secure by design".
SEC 22.215	M	The security architecture of the IS „NFR" should be documented at the technical level.
SEC 22.216	M	The documentation will contain the description of the implemented security model, present components and the role of every component from security point of view.
SEC 22.217	M	The documentation will contain the peculiarities for placing at the network level the components of the IS „NFR" and the recommendations of the Provider regarding the access rules to the network, to be set by MAFI for secured access to all the system components (example: communication between services matrix).
SEC 22.218	M	All the system processes related to the components of the IS „NFR" will roll out with minimum privileges necessary for carrying out the attributed tasks.
SEC 22.219	M	All the access credentials used by the information system should be set in administrative interfaces. IS „NFR" will not contain hard-coded access credentials.
SEC 22.220	M	IS „NFR" will not contain open access credentials at the level of its components (based on data, configuration files).
SEC 22.221	M	All the interfaces of the IS „NFR" will be accessed applying safe login methods (example: X.509 certificate).
SEC 22.222	M	The access to functions provided to unauthenticated users (public interface provided by IS „NFR") should be controlled with protection means against the over-demand of the service by one or several nodes of the network.
SEC 22.223	M	The field content in the forms filled in by the users should be valid on binding basis on the client computers and on the server.

SEC 22.224	M	IS „NFR” will be secured for OWASP Top 10 vulnerabilities (2017).
SEC 22.225	M	IS „NFR” will ensure confidentiality of data which are sent-received on communication channels.
SEC 22.226	M	Users’ actions should be registered in electronic logs.
SEC 22.227	M	IS „NFR” will issue a periodical signal, which indicated its functional status.

Requirements for the authentication mechanism

ID	Binding nature	Requirement
SEC 22.228	M	IS „NFR” will allow accessing its functions only after the successful authentication of the user. IS „NFR” will provide support for at least the following authentication methods: based on login and password, Windows authentication (integration with Active Directory), two step authentication (2FA) and authentication through electronic or mobile signature (MPass). IS „NFR” will allow the users to change individual passwords.
SEC 22.229	M	IS „NFR” will allow registering users and profile information related to them (example: login, password, name, surname, IDNP/fiscal code, Email etc.).
SEC 22.230	M	Users’ passwords should be protected. Protection method for passwords should ensure the impossibility of their wiretapping, deduction or recovery.
SEC 22.231	D	IS „NFR” will allow differentiated application of policies to use passwords for different groups of users.
SEC 22.232	M	IS „NFR” will allow blocking, deactivating or suspending users’ accounts at the application level.
SEC 22.233	M	IS „NFR” will be integrated with the LDAP solution implemented in the MAFI for internal users. When creating a new user account, the IS „NFR” will have the option to select from the list of users available in the directory service.
SEC 22.234	M	IS „NFR” will be able to be integrated with external services of Identity Services Providers type. For this purpose, standards and open protocols in the area will be used (example: SAML). Authentication methods to be supported with the involvement of an external ISP are: ● login and password; ● Certificate X.509;

		● OTP (One Time Password). ● MPass government service must be used as a ISP solution.
SEC 22.235	M	When using mobile applications, the access will be carried out based on access credentials of an user and a unique key set in the client application configuration. Communication with the IS „NFR" served will be encrypted.
SEC 22.236	D	IS „NFR" will allow the differentiated application of authentication methods, depending on accessed resources (example: implicit electronic or mobile signature for authentication of candidates, login and password for the employees of the REC, OTP for the administrative interface).
SEC 22.237	M	IS „NFR" will allow setting the number of simultaneous connections to be initiated by one user.
SEC 22.238	M	IS „NFR" will allow setting the time for expiration of users' sessions in case of inactivity.
SEC 22.239	M	IS „NFR" will have efficient mechanisms to prevent the unauthorized taking over of active sessions initiated by authorized users.
SEC 22.240	M	The working session in the IS „NFR" will be blocked upon the user's request or automatically, upon the expiry of the time set for the session.

