Annex 1 to RfP

TERMS OF REFERENCE

Intended for the Development of the IT Subsystem "Civil Status Acts" under the AIS "State Register of Population"

TABLE OF CONTENTS

Introduction

The Public Entity "Public Services Agency" has been established following the reorganisation of the *State-owned Enterprise "Centre for State Information Resources "Registru"*. The newly created public entity has included, by merger, the *State-owned Enterprise (SOE) "State Registration Chamber"*, *SOE "Cadastru"*, the *Civil Status Service* under the *Ministry of Justice* and the *Licensing Chamber* under the *Ministry of Economy*. By virtue of unifying the providers of public services and implementing the "One-Stop Shop" approach it has been envisaged to facilitate access to public services, cut down the costs incurred by citizens, reduce the documentation load by cancelling needless requirements on submitting excessive information, streamline and upgrade the services, including through their digitisation, and make the operational procedures more efficient.

The contemporary requirements in the area of public services provision and the development level of interoperable systems dictate using a comprehensive approach to the range of issues identified in the process of registering the civil status events, namely:

- Officials of Diplomatic Missions and Consular Offices are not able to register civil status events directly through the information systems;
- Local Government employees in charge for registering civil status acts have no direct access to information systems intended to update the civil status data. The Civil Status Bodies register the civil status events during the reporting period only on a monthly basis; therefore, the delays in entering the records into the SRP may exceed one month;
- General Civil Status Division has no real-time access to statistical reports on the registered civil status events, the quantity of documents of strict accountability issued or spoiled, volume of provided services (free-of-charge or for a fee) and, therefore, is not able to review the accumulated information, carry out operational monitoring of key indicators, and such facts significantly reduce the work efficiency;

The Information Subsystem "Digitised Archive Fund" (SAIS – Scan Archive Information System) contains scanned images of some 14 million civil status acts and related metadata. It is not possible to develop the SAIS in order to cover all needs of Civil Status Bodies.

The development and implementation of a single information system for all civil status bodies – ITSS the "Civil Status Acts" *(hereinafter referred to as ITSS "CSA", or the System)*, interoperable with the information systems of institutions empowered with attributes, shall enable:

- creating a single information resource to cover all civil status events;
- excluding the civil status paper acts;
- excluding the need to submit the documents required for registering the civil status facts, which can be identified/verified in the field-related information systems (civil status documents issued on the basis of civil status acts registered and kept by the General Civil Status Division, IDs from the documentation system of the RM, birth/death confirming medical certificates);
- preserving the paper Archive Fund kept by the structural subdivisions of the General Civil Status Division;
- issuing statements from the *ITSS "CSA"*, comprising all civil status facts related to the statement holder;
- excluding the handwritten registers to keep records on the civil status forms of strict accountability (for authorised use only);
- excluding the territorial principle for rendering the civil status service;
- excluding the standard paper forms (declarations, applications, conclusions, etc.);
- excluding handwritten registers used to record the applications/declarations, forms of strict accountability, supporting documents to register civil status acts, etc.
- receiving, via MConnect, the birth/death confirming medical certificates to register the fact of birth/death (*Ministry of Health, Labour and Social Protection*);

- receiving, via *MConnect*, the judgments on dissolution of marriage, enforceability of adoption, confirming the facts of birth/death, amending personal data (*Ministry of Justice*);
- verifying of information on the issuance of powers of attorney/powers (*Ministry of Justice*), via *MConnect*;
- creating the possibility to submit the statements/applications online by the Applicant for service, having appended the documents in .pdf format (*documents other than those that can be identified in the ITSS "CSA" or SRP*) aimed to register the civil status facts (birth, death, marriage, change of Last Name and/or First Name, filling in the Divorce Certificate) and asking for the issuance of statements and civil status documents (issued as per the Conventions the RM is a Party);
- generating, by the System, statistical reports, economic-financial reports on civil status services provided.

1. General Information

1.1. Abbreviations used in the Scope of Work

All the acronyms and abbreviations used in this document are specified in Table 1.1.

Table 1.1. Abbreviations and acronyms used in this document.

No.	Abbreviation/Acronym	Description
1.	CSA	Civil Status Act
2.	PSA	Public Services Agency
3.	ARIS	Address Registration Information System
4.	DB	Database
5.	COTS	Commercial off-the-shelf
6.	GCSD	General Civil Status Division
7.	CSD	Civil Status Document
8.	ESB	Enterprise Service Bus. A bus of corporate services intended to direct the exchange of information amongst applications
9.	KPI	Key Performance Indicators
10.	QBE	Query by Example is a method of query creation in the database based on the syntax as a native text. The main advantage is the absence of specific requirements towards the structure of the request for information
11.	SAIS	Information Subsystem "Digitised Archive Fund"
12.	SDD	Software design document
13	IRAMS	Information Resources Access Management System under the PSA
14.	DBMS	Database Management System
15.	ITS	IT System
16.	ITSS	IT Subsystem
17.	ITSS "CSA"	IT Subsystem "Civil Status Acts"
18.	SLA	Service Level Agreement
19.	MCSFRU	Methodical and Civil Status File Review Unit
20.	EDSS	Electronic Document Standard Structure
21.	TOGAF	The Open Group Architecture Framework (a methodology for developing complex architectures, which provide an approach for designing, planning, implementing and governing IT architectures within corporate IT solutions)
22.	SRS	Software Requirements Specification
23.	SPOF	Single Point of Failure
24.	IT	Information Technology
25.	ICT	Information and Communication Technology
26.	TLS/SSL	The TSL Protocol or its predecessor, the SSL Protocol, are cryptographic protocols that ensure safe communication between two nodes of

No.	Abbreviation/Acronym	Description
		computers network for such actions as visiting Web pages, e-mail, Internet-fax, exchange of instant messages and other transfers of data.

1.2. Notions used in the ToR

All the definitions of notions frequently used in this document are displayed and explained in Table 1.2.

Table 1.2. Definitions and notions used in this document.

No.	Abbreviation/Acronym	Description
1.	Database	Set of data organized according to the conceptual structure that describes the basic features and the relationship between entities.
2.	Credentials	Set of attributes that define the identity and authenticity of Users and systems within the information systems.
3.	Data	Elementary information units about people, issues, facts, events, phenomena, processes, objects, situations, etc. presented in a form that allows notification, commenting and their processing.
4.	Personal data	Any information related to an identified or identifiable individual (subject of personal data). In this respect an identifiable person is one who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more specific elements related to his/her physical, physiological, mental, economic, cultural or social features.
5.	Data integrity	Data status when they maintain their content and are interpreted unambiguously in cases of random actions. The integrity is deemed preserved unless the data have been altered or damaged (deleted).
6.	Logging	Function of registering information about events. In the information systems, the records on the events include details about date and time, user, undertaken action.
7.	Metadata	The way of assigning semantic value to the data stored in the database (data about data).
8.	Information object	Virtual representation of tangible and non-tangible entities in place.
9.	Information resource	A range of documented information within the IT system maintained in compliance with the requirements and legislation in force.
10.	ITSS "CSA"	The IT solution intended to automatize the workflows carried out by Civil Status officials and by the employees of institutions in charge for the registration of civil status facts (Diplomatic Missions and Consular Offices, Local Governments), as per the conditions of these Terms of Reference.
11.	IT System	Set of software and equipment that shall ensure automatic data processing (automated information system component).
12.	Information system	System for information processing along with the related organisational resources, such as human and technical resources, that supply and distribute the information.
13.	Software design document	IT System guiding document comprising detailed description of the following approaches: data structures and their constraints, IT System

No.	Abbreviation/Acronym	Description
		architecture, which provides all conceptual sections of an IT System, IT System interface covering the conceptualisation of all User interface components, IT System functionalities comprising detailed description of all IT System implementation scenarios.
14.	Software Requirements Specification	A document containing detailed description of all interaction scenarios between Users and the IT Application.
15.	IT Subsystem	A component (with the possibility of functional decoupling) of a complex IT system.
16.	Information and Communication Technology	Common term that includes all technologies used for information exchange and processing.
17.	Reliability of data	The extent to which the data stored in the computer memory or in documents correspond to the real status of the field-related objects mirrored in those data.

2. *ITSS "CSA"* Goals and Implementation Area

2.1. ITSS "CSA" Implementation Goals

The Information Subsystem shall represent all data, information, information flows and channels, the procedures and means for information storage and use intended to underpin the achievement of civil status fact registration goals, issuance of statements and civil status documents (issued as per the Conventions to which the RM is a Party). At the same time, it shall create an affordable, modern and secured information environment to ensure communication and collaboration among all authorities in charge by legislation to register civil status facts: structural subdivisions of the General Civil Status Division, Mayoralties, Diplomatic Missions and Consular Offices of the Republic of Moldova abroad.

- **Registration of births** and all other related functions as per the legal requirements on the: registration of a child born in wedlock; registration of a child born out of wedlock; establishment of affiliation of a child; registration of children born without signs of life; registration of a newborn who died within the first week of life; registration of a child found abandoned; registration of a newborn abandoned within healthcare facilities.
- **Registration of marriages** and all other related functions as per the legal requirements with regard to the marriage of two citizens of the Republic of Moldova; the marriage of a Moldovan citizen and a foreign citizen; or the marriage of two foreign citizens.
- **Registration of divorces** and all other related functions as per the legal requirements with regard to the dissolution of marriage on the basis of a common statement made by the spouses, a statement made by one of the spouses and a court judgment (sentence) (when the other spouse was declared under a disability, missing, sentenced in prison for a term exceeding three years) or on court judgement regarding the dissolution of marriage.
- **Registration of deaths** and all other related functions as per the legal requirements with regard to the death of a Moldovan citizen or a foreign citizen who died on the territory of the Republic of Moldova, including the death through suicide, accidents and other violent cases, as well as registration of death after the expiry of those three days of legal period for declaring the death of a person.
- **Registration of adoption based of a court judgement regarding the enforceability of adoption** and all other related functions as per the legal requirements with regard to national and international adoption.
- **The change of the Last Name and/or of the First Name** and all other related functions as per the legal requirements.
- **Subsequent registration of the birth/death fact** when the registration of a civil status fact was omitted by the Civil Status Body.
- **Transcription/Transliteration of a civil status fact registered abroad** and all other related functions as per the legal requirements.
- **Cancellation of a civil status fact registration and recognition of invalidity of an issued civil status document** and all other related functions as per the legal requirements when the documents were unlawfully produced, when repeated fact registration was identified or when false documents served as basis for primary registration.
- **Restoration of a civil status fact** and all other related functions as per the legal requirements.
- **Issuance of civil status documents**, upon request, as per the legal requirements.
- **Amending the personal data** (including the correction or supplementing a previously registered civil status act), as well as all other related functions as per the legal requirements.
- **Certifying the civil status facts registered on the left bank of Nistru River** and all other related functions in compliance with the provisions of Article 13^1 of Law 100-XV of 26.04.2001 on Civil Status Acts.

- **Managing the forms of strict accountability (for authorised use only).**

Overall Goal:

The overall goal is to improve and automatize the service provision processes, improve the quality of rendered services and make the work of the General Civil Status Division under the PSA more efficient.

Core Objectives:

- Reengineer the business processes related to the state registration of civil status events;
- Consolidate the existing databases;
- Reduce the time needed for processing the requests and the costs for storing the information;
- Enhance the interoperability level of central and local systems;
- Eliminate the existing information redundancy in the central and local systems;
- Store electronically and manage the archive of digitised documents;
- Increase the level of collaboration and communication amongst the PSA General Civil Status Division, Local and Central Public Authorities, Diplomatic Missions and Consular Offices of the Republic of Moldova.

Specific Objectives:

- Carry out in a safe and efficient way, though electronic means, the civil status workflow aimed at setting, storing, keeping records, as well as at issuing civil status documents related to civil status events;
- Convey and receive official applications and documents, check the status of citizens-applicants in the process of issuing the civil status document through a web interface that shall balance the access and use easiness with the need to protect confidentiality, integrity and availability of citizens' personal data;
- Secure the access to applications/data/systems/infrastructure, having applied security policy, identity profiles and solutions for access management;
- Manage and administer the Archive Fund of previously registered civil status acts;
- Issue, archive and manage the whole life cycle of civil status documents, as per the legislation in force.

2.2. ITSS "CSA" Development Principles

In order to ensure the attainment of the objectives outlined for the *ITSS "CSA",* in the process of its designing, developing and implementing full account shall be taken of the following general principles:

- **Principle of legitimacy** – functions and operations performed by system Users are legal as per the human rights and the national legislation.
- **Principle of authenticity** – the data stored and displayed by the system are authentic. Data authenticity is certified by the registration of data creation, as well as by the affixed electronic signature.
- **Principle of single identification** – the information packages are assigned a classification code at the country level by which unambiguous identification is possible.
- **Principle of system audit** – the system shall record the information about any changes made to make possible the recovery of a document history or status at a previous stage.
- **Principle of single centre/first person** – even if the system offers multiple functionalities, the subsystem is build up as an integral element, used by civil status officials, as well as by the other public authority officials assigned with the duties to register civil status events, via a single interface.
- **Principle of User-orientation** – the structure, content, means of access and navigation are focused on efficiency and user-friendly system.

- **Principle of flexibility/scalability** – capacity to quickly adjust and scale-up the existing system functionalities without major costs for complying with the continuously changing needs.
- **Principle of using open standards** – facilitates interoperability with external systems.
- **Principle of security** – protecting the information integrity, accessibility and confidentiality.

2.3. References and Legal Issues for Developing the IT System

Following the review of the Moldovan regulatory framework in force, a number of documents can be highlighted to be taken into due consideration in the process of *ITSS "CSA"* development. Hence, a package comprising 30 legal and regulatory documents has been identified for the development, implementation and operation of the *ITSS "CSA",* namely:

documents governing the business processes related to the *Public Services Agency* activity;

documents governing initiatives and ICT promoted by the Republic of Moldova, which shall be implemented within the IT System;

generic documents to establish the overall framework for the IT System operation.

I. Documents governing the business processes related to the Public Services Agency activity:

The review allowed identifying a range of legislative, regulatory and in-house documents to be used as basis for modelling and implementing the *Public Services Agency* business processes in the *ITSS "CSA".* This category of documents comprises also review documents and visions aimed at computerising the *PSA* business processes. The legal framework specifying the business processes to be implemented and automated under the *ITSS "CSA"* covers the following:

1. *Law No. 100-XV from 26.04.2001 on Civil Status Acts*, Official Gazette No. 97-99 of 17.08.2001. The Law on Civil Status Acts is to be amended as per the reengineering of civil status acts registration processes, using a single and interoperable information system by all civil status registrars.
2. *Government Decision No. 314 of 22.05.2017 on the establishment of the Public Services Agency,* Official Gazette No. 162-170 of 26.05.2017.
3. *Government Decision No. 757 of 04.07.2006 on approving the templates for civil status certificates,* Official Gazette No. 102-105 of 07.07.2006.
4. *Government Decision No. 558 of 18.05.2007 on approving the standard templates for civil status documents,* Official Gazette No. 74-77 of 01.06.2007.
5. *Government Decision No. 258 of 03.04.2009 on streamlining the procedure for registering the new-borns*, Official Gazette No. 68 of 07.04.2009.
6. *Government Decision No. 385 of 05.07.1996 on developing the State Register of Population,* Official Gazette No. 65-66 of 10.10.1996.
7. *Government Decision No. 333 of 18.03.2002 for approving the Concept of the automated information system the "State Register of Population" and the Regulation on the State Register of Population,* Official Gazette No. 43-45 of 28.03.2002.
8. *Government Decision No. 738 of 20.06.2008 for approving the List of services and tariffs for services rendered by the Civil Status Service and its Civil Status Offices, as well as the Regulation on accruing and using special means*, Official Gazette No. 112-114 of 27.06.2008.
9. *Public Services Agency Written Order of 21.07.2017 on approving the List of services and tariffs for services rendered by the* Public Services Agency.

II. Documents governing the ICT initiatives in the Republic of Moldova:

In the process of developing the ITSS "CSA" we deem it necessary to take into account and implement the requirements and recommendations comprised by the regulatory documents on ICT initiatives in the Republic of

Moldova. In order to comply with the e-Government framework promoted by the Moldovan Government the documents listed below shall be taken into consideration:

10. *Government Decision No. 7104 of 20.09. 2011 on approving the Strategic Programme for Governance Technological Upgrading (e-Transformation)*, Official Gazette No. 156-159 of 23.09.2011.
11. *Government Decision No. 128 of 20.02.2014 on Common Government Technological Platform (MCloud)*, Official Gazette No. 47-48 of 25.02.2014.
12. *Government Decision No. 656 of 05.09.2012 approving the Programme on Interoperability Framework*, Official Gazette No. 186-189 of 07.09.2012.
13. *Government Decision No. 1090 of 31.12.2013 on Government electronic service for authentication and control of access (MPass)*, Official Gazette No. 4-8 of 10.01.2014.
14. *Government Decision No. 405 of 02.06.2014 on Government integrated electronic service for digital signature (MSign)*, Official Gazette No. 147-151 of 06.06.2014.
15. *Government Decision No. 280 of 24.04.2013 on certain actions aimed at implementing the Government e-Payment Service (MPay)*, Official Gazette No. 109 of 10.05.2013.
16. *Government Decision No. 708 of 28.08.2014 on Government e-Logging Service (MLog)*, Official Gazette No. 261-267 05.09.2014.
17. *Government Decision No. 916 of 06.08.2007 on Government Portal Concept*, Official Gazette No. 127-130/952 of 17.08.2007.
18. *Government Decision No. 330 of 28.05.2012 on establishing and administering the single Government Portal of Public Services*, Official Gazette No. 104-108 of 01.06.2012.
19. *Law No. 91 of 29.05.2044 on Electronic Signature and Electronic Document*, Official Gazette No. 174-177 of 04.07.2014.
20. *Government Decision No. 945 of 05.09.2005 on Centres for Certification of Public Keys*, Official Gazette No. 123-125 of 16.09.2005.
21. *Government Decision No. 320 of 28.03.2006 approving the Regulation on affixing digital signatures on electronic documents issued by Public Authorities*, Official Gazette No. 51-54 of 31.03.2006.