Requirements for the authorization mechanism

ID	Binding nature	Requirement
SEC 22.241	M	IS „NFR" will allow the granular management of the access rights to all its objects and possible actions for them (example: electronic forms, menus, reports, actions to create/view/update/remove etc.).
SEC 22.242	M	The authorization method within the system will be based on the principle „everything which is not explicitly allowed is prohibited".
SEC 22.243	M	IS „NFR" will allow defining the groups of users, roles and association of users to these groups and roles.
SEC 22.244	M	IS „NFR" will allow providing access rights at the level of explicit user, group and role. A group of users will be able to contain more subgroups/roles. One user may be associated to one or more groups and roles, its access rights being determined cumulatively.

SEC 22.245	M	IS „NFR" will allow providing access rights based on business rules (example: modification of the document only if the user is author or if the operation is performed within a certain time interval, condition or context).
SEC 22.246	M	IS „NFR" will allow attributing temporarily the rights held by one user towards another user. This attribution will be able to be performed by keeping or suspending the rights held by users to whom these rights are delegated.
SEC 22.247	D	IS „NFR" will allow segregating the administrative activities (example: Administrator 1 modifies, Administrator 2 confirms).
SEC 22.248	M	IS „NFR" will provide views and reports regarding the set access rights. It will be possible to set parameters for them depending at least on the following criteria: group of users/roles, user login, admitted actions, etc.
SEC 22.249	M	IS „NFR" will have the capabilities to authenticate and authorize users through internal mechanisms, as well as through MPass governmental service.
SEC 22.250	M	IS „NFR" will authorize authorized users' access to sensitive compartments of the interface and data after verifying their rights through Mpower.

Requirements for the mechanism of validating the entry/exit data

ID	Binding nature	Requirement
SEC 22.251	M	IS „NFR" will have an adequate mechanism for preventing the manipulation of entry data (entry data coming from authorized users, entry data coming from external applications).
SEC 22.252	M	All the actions for modifying critical and sensitive data in the IS „NFR" will be carried out through specialized forms and documents, according to the workflow set for these categories of documents (example: correcting data in the filled in and signed questionnaire).
SEC 22.253	M	IS „NFR" will carry out the complete and independent validation of data at the level of presentation, level of business logic, level of data, so as to ensure integrity, completeness and correctness of data.
SEC 22.254	M	All the displays of data within the IS „NFR" should be accompanied with security mark, according to a classifier set for this purpose in the IS „NFR".

SEC 22.255	M	Confidential data will not be stored and accessed in unsecured way in the IS „NFR" (example: log files, caching etc.).
SEC 22.256	M	IS „NFR" will have mechanisms for additional protection of especially confidential data (example: concealed display of data, storage of data in encrypted form, repeated authentication or use of additional means by user, etc.).
SEC 22.257	M	IS „NFR" will have routine procedures to verify and detect possible corruption of data integrity relations.
SEC 22.258	M	IS „NFR" will have adequate mechanisms to prevent manipulation of data stored in the application.

Requirements for the log and audit mechanism

ID	Binding nature	Requirement
SEC 22.259	M	IS „NFR" will have audit components which will collect and managed in a centralized way the audit entries at the level of every information system module.
SEC 22.260	M	The audit component will allow granular setting of audit policies.
SEC 22.261	M	IS „NFR" will allow establishing audit policies at the level of functional component/user interface compartment, categories of data and level of logged event.
SEC 22.262	M	IS „NFR" will allow establishing characteristics which are specific for events to be logged (example: produced within a certain time interval, which are in a specific status or which transit a certain status, etc.).
SEC 22.263	M	IS „NFR" will allow auditing any event, at the level of any object or business entity from the information system.
SEC 22.264	M	Every audit entry will contain at least: ● time when the event was produced; ● event's subject (user identifier); ● impacted object or entity; ● occurred event; ● IP address from where the event was initiated.
SEC 22.265	M	Audit entries will not contain confidential data (example: passwords entered for failed authentication attempts).