The *ITSS "CSA"* design, development and implementation shall be in compliance with the national standards and methodology, as well as with the ICT Sector enshrined recommendations and requirements. Hence, out of this category of regulatory documents the following regulations and standards shall be complied with:

22. *Standard of the Republic of Moldova MR ISO/CEI/IEEE 15288:2015, "Systems and Software Engineering. System life-cycle processes"*.
23. *Technical Regulation "Software life-cycle processes" RT 38370656-002:2006*; Official Gazette No. 95-97/335 of 23/06/2006.
24. *The Handbook on "Information and Communication Technologies in Parliamentary Libraries"*, Global Centre for Information and Communication Technologies in Parliament, July, 2012), http://www.ictparliament.org/appendements/handbook-libraries/handbook-libraries.pdf
25. Michael O. Leavitt, Ben Shneiderman, *Research-Based Web Design & Usability Guidelines*, https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf
26. *World Wide Web Consortium (W3C) Recommendations* (http://www.w3c.org) on the quality of web page content, possibilities to view the information correctly by the commonly used Internet browsers and compatibility with different IT platforms.
27. *W3C Recommendations* (http://validator.w3.org) on WEB page testing. All WEB pages generated by the *ITSS "CSA"* shall be tested as per these Recommendations.

The ITSS "CSA" will not be isolated; it will interact with the IT Systems of other Central Public Authorities of the Republic of Moldova. To this end, it is appropriate to use the Government Interoperability Framework for connecting with third IT Systems or to use the platform services provided by it.

Likewise, *MConnect* interoperability framework governed by *Government Decision No. 656 of 05.09.2012* shall enable system-system interaction type not just among the IT solutions hosted by *MCloud*, but also with the providers of IT services outside *MCloud.* In the *ITSS "CSA"* context, *MConnect* shall serve as platform through which automatic interaction with external systems will be carried out to automatically retrieve, check and insert the data in the *PSA* business processes.

Government Decision of the Republic of Moldova No. 916 of 06.08.2007 on *Government Portal Concept* was adopted to ensure citizens' access to state information resources or to services rendered by state bodies via electronic devices or means. It imposes certain requirements and standards to ensure efficient, quick and high-quality interaction to exchange information amongst the society components (Government, citizens, business environment, and civil society). The Decision stipulates that the interaction of Public Authorities with citizens and business environment while rendering public services via electronic means shall be carried out via a single Government gateway, i.e. the "Government Portal". The latter was established in compliance with *Government Decision No. 330 of 28.05.2012*, being named the *Public Services Portal.*

The Government Portal is a support tool in the e-Government activity to ensure the exchange of information between individuals/legal entities and Public Authorities via communications networks, including the Internet, representing an access point to information services provided by State Authorities.

The *Government Portal Concept* contains also the vision regarding the way of access and provision of information to citizens, economic operators or to other category of Users. Hence, the Government Portal makes an access tool available to Users, connecting the latter with the multitude of services provided by public bodies as per the One-Stop Shop approach, while the provision of information to citizens shall allow using a single state system for identification, have access to the range of services offered by the Portal without the need to use distinct authentication data for each e-service separately.

The basic conclusions stem from the *Government Portal Concept;* they shall be taken into account in the process of developing the *ITSS "CSA",* namely:

any information or electronic service provided to citizens by the *PSA* should be made accessible also via the *Public Services Portal* (http://servicii.gov.md);

use a single identification system for all services available via the *Public Services Portal* (http://servicii.gov.md).

III. Generic documents related to the commissioning and operation of the ITSS "CSA":

In addition to legal and regulatory documents based on which the IT solution shall be developed and implemented intended to implement the *ITSS "CSA"* concept, it is required to take into account a range of legal documents imposing organisational measures and external constraints on IT System operation. Out of this category of documents to be taken into account by *ITSS "CSA",* the following shall be mentioned:

28. *Law No. 467-XV of 21.11.2003 on Computerisation and State Information Resources*, Official Gazette No. 6-12/44 of 01.01.2004.
29. *Law No. 71 of 22.03.2007 on Registers*, Official Gazette No. 70-73 of 25.05.2007.
30. *Law No. 982-XIV of 11.05. 2000 on Access to Information*, Official Gazette No. 88, Art. No. 664 of 28.07.2000.
31. *Law No. 133 of 08.07.2011 on Personal Data Protection*, Official Gazette No. 171-175 of 14.10.2011.
32. *Government Decision No. 1123 of 14.12.2010 approving the Requirements on ensuring the personal data security during their processing via information systems*, Official Gazette No. 254-256 of 24.12.2010.
33. *Government Decision No. 945 of 05.09.2005 on Centres certifying Public Keys*, Official Gazette No. 123-125 of 16.09.2005.

34. *Law No. 982-XIV of 11.05. 2000 on Access to Information*, Official Gazette No. 664 from 28.07.2000.
35. *Law No. 1069-XIV of 22.06.2000 on Information Science*, Official Gazette No. 073 of, 05.07.2001.
36. *Law No. 241-XVI of 15.11.2007 on Telecommunications*, Official Gazette No. 51-54 of 14.03.2008.
37. *Government Decision No. 967 of 09.08.2016 on public consultation mechanism with the civil society in the decision-making process*, Official Gazette No. 265-276 of 19.08.2016.
38. *Government Decision No. 840 of 26.07.2004 on establishing the Telecommunication System of Public Administration Authorities*, Official Gazette No. 130 of 30.07.2004.
39. *Government Decision No. 735 of 11.06.2002 on Special Telecommunication Systems of the Republic of Moldova*, Official Gazette No. 79-81 of 20.06.2002.
40. *Written Order No. 94 of 17.09.2009 of the Ministry of Information Development approving Technical Regulations (recordkeeping of public e-services, rendering public e-services, ensuring information security while rendering public e-services, determining the costs for developing and implementing automated information systems)*, Official Gazette No. 58-60 of 23.04.2010.
41. Other laws, regulatory documents, standards in force in the area of ICT.

Another important legal restriction to be complied with is to ensure security of personal data managed via the *ITSS "CSA". Law No. 133 of 08.07.2011 on Personal Data Protection* stipulates the obligation to ensure confidentiality of personal data. Moreover, in compliance with this Law, the Owner of the *ITSS "CSA"* must register the IT System into the *State Register of Personal Data Operators,* which is managed by the *National Centre for Personal Data Protection*.

3. ITSS Architecture

The ITSS "CSA" will be able to access all the data with reference to civil status keyed in up until now via the current systems and stored in the *SRP*.

The ITSS "CSA" shall use open standards and be compatible with the services that comply with the non-proprietary specifications and with the standards in place. Open standards are recommended for use in case of data exchange with other systems.

The ITSS "CSA" shall be operational 24/24 and 7/7, with short-term breaks in exceptional cases to restore its full operation capacity.

The ITSS "CSA" shall deliver a WEB interface accessible via an Internet widely used Browser (*MS Internet Explorer/MS Edge*, *Mozila FireFox*, *Opera*, *Google Chrome* or *Safari*). From the functional standpoint, it is envisaged to develop a reliable and scalable solution to deal both with the increasing number of concurrent Users and with the increasing volume of information managed by it. The communications system shall be based on the local network infrastructure and equipment, which shall include the possibility to connect to the Internet and offer the appropriate performance and capacity levels.

The ITSS "CSA" shall interact with other PSA internal systems, especially with the State Register of Population to supplement the latter with new inputs of civil status facts, write down the data on the forms used in the data stock for keeping records on those forms and retrieve data from the Archive of digitised civil status documents (SAIS). In the process of registering civil status events, *the ITSS "CSA"* will retrieve or receive data from third IT Systems.

The ITSS "CSA" will be based on a client-server architecture of at least three levels (that excludes direct interaction of the application with the database) based on appropriate WEB technologies. In order to ensure an appropriate level of information security the delivered application shall allow for secured connections amongst client stations and application server to ensure safe/reliable delivery of information (via VPN channels and TLS/SSL sessions).

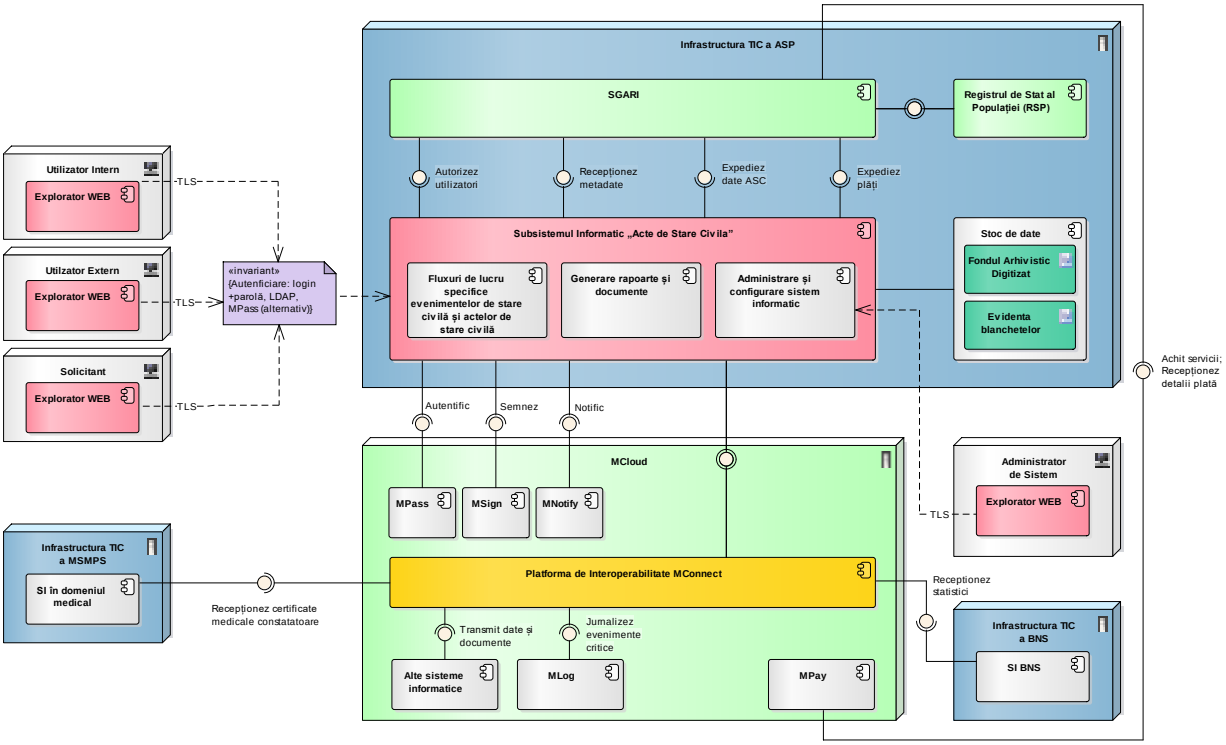

Figure 3.1. ITSS "CSA" Location within the Infrastructure.

The ITSS "CSA" will be installed and operated within the PSA technological platform. To ensure the attainment of the goals outlined for the IT solution it is required to take account of the architecture described in Figure 3.1 while designing, developing and implementing *the ITSS "CSA"*.

As shown in Figure 3.1, the solution for resource pooling to ensure the *ITSS "CSA"* functionality consists of three categories of distinct hubs:

- **ICT Infrastructure of the Public Services Agency** – the PSA ICT infrastructure that hosts the *State Register of Population, IRAMS, Data stock (Form recordkeeping and the Digitised Archive Fund).*
- **M-Cloud** – ICT infrastructure of the Common Government Technological Platform that serves as foundation for the Government Cloud (*MCloud*) where the *MPass*, *MSign*, *MPay*, *MNotify*, *MLog* and other public authority systems and registers are hosted. All the connections with external IT Systems will be secured via the interoperability platform *MConnect.*
- **Client computers** – computers from where Users (depending on the assigned rights and roles) will access t*he ITSS "CSA"* functionalities.

Client computers shall use at least three of most widely-used Internet Browsers, which meet the minimum requirements of HTML 5, CSS 3, as client application to access and use the *ITSS "CSA". C*ompatibility with *MS Edge/MS Internet Explorer* is binding. The interface and functionalities delivered to each User will depend on the User's level, rights and roles.

Regardless of the Users' access level, all Users' connections to the *ITSS "CSA"* will be made via reliable connections (VPN or TLS/SSL).

According to the performance diagram displayed in Figure 3.1, *the ITSS "CSA"* shall consist of three basic components:

- **Workflows intended to register civil status events** – an interface made available to *ITSS "CSA"* authorised Users, which delivers all the functionalities used to provide the IT support to workflows carried out to manage the business processes related to registering the civil status events;
- **Generating reports and statistics** – functionality intended to generate statistical reports to be used for review and decision-making, as well as standard documents related to business processes carried out to register civil status events.
- **ITSS "CSA" Administration and configuration** – a component that shall deliver all the functionalities to administer the *ITSS "CSA"* available largely to Users assigned with the role of *Information System Administrator* and, to some extent, to authorised Users under the PSA *GCSD*.

To implement a number of functionalities, *the ITSS "CSA"* will consume a range of services provided by external IT Systems, namely:

1. **WEB Service Authenticate** delivered by *MPass* with the aim to authenticate Users via electronic signature or via User Name+Password. Authorisation within the *ITSS "CSA"* shall be based on the data regarding the roles and rights furnished by the PSA IRAMS.
2. **WEB Service Sign** delivered by *MSign* with the aim to affix electronic or mobile signature on documents upon requesting electronic services.

   To sign the forms prepared under the business processes for the registration of civil status events, the *ITSS "CSA"* shall use internal mechanisms for signature.
3. **WEB Service Notify** delivered by *MNotify* with the aim to implement a universal and centralised mechanism to notify the *ITSS "CSA"* External Users.
4. **WEB Service Log** delivered by *MLog* with the aim to log the interaction events with external systems via MConnect.
5. **WEB Service Pay** delivered by the PSA IRAMS with the aim to keep records on payment settlements and integrated with *MPay*.

6. **WEB Service Retrieve and Update Person's Data** delivered by the PSA IRAMS with the aim to exchange data with the SRP.

4. Involved Parties and *ITSS "CSA"* roles

4.1. ITSS "CSA" Business Roles

In compliance with the legislation in force, the following Moldovan entities have an interest or shall be involved in the development and smooth operation of the *ITSS "CSA"*.

- **Public Services Agency** – as the entity responsible for the development and smooth operation of the *ITSS "CSA". The Public Services Agency* is the Project Financier and shall take active part in all phases of IT Subsystem development, commissioning and operation.
- **Ministry of Foreign Affairs and European Integration of the Republic of Moldova** – as the *ITSS "CSA"* Registrar. According to Article15 (4) of the Law on Civil Status Acts, it shall exercise oversight and control functions over the activity of Diplomatic Missions and Consular Offices of the Republic of Moldova accredited abroad in the area of registering civil status facts.
- **Local Public Authorities –** the personnel of public authorities in charge to register civil status facts shall be authorised to enter and modify the data within the *ITSS "CSA"*.
- **Healthcare facilities** – shall register the data on the issuance of medical certificates confirming the birth/death; declare the birth of a child if the parents of the newborn are not able to do that (including the case of abandoned children within healthcare facilities). The SRP updated information regarding the issuance of confirming medical certificates would enable the oversight of state registration of newborns and deceased people.
- **National Bureau of Statistics** – shall receive data on demographic statistics based on civil status facts registered by the Civil Status Bodies and updated within the SRP.
- **Social Assistance Bodies** – shall be notified on a monthly basis about the number of non-registered children (as per the domicile of the child's mother) and participate as Declarant at the registration of the death of a person who died in a social protection institution.
- **Child protection authorities** – shall participate as Declarant in the process of state registration of a minor child without parental care; issue opinions related to administrative procedures to determine the fatherhood of a child, upon the father's request, if the child's mother died, is declared dead, is not capable or is missing, or when it is not possible to locate her, as well as when she has been deprived of motherhood rights, and decide upon changing the child's Last Name until the age of 16 when the parents failed to understand each other, by issuing an appropriate opinion.
- **Ministry of Internal Affairs** – is notified on a monthly basis about the cases of failure to register the births and deaths in due time as per the last domicile of the newborn mother and, respectively, of the deceased person.
- **Social Assistance and Family Protection Division** – notification about the non-registered children.
- **National Social Security House (CNAS)** – the CNAS Territorial Social Security Bodies shall update their database pursuant to the birth/death facts registered by the Civil Status Bodies and stored in the SRP.
- **e-Government Centre** – as a body empowered with *e-Transformation* activities. The e-Government Centre shall ensure access to the interoperability platform *MConnect and* to *MCloud* platform services *(MPass, MSign, MLog, and MNotify).*

People in charge to register civil status events:

- **External Users** – officials of *Local Governments,* Diplomatic Missions and Consular Offices in charge to register civil status facts;
- **Internal Users** – employees of GCSD structural subdivisions.

4.2. ITSS "CSA" Owner

The Public Services Agency shall be the ITSS "CSA" Owner. As such, the PSA shall designate the people authorised to operate the IT System depending on their job duties, roles and rights of access to User Interface and data. Likewise, *the Public Services Agency* shall ensure all support activities, maintenance and further development of the *ITSS "CSA"*.

4.3. ITSS "CSA" Possessor

The Public Services Agency is also the *ITSS "CSA"* Possessor as it holds the technological platform on which the system will be implemented and troubleshoot all technical issues related to its operation.

4.4. ITSS "CSA" Registrar

Registrars of the *ITSS "CSA"* are the General Civil Status Division under the *Public Services Agency* and its territorial offices, public authority personnel in charge to register civil status facts, employees of Diplomatic Missions and Consular Offices.

4.5. ITSS "CSA" Purchaser

The UNDP "Enhancing Democracy in Moldova through Inclusive and Transparent Elections" Project and the Public Services Agency are the ITSS "CSA" Purchaser.

4.6. Users and their role within the ITSS "CSA"

The human roles or the IT Systems that interact with *the ITSS "CSA"* are displayed in Figure 4.1. As shown in this Figure, seven categories of human actors, eight IT Systems and platform services MCloud, three PSA IT systems and other external IT systems described below will interact with the *ITSS "CSA"*.