SEC 22.266	M	Errors which may occur when logging audit entries should not influence the normal functioning of the information system.
SEC 22.267	M	The audit component will use the system clock set at the level of the operation system of the application server in which the component operates.
SEC 22.268	M	The audit component will have a mechanism for archiving past audit entries. Parameters can be set for the archiving process (frequency, length of data, archiving format, destination, etc.).
SEC 22.269	D	IS „NFR" will be able to generate automatically notifications to persons responsible for producing certain security events, according to set configurations.
SEC 22.270	D	It will be possible to integrate the audit component in the basis of open standards with solutions of SIEM type (Security Incident and Event Management) so as to take over the audit entries produced within the system, by the respective solutions.
SEC 22.271	M	IS „NFR" will allow fixing the historical versions of data, which will be considered to be very sensitive.
SEC 22.272	M	The activities for changing entries' status and responsible will be logged.
SEC 22.273	M	IS „NFR" will have convenient tools to access and process logged events, including filtering the audit entries according to held fields and to export them in usual format. The audit tools of the information system will be used also for the purpose of importing archives with audit files for occasional analysis activities.
SEC 22.274	M	IS „NFR" will have safe mechanisms for protecting entered audit information integrity.
SEC 22.275	M	Critical business events should be logged in parallel through MLog log service.
SEC 22.276	M	IS „NFR" will provide a mechanism to set business events which will be logged in parallel through the MLog governmental service.

Requirements for the mechanism to manage exceptions and errors

ID	Binding nature	Requirement
SEC 22.277	M	IS „NFR" will register in a centralized way all the exceptions and errors generated by its components.

SEC 22.278	M	When an error occurs, the IS „NFR" will display a generic error message for the user. It may contain an error code and a single identifier of the error, to facilitate the involvement of support services.
SEC 22.279	M	IS „NFR" will have the necessary tools for analysis and processing of entries related to exceptions and errors.
SEC 22.280	M	IS „NFR" will be able to generate automatically notifications to persons responsible for producing certain errors in the operation of its components.

Requirements for the resilience capabilities and continuity of the IT system

ID	Binding nature	Requirement
SEC 22.281	M	IS „NFR" will have implemented tools for executing the procedures for automatic backup generation and historical backup management.
SEC 22.282	M	IS „NFR" must have mechanisms to ensure the integrity of the data in the event of any component failures.
SEC 22.283	M	IS „NFR" must have mechanisms to operatively restore availability and accessibility in the event of continuity incidents.
SEC 22.284	M	IS „NFR" architecture must be resistant to component failures and not have single points of failure (SPOF).
SEC 22.285	M	IS „NFR" must have mechanisms to ensure data integrity in the event of accidental drops in any of its components.
SEC 22.286	M	IS „NFR" must have mechanisms to operatively restore the availability and accessibility in the event of continuity incidents.

DEP 23: Requirements for the deployment of the IT system

The minimum requirements regarding the deployment mechanisms of the IS „NFR" to be implemented by the Provider, corresponding to the requirements for the IT systems of the central public authorities of the Republic of Moldova are presented below.

ID	Binding nature	Requirement
DEP 23.287	M	IS „NFR" must be able to be installed on dedicated servers and in virtualized media.

DEP 23.288	M	IS „NFR" must be able to provide a containerized infrastructure for deployment on relevant media (example: Docker Engine, Kubernetes).
DEP 23.289	M	IS „NFR" must be able to initiate deployment on several media simultaneously (example: development, testing, production) initiated from scratch.
DEP 23.290	M	The deployment of the IS „NFR" must be carried out through specialized instruments.
DEP 23.291	M	The deployment mechanism of the IS „NFR" must be able to define the component of the container to be updated (example: new version of the platform software, updated functional mode, etc.).
DEP 23.292	M	The deployment mechanism of the IS „NFR" must be able to manage the contents of the container.
DEP 23.293	M	The deployment mechanism of the IS „NFR" must be able to add new components to the contents of the container.
DEP 23.294	M	For the deployment of the IS „NFR" it is necessary that the deployment mechanism can specify in which cluster (dedicated server or cloud) the deployment must be performed.
DEP 23.295	M	For the deployment of the IS „NFR" it is necessary that the deployment mechanism provides workflow for compiling the code or registers.
DEP 23.296	M	The deployment mechanism of the IS „NFR" should provide functionalities for the delivery of the IT solution and performance of third party actions (example: installation of additional packages, configuration of notifications, etc.) using existing tools.
DEP 23.297	M	The production environment of the IS „NFR" must be able to be automatically updated with the possibility of manual intervention (manual build approval).
DEP 23.298	M	The developer will deliver to the MAFI all the tools and scripts necessary for the automated deployment of IS „NFR".