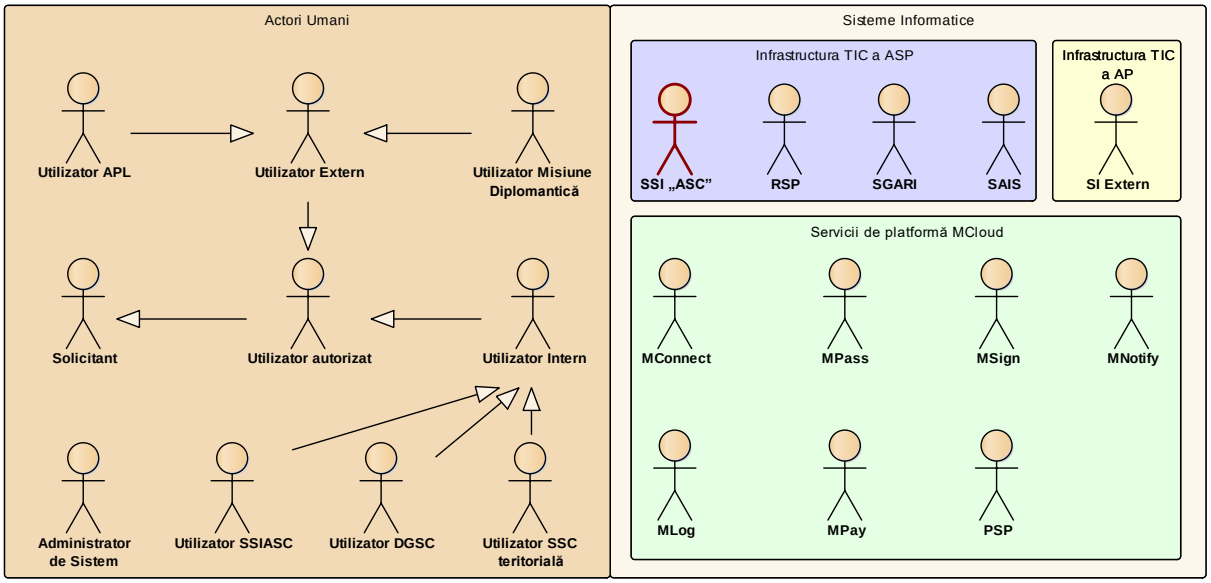

Figure 4.1. ITSS "CSA" Actors.

Applicant – a human actor assigned with the functionality to submit applications and statements. The system shall enable:

a) the Applicants for civil status services, via the PSA official web page or public services Government Portal (servicii.gov.md), to require civil status public services online.

b) the Applicants to identify themselves via electronic or mobile signature related to the electronic application requiring civil status services. The Applicant shall be responsible for the veracity of personal data and of appended documents *(other than those that can be identified by the CSA system and SRP);*

Authorised Users – human actors representing all Internal and External Users (this category of actors comprises: *PSA Operators, CS Officials, LPAs Officials, DM/CO Officials, CS Decision-makers*). These actors shall have access to the following functionalities:

External Users are officials of Local Government, Diplomatic Missions and Consular Offices in charge to register civil status facts.

1. *Local Government Users shall*:
    - Receive statements/applications on registering civil status facts;
    - Identify and view electronic forms of registered civil status facts;
    - Register births, marriage, death; determine fatherhood;
    - Issue statements based on registered civil status facts;
    - Receive applications requiring the issuance of statements and civil status documents (issued as per the Conventions to which the RM is a Party), rechanneling them to the territorial Civil Status Service for implementation;
    - Issue statements and civil status documents (issued as per the Conventions to which the RM is a Party), produced by the Civil Status Service, to Applicants demanding civil status services;
    - Generate statistical reports on provided civil status services.
2. *Diplomatic Mission and Consular Office Users*:
    - Receive statements/applications on registering civil status facts;
    - Identify and view electronic forms of registered civil status facts;
    - Register/modify/transcribe civil status facts;
    - Issue statements based on the registered civil status facts;
    - Receive applications requesting the issuance of statements and civil status documents (issued as per the Conventions to which the RM is a Party), rechanneling them to the GCSD for implementation;
    - Issue statements and civil status documents (issued as per the Conventions to which the RM is a Party), produced by the General Civil Status Division to Applicants requesting civil status services;
    - Generate statistical reports on provided civil status services.

Internal Users are the employees of GCSD structural subdivisions.

Internal Users are connected to the ITSS in compliance with the Regulation on granting access to information resources held by the public institution "Public Services Agency" for Internal and External Users, approved by the PSA Written Order No. 262 of 27.12.2017. The internal User shall authenticate by User Name + Password in *the ITSS "CSA"*.

Administration of Internal Users will be carried out within the PSA IRAMS used as User's authentication/authorisation mechanism and access intermediation to the APIs displayed by the PSA IT systems.

The roles are assigned to Internal Users as per the functional attributions performed by them:

1. *Users of territorial civil status services*:
    - Receive statements/applications to register civil status facts;
    - Identify the personal data mentioned in the statement /application in the SRP;

- Identify and view the electronic forms of registered civil status facts;
- Register/modify/cancel/transcribe/ recover/ record subsequently the civil status facts;
- Approve the cases related to the registration of civil status facts under special procedure;
- Receive online and off-line statements/applications requiring civil status services;
- Validate, rechannel or reject the statements/applications received online or off-line requiring civil status services;
- Certify the civil status facts registered on the left bank of Nistru River and Bender Municipality (in the case of Civil Status Services assigned with such duties);
- Receive and fulfil the applications requesting the issuance of civil status documents submitted by territorially subordinated mayoralties;
- Issue statements and civil status documents;
- Generate statistical and economic-financial reports on the provided civil status services by the Civil Status Service;
- Check electronic forms of civil status facts registered by the administrative-territorially subordinated Mayoralties.

2. *Users from the central subdivisions of the General Civil Status Division*:
   - Receive statements/applications on registering civil status facts;
   - Identify, within the SRP, the personal data mentioned in the statement/application;
   - Identify and view the registered electronic forms of civil status facts;
   - Amend the personal data in the forms used to register the civil status facts;
   - Receive applications online and off-line requiring civil status services;
   - Validate, rechannel or reject the application submitted online or off-line requiring civil status services;
   - Receive and fulfil the applications requesting the issuance of civil status documents submitted by territorially subordinated mayoralties;
   - Certify the civil status facts recorded on the left bank of Nistru River and Bender Municipality;
   - Issue statements and civil status documents;
   - Generate statistical and economic-financial reports on civil status services provided by the subdivision;
   - Check electronic forms of civil status facts registered by Mayoralties, Civil Status Services, Diplomatic Missions and Consular Offices.
3. *Users from the Unit of Statistics and Integrity of Civil Status acts under the General Civil Status Division*:
   - Identify and view the electronic forms of registered civil status facts;
   - Register/modify/cancel/transcribe/recover/register subsequently the civil status facts;
   - Correct the errors committed in the forms used to register civil status facts, as per the notes submitted by Territorial Civil Status Services or the conclusions made by the competent subdivisions;
   - Generate statistical and economic-financial reports on civil status services provided by the GCSD structural subdivisions;
   - Check electronic forms of civil status facts registered by Mayoralties, Civil Status Services, Diplomatic Missions and Consular Offices.

System Administrator – human actor empowered with the duties to target the system users, configure the IT system and start/stop/restart the IT system components. If the technologic environment includes sufficient capacities to carry out administration, then their implementation within the system is optional. This category of actors shall play the following distinctive roles:

- have access to the functionalities of Users assigned with the Applicant role;
- use Dashboard for rapid access to relevant notifications and tasks;
- administer the system of own nomenclatures and metadata characteristic for the system;
- configure the flows, forms and templates of documents;
- generate reports related to the audit of IT system and information content of its database;
- receive notifications.

PSA IT Systems:

SRP *(State Register of Population)* – IT system administered by the Public Service Agency for which the *ITSS "CSA"* represents the interface for updating and obtaining the data from the automated outline for keeping records and controlling the registration of civil status facts/acts.

SAIS – Archive Fund of Digitised Civil Status Acts, includes approximately 14 million of scanned documents covering the period of 1900-2007. SAIS comprises the images of scanned acts and data related to act registration.

IRAMS – the PSA Information Resources Access Management System used as a mechanism to authenticate/authorise the Users and intermediate the access to the APIs displayed by the PSA information systems.

External IT systems:

CMIP *(Case Management Integrated Programme)* – an IT system intended to computerise business processes of courts via which the *ITSS "CSA"* shall retrieve the data related to court judgments. The following judgments shall be conveyed by the CMIP and received by *ITSS "CSA"*:

a) judgment on the dissolution of marriage (as per Article 39 (3) of the Family Code and Article 45 (2) of the Law on Civil Status Acts, the court is required to convey, no later than three days after the judgment on the dissolution of marriage became final, a copy of this judgment to the Civil Status Office within its territorial jurisdiction for the state registration of divorce pronounced by the court);

b) judgment depriving of parenthood rights (as per Article 68 of the Family Code, the court must convey no later than three days after the judgment depriving of parenthood rights became final, a copy of this judgment to the Civil Status Office within the court territorial jurisdiction);

c) judgment on the enforceability of adoption (as per Article 292 of the Civil Procedure Code, no later than five days after the judgment on adoption became binding, a legalised copy of the judgment shall be sent to the Civil Status Office within the jurisdiction of the court that pronounced the judgment with the aim to make the state registration of the adoption).

Minister of Internal Affairs (MIA) – the *ITSS "CSA"* shall enable the generation of a monthly report on the failure to register in due time the births and deaths for subsequent conveyance to the MIA.

CNAS AIS – CNAS Automated Information System. The CNAS AIS shall initiate a query to the SRP to obtain data from the *ITSS "CSA" (*from the SRP Civil Status outline) on the new registrations of births for subsequent initiation of the process for granting childbirth allowance or on the registration of deaths of people who reached the retirement age.

IT systems and MCloud platform services:

PSP (Public Services Portal) – represents an electronic catalogue of public services provided by the authorities to the population and business environment.

MConnect – represents Government interoperability and data exchange platform. *ITSS "CSA"* shall use this platform to exchange data with third IT systems.

The ITSS "CSA" will integrate with the following categories of actors from the category of MCloud platform services:

a) **MPass** – MCloud service used to authenticate and control the access;

b) **MSign** – MCloud service used to affix and validate the electronic signature.

c) **MNotify** – MCloud service used as a notification mechanism;

d) **MLog** – MCloud service used for logging and auditing the business events (important for the recipient or with legal effect).

e) **MPay** – Government service of electronic payments.

5. ITSS "CSA" Functional Model

5.1. ITSS "CSA" Information Objects

Following the review of the modelled domain, it is possible to outline all information objects to be considered while developing the ITSS "CSA". Figure 5.1 displays the information objects, which will lay down the foundation for designing and developing the ITSS "CSA". As shown in Figure 5.1, the *Civil Status Act* is the core element of the ITSS "CSA" data architecture.

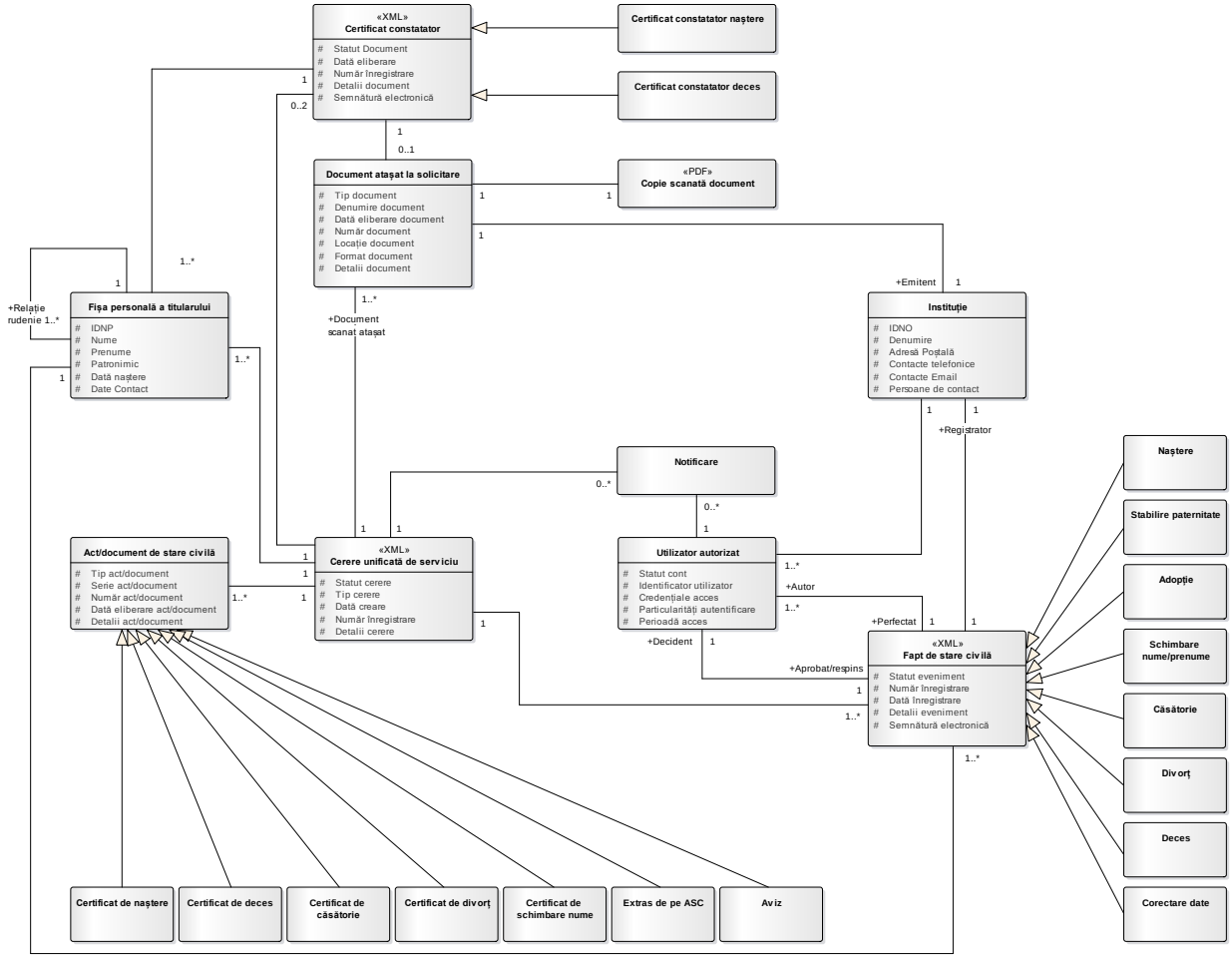

Figure 5.1. ITSS "CSA" Information Objects.

In order to ensure the *ITSS "CSA"* smooth operation, it is required to implement the functionalities necessary for managing the following information objects:

- holder's personal records;
- civil status fact;
- previously registered civil status act;
- civil status document;
- unified application to require a civil status service;
- appended document;
- institution;
- authorised User's profile;

- notification;
- form of strict accountability of the civil status document;
- medical certificate confirming the birth or death.

1. Civil Status Fact (Event):

This is the key information object that groups all the data regarding the civil status event registration process. A civil status event shall manage and group the following categories of data:

a) Date of creation;
b) Number of the registration form;
c) Status;
d) Type:
    - registration of birth;
    - registration of death;
    - registration of marriage;
    - registration of divorce;
    - registration of changing the Last Name and/or the First Name;
    - change of personal data or of previously registered civil status document;
    - cancelling the registration of the civil status fact;
    - recovering the registration of the civil status fact;
    - transcription of the civil status fact registered abroad;
    - subsequent registration of the civil status document.
e) Reference to the information object *Holder's personal records* (reference to the personal records of parents, spouse, civil status fact Declarant);
f) Reference to the information object *Civil Status Fact* (may include one or more facts);
g) Reference to the information object *Form of strict accountability* (if a *CSD should be issued*);
h) Reference to the Authorised User's Profile;
i) Reference to the appended documents;
j) Electronic signature.

2. Appended Document:

This is an information object that represents all files with copies of documents appended to the registration of civil status events. As a rule, all the documents received from outside *(other than those that can be identified in the CSA system and SRP)*, as well as the documents requiring handwritten signature will be scanned and appended to the case file. A document appended to the case file shall be described by the following data:

- File name;
- File Format;
- Date of File creation;
- File size;
- Application relevant for the file;
- File encoding.

3. Institution:

This is a complex information object that shall include the data on Civil Status Bodies (CSBs). The data on the CSB profile will be retrieved from the IRAMS and shall contain the following fields:

a) CSB Identifier;
b) CSB Name;
c) CSB address;
d) CSB phone number;
e) CSB Email;
f) CSB personal contact data;
g) CSB Head;
h) Other relevant data.

4. Profile:

This is a complex information object that defines all profiles of individual and legal entities registered in the *ITSS "CSA".* This information object implies there are three profile categories in place, namely:

A. ***Holder's personal records***. It represents the registration data of any individual who is the subject of civil status event registration case. As a rule, the completeness of an individual profile depends on his/her role and contains the following categories of data:

a) IDNP;
b) Last Name;
c) First Name;
d) Date of birth;
e) Place of birth;
f) Gender;
g) Domicile;
h) Residence;
i) Civil status;
j) Phone number;
k) Email;
l) Other relevant data.

Holder's personal records will be retrieved from the *SRP* (where it is managed as a primary information object).

B. ***Authorised Person's Profile***. It represents the profile of IT System authorised Users to be involved in the *ITSS "CSA"* business processes *or who* will need access to the details contained in the registration case (represents authorised persons: external and internal Users).

The profile of authorised persons will be retrieved from the IRAMS, where they are managed.

The authorised person's profile shall comprise the following data:

a) Access credentials;
b) Reference to the individual's **profile** (personal and contact data);
c) Authentication strategy/restrictions (User name + Password, electronic/mobile signature, IP access address, etc.);

d) Access validity period;

e) Roles assigned/held;

f) Profile status.

C. ***Institution Profile***. It represents the profiles of institutions, which employees have authorised access to the *ITSS "CSA"* User Interface (*Local Governments and Diplomatic Missions or Consular Offices*).

The institution profile will be retrieved from the IRAMS where it is managed.

The following data should be stated for the institution profile:

a) IDNO;

b) Institution name;

c) Postal mail address;

d) Phone number;

e) Email;

f) Contact persons (and their phone number and Email).

5. Notification:

This is a complex information object that contains all the details related to the message sent to authorised Users or to Applicants/Declarants. The notification shall be described by the following data:

- Message layout;
- Author;
- Recipient;
- Date of notification (timestamp);
- Priority;
- Actions to be undertaken (in case of warnings);
- Reference to appended documents (if any).