DOC 24: Requirements for the documentation

The minimum requirements regarding the documentation of the IS „NFR" are presented below.

ID	Binding nature	Requirement

DOC 24.299	M	The Provider will prepare and publish interactive guidance materials included in the user interface of IS „NFR".
DOC 24.300	M	The Provider will prepare and deliver the user manual in Romanian language.
DOC 24.301	M	The Provider will prepare and deliver the administrator guide in Romanian language.
DOC 24.302	M	The Provider will prepare and deliver the system installation and configuration guide (which includes at least code compilation, application installation, hardware and software requirements, platform description and configuration, application configuration, disaster recovery procedures).
DOC 24.303	M	The Provider will prepare and deliver the technical project of the delivered IT system based on which all the development / acceptance activities of the IT system (SRS and SDD) will be performed.
DOC 24.304	M	The Provider will prepare and deliver the System Architecture documentation with the description of the models in UML language, including a sufficient level of detail of the architecture in several sections (including the logical and physical model of the data).
DOC 24.305	M	The Provider will prepare and deliver the documentation of the consumed and exposed APIs for integration with external IT systems.
DOC 24.306	M	The Provider will deliver all the instructions necessary for the proper operation of IS „NFR" and solution of any technical problems/
DOC 24.307	M	The Provider will deliver the source code for the applications and components developed within the project with the necessary comments to understand the program code.
DOC 24.308	M	The Provider will deliver the training documentation for all roles of users of IS „NFR".

GMS 25: Requirements for warranty, maintenance and technical support of the IT system

The Provider will provide post-implementation warranty and technical support that includes the compartments included with the following minimum equirements.

ID	Binding nature	Requirement
GMS 25.309	M	The developer will provide warranty and technical support for 12 months after the final acceptance of IS „NFR".

GMS 25.310	M	The guarantee and technical support will correspond to the national standard SM ISO /IEC 14764: 2015 - Software engineering. Software life cycle processes. Maintenance.
GMS 25.311	M	The developer will provide MAI with a Help Desk service available on all the working days of the year.
GMS 25.312	M	MAFI users will be able to call the Help Desk service at a national telephone number (which corresponds to the telephone number of the Republic of Moldova).
GMS 25.313	M	Language of communication with the Help Desk service - Romanian or Russian.
GMS 25.314	M	MAFI users will be able to alternatively report technical problems caused by ticketing mechanism, Email or instant messages.
GMS 25.315	M	The Provider will provide documentation support for technical issues and their traceability to the MAFI.
GMS 25.316	M	The deadline for responding and remedying the reported technical problems will not exceed 8 hours from their reporting.
GMS 25.317	M	In case of problems of major complexity, the term for their solving will not exceed 72 hours.
GMS 25.318	M	Support services will be provided remotely. If necessary, the Provider's specialists will travel to the MAFI headquarters.
GMS 25.319	M	For the provision of post-implementation support and maintenance services, the Provider will provide the MAFI with an application platform, available for users of the IT system through the Internet.
GMS 25.320	M	The application platform will be adequately secured. All interactions between the Provider and the MAFI in the provision of support and post-implementation maintenance services will be performed through the respective platform.
GMS 25.321	M	The Provider will monitor the quality of post-implementation support and maintenance services and will react to the allowed deviations in order to prevent them.
GMS 25.322	M	The Provider will submit monthly reports to the MAFI on the services provided and their level. The reports will also contain information on the actions taken by the Provider or planned, in order to improve the quality of services.

GMS 25.323	M	The Developer will demonstrate the ability to provide post-delivery technical support in accordance with GMS 001-GMS 014 requirements.
GMS 25.324	M	Any program errors detected during the warranty period will be remedied by the Developer free of charge and in a timely manner.
GMS 25.325	M	In case of additional implementation requests, they will be subject to an amendment to the contract and payment of the value of the services.
GMS 25.326	M	The Provider and the MAFI will sign an SLA that will specify in detail the principles of providing warranty, maintenance and support services.