6. Forms of strict accountability:

This is a complex information object that contains all the details related to a form of strict accountability on which the Civil Status Document is printed. The form of strict accountability shall be described by the following data:

- Form series;
- Form number;
- Form status:
  a) issued;
  b) deteriorated/spoiled;
  c) available;
  d) lost;
  e) cancelled;
  f) null;
  g) under control;
- Form type;
- Institution the form was sent to;
- Date the form was issued;

- Reference to the case of CSA issuance (for the status Issued);
- Other relevant data.

7. Civil Status Act:

This is a complex information object that contains all the details related to a civil status act. The fields of civil status acts are described in details in *Chapter 3.1 Forms for data inputs* of the "Civil Status Events Registration Flows". The successful Bidder shall define the list of fields for each Civil Status Act during the business process review.

8. Confirming Medical Certificate:

This is a complex information object that contains all the details related to the Confirming Medical Certificate relevant to register birth/death events.

5.2. Functionalities provided by ITSS "CSA"

Functionalities provided by *ITSS "CSA"* are outlined in the diagram from Figure 5.2.

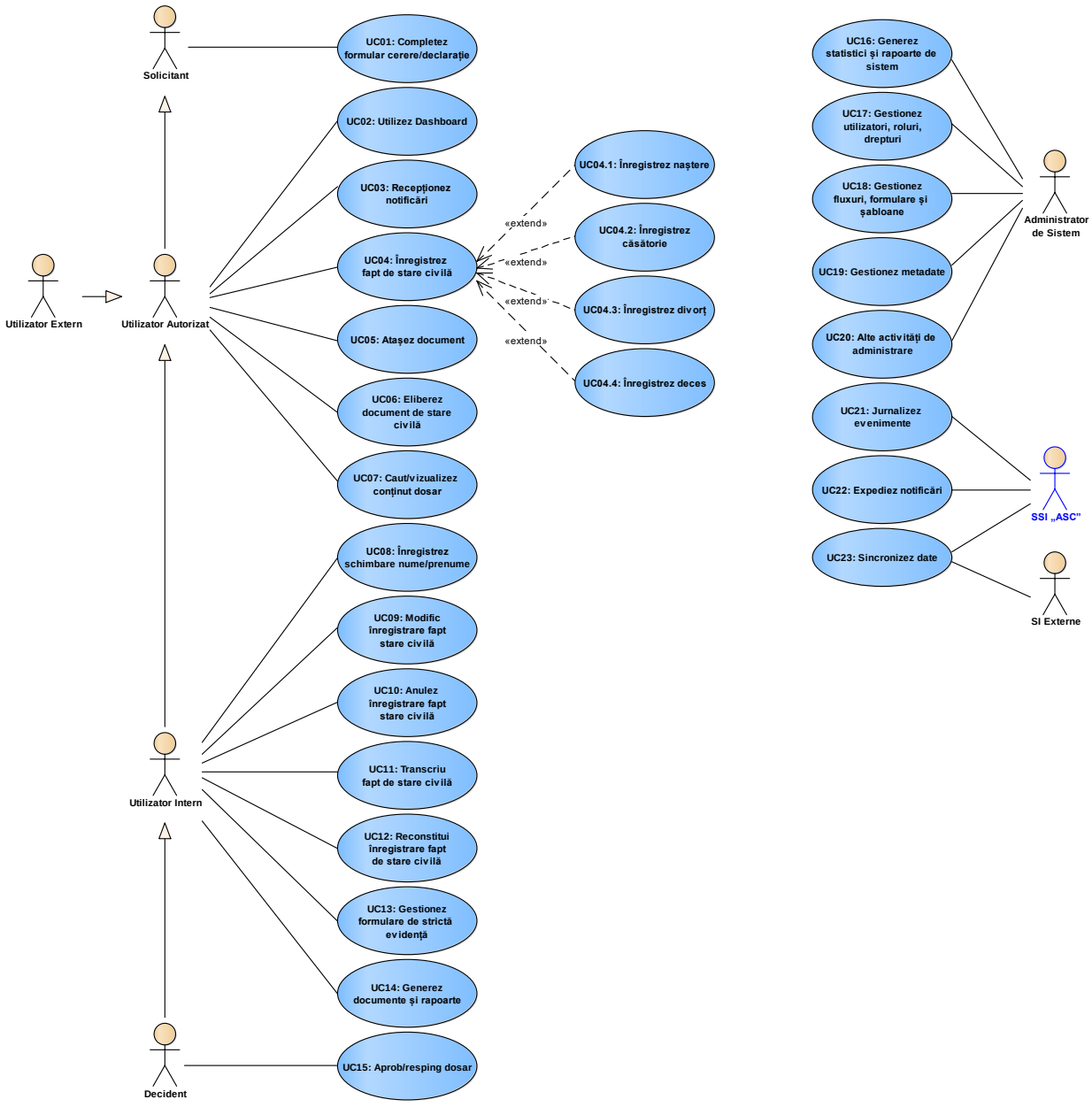

Figure 5.2. Use Cases provided by the ITSS "CSA".

UC01: Complete an unified application form or a statement

A Use Case that offers the Applicants all options to produce and send the application or statement to the Civil Status Body. Regardless of the method of submitting the unified application or statement (traditional or electronic), all would end with the creation of a case file for the registration of the civil status event or issuance of civil status document, electronic processing and provision of electronic services to notify and verify the case traceability.

UC02: Use Dashboard

It represents a functionality via which the ITSS "CSA" authorised User will be alerted, be able to view and rapidly access all business events related to its interaction with the ITSS "CSA" and job duties (system notifications, workflow events, etc.).

Likewise, it shall have direct access to functionalities related to notified business events (direct access to the case file on the registration of civil status events or of the lodged application form/statement, etc.).

The main page of User interface of the ITSS "CSA" authorised User will serve as Dashboard where all User's related elements and notifications will be displayed.

The Dashboard shall have also an area to display the list of case files aimed at registering newly opened civil status events, on-going events, recently reopened events and recently closed events, which the User is authorised to access.

UC03: Receive notifications

A Use Case via which the authenticated Users, regardless of their role (external User, internal User, *System Administrator,* etc.) shall receive the notifications sent by the *ITSS "CSA"* related to the business events they are involved in.

The ITSS "CSA" shall ensure the generation of notification in the requested format and its delivery. All categories of authorised Users would be able to configure individually their preferences for receiving the notifications via the personal Dashboard.

The ITSS "CSA" shall have the functionality to send out the notifications to individuals or entities via the platform service *MNotify*.

UC04: Register civil status facts

A Use Case that furnishes all the functionalities required to initiate and complete the electronic case file regarding the registration of a civil status fact.

UC05: Append documents

It represents a functionality via which the individual or authorised Users shall have access to all functionalities required to append documents to the case file regarding the registration of civil status facts (this Use Case shall be used whenever is needed to append files to the case) or to the unified application form.

UC06: Issue civil status documents

A Use Case via which it is envisaged to ensure the functionality of issuing civil status documents. Use Case UC14 shall deliver the data regarding the form of strict accountability series and number related to the CSD issuance to implement Use Case UC15.

UC07: Search/view Case content

A Use Case furnished by the ITSS "CSA" via which the authorised Users would be able to explore the stock of data they have access to, based on the role they hold within the IT system and their job duties.

To this end, the ITSS "CSA" shall offer a mechanism to search the case files on registering civil status facts and their content, using different criteria, such as:

- data for person identification;
- data related to Case authorised Users;
- data to identify the case file regarding the registration of civil status facts;
- calendar data related to case files to register civil status facts;
- calendar data related to business event forms of case files to register civil status facts;
- data related to CSB;
- data on business events related to cases regarding the registration of civil status facts;
- person's civil status;
- status of the case regarding the registration of civil status facts;
- etc.

ITSS "CSA" shall display as found search results:

- persons;
- case files to register civil status facts;
- business events of cases regarding the registration of civil status facts.

For each result category the *ITSS "CSA"* shall allow to carry out the following operations:

- for the persons found: view their profile, view the cases regarding the registration of civil status facts related to those persons, view business fact documents related to the cases regarding the registration of civil status facts;
- for the case files to register civil status facts: accessing the case content;
- for the business events related to the cases regarding the registration of civil status facts: view the document afferent to the event, access the electronic form to produce the business event.

In addition, the *ITSS "CSA"* shall deliver a mechanism for indexed search of data with full text search options and display the results depending on the relevance of the phrased query result.

UC08: Register the change of Last Name/First Name

A Use Case that furnishes all the functionalities required by the CSB Users for the registration of any change in the Last Name and/or the First Name.

UC09: Modify the registered civil status fact

A Use Case that furnishes all the functionalities required to initiate and complete the electronic case file to change a registered civil status fact.

UC10: Cancel the registration of a civil status fact

A Use Case that furnishes all the functionalities required to initiate and complete the electronic case file to cancel a registered civil status fact.

UC11: Transcribe a civil status fact registered abroad

A Use Case that furnishes all the functionalities required to initiate and complete the electronic case file to transcribe a civil status fact registered abroad.

UC12: Recover the registration of a civil status fact

A Use Case that furnishes all the functionalities required to initiate and complete the electronic case file to recover a registered civil status fact.

UC13: Manage forms of strict accountability (for authorised use only)

A Use Case via which the management and inventory of forms of strict accountability shall be ensured.

UC14: Generate documents and reports

This functionality is accessible to authorised Users of the *ITSS "CSA"* and *System Administrators* and allows for the generation of pre-defined and ad-hoc reports on the IT system information content and activity of authorised Users.

These Reports are useful to review the IT system information base, the authorised Users' activity performance, in particular, of entities they represent, enabling the retrieval of certain performance indicators to be used for reviewing the business processes of cases regarding the registration of civil status facts.

It is appropriate that the IT system comprises a solution intended to configure and generate reports (Report Generator) to be reused also for the configuration and retrieval of standard documents specific for *ITSS "CSA"* business processes. The documents can be generated also on the basis of configurable templates.

UC15: Approve/reject a Case

A Use Case available for the Users assigned with decision-making role within the *ITSS "CSA"* via which the Users would be able to approve or reject the draft electronic cases of business events related to the cases of registration, modifying, cancelling, transcribing or recovering civil status facts.

The process of approving or rejecting the business event electronic form consists of producing an opinion/comment, selecting the approval/rejecting option and affixing the electronic signature of the User assigned with decision-making role.

UC16: Generate statistics and system reports

This is a Use Case that furnishes all the functionalities accessible to Users of *System Administrator* level, which allows generating administrative predefined and ad-hoc reports on *ITSS "CSA"* operation events.

Such Reports are useful for reviewing the unrolled processes, the IT system information base, the authorised Users' activity performance, allowing to anticipate information security issues. Unlike UC16, the Use Case UC18 is intended for IT audit processes to assist the information security mechanisms.

UC17: Manage Users, roles, rights

The access rights shall be managed through the *IRAMS AIS Administrator*. The sets of roles for certain User groups will be created on the basis of the List of access roles.

The connection, disconnection, reconnection, change of rights will be done through *IRAMS AIS Administrator* only. The *ITSS "CSA"* shall retrieve the data about the rights of access from the IRAMS.

UC18: Manage flows, forms and templates

It represents a Use Case intended for *ITSS "CSA"* Administrators, which describes all the functionalities available to them to update the workflows, electronic forms and models of standard documents usable under each type of input and output document (configuring the areas of headings, footnotes, static and dynamic content, formatting, graphical appearance, etc.).

A document template shall comprise beacons, via which it would be possible to populate the template with content information retrieved from the content of the case file regarding the registration of civil status facts. Hence, it would be possible to harmonise and standardize the package of documents issued and processed under the *ITSS "CSA"*.

UC19: Manage metadata

A Use Case that furnishes to Users assigned with *System Administrator* roles access to functionalities intended to administer own nomenclatures, classifiers and metadata necessary to manage the whole system of metadata (classifiers, nomenclatures, constants, IT system configuration and operation parameters) of the *ITSS "CSA"*. The SRP general classifiers will be retrieved and updated from the *IRAMS*.

UC20: Other administration activities

It represents a Use Case intended for the *System Administrator,* describing all the accessible functionalities to administer and audit the *ITSS "CSA"*. The Use Case for *ITSS "CSA"* administration shall implement all the functionalities to ensure the IT system viability and integrity.

UC21: Logging events

A Use Case via which the business events generated by the *ITSS "CSA"* functional components shall be logged. Any event generated under the business processes implemented within the *ITSS "CSA"* shall be logged and saved in the corresponding DB tables.

The logging mechanism shall be developed based on the standards and best practices implemented in this field. The IT system shall deliver functionalities to configure the logging strategy of business events, including: categories of business events subject to logging, the calendar period of logging (specified or unspecified), etc.

For critical or sensitive business events, logging shall be carried out in parallel, using the platform service *MLog* (for instance, access via *MConnect*).

UC22: Send notifications

A Use Case that furnishes functionalities to notify the *ITSS "CSA"* authorised Users. All notifications shall be stored in the authorised Users' Dashboard to ensure direct access to the electronic form of the business event that generated the notification.

The ITSS "CSA" shall automatically generate and send out notifications afferent to each business event generated by civil status event registration processes and changes in the case status.

Likewise, the *ITSS "CSA"* shall automatically generate and send out to authorised Users notifications related to any business event requiring their involvement.

The System shall furnish the mechanisms for in-house notification (integrated under the *ITSS "CSA"*) and integrate external notification mechanisms via the platform service *MNotify*, as appropriate.

UC23: Synchronise data

A Use Case that shall furnish the functionalities required by the *ITSS "CSA"* to exchange data with external IT systems.

This synchronisation refers to the specialised API displayed by external IT systems intended to furnish relevant data contained in the electronic case files to register civil status facts or issuance of civil status documents and the use of *APIs* provided by third IT systems to complete the electronic case file regarding the registration of civil status facts.

To a large extent, all synchronisations shall be carried out via the interoperability platform *MConnect*. Likewise, the *ITSS "CSA"* shall interact with the core platform services: *MPass, MSign, MLog, and MNotify*.

5.3. User interface ITSS "CSA"

The ITSS "CSA" shall offer an ergonomic, intuitive User interface that is accessible to all types of Users. The IT system User interface shall be accessed via an Internet Browser. The *ITSS "CSA"* shall have an intuitive, agreeable, balanced and distinctly optimised graphical design for a minimum resolution of 1360x468 to work on PC-type computers.

Likewise, the User interface shall be responsive to the resolutions of such devices as smartphones and tablets and be optimised for touch-screens.

For the Users' usability, the IT solution shall have a contextual on-line help system at the level of each User interface.

Depending on the categories of Users (their rights and roles), the IT system shall furnish a customised interface for each category of Users.

The ITSS "CSA" shall furnish an interface in Romanian. The information and record retrieval/tracing procedures will be implemented via simple searches (specifying search series) or more complex searches to ensure more precise filtering of the information (QBE forms). Regardless of the nature of the searched information, the User shall use the same information query and retrieval method for each part of the IT product.

In addition to the search module based on QBE principle, which would enable defining visually sophisticated queries, the interface shall provide the possibility to fine-tune the search results by granting the possibility to filter the data in the list of search results.

The IT system User interface shall ensure filtering the records that match the search criterion granted to Users depending on their access rights.

There should be the possibility to filter the indexed values (from classifiers, nomenclatures) by choosing the value form a predefined list. Also, there should be the possibility to filter the fields of numerical types or calendar dates by the precise value of the searched characteristics or by search mask.

There should be the possibility to export the content of any result-containing table or electronic form in CSV, RTF and PDF format, depending on the nature of the comprised information. The data export shall be strictly outlined by the roles. All export actions shall be logged.

5.4. Reporting, Auditing and Statistics System of the ITSS "CSA"

The ITSS "CSA" should have implemented auditing/logging functionalities widely used in this area. This is configurable for logging technical and business events. The IT System shall deliver a mechanism to generate predefined and ad-hoc reports capable to ensure pertinent reviews or assessments of anti-corruption survey processes of legislative/regulatory documents.

The ITSS "CSA" reporting system shall outline three categories of reports:

- **Performance Indicators** – this is a range of KPIs based on which the status of the drafted document or the work performance of the PSA Users will be assessed, regardless of the assigned role;
- **Monitoring Reports** – this is a category of reports intended for PSA Decision Makers to assess the way of interaction of authorised Users with *the ITSS "CSA".* This category of reports shall allow anticipating performance issues in the activity of PSA subdivisions and employees *or* IT System security and vulnerability issues;
- **Performance Reports** – this is a category of static reports (as a rule, implemented physically in the IT System content) focused on auditing and reviewing the ITSS "CSA" information content *(example: authorised User performance report; territorial subdivisions performance report; PSA performance report, etc.).*

6. ITSS "CSA" functional requirements

6.1. Agreements used to draw up the functional requirements

The requirements outlined in this document are marked using the following agreement:

- all requirements are indexed with three values: **C, X,** and **Y**, where **C** represents the category of requirements (FR – functional requirement); **X** represents the Use Case for which a functional requirement is phrased; and **Y** is the single identifier of requirements for the Use Case it is part of.
- the binding level is shown for each functional requirement: **M** – mandatory requirement to be implemented, **D** – desirable/optional requirement to be implemented.

The bid submitted by the *Bidder* shall meet all the requirements stated as binding.

The bid submitted by the *Bidder* shall get competitive advantage for each desirable/optional requirement it comprises.

The informative requirements are intended to offer more data to ensure better understanding of the context of other requirements.

6.2. UC01: Complete a standard Application/Statement form

The functional requirements for the component related to producing a unified Application Form requiring civil status services are displayed in Table 6.1.

Table 6.1. Functional Requirements for Use Case UC01

Identifier	Binding level	Description of Functional Requirements
FR 01.01	M	The System shall deliver a mechanism for the completion of application forms and statements intended for Applicants, external or internal User-type actors.
FR 01.02	M	The actors assigned with *Applicant* role shall access the application form/statement via *PSP (http://servicii.gov.md) or* the PSA Official WEB Page *(http://asp.gov.md).*
FR 01.03	M	The actors assigned with *Applicant* role shall access and complete the application/statement form, having authenticated themselves via *MPass.*
FR 01.04	M	In case of authentication through *MPass* the *Applicant* identification data *will be* completed automatically with the relevant information furnished by *MPass.*
FR 01.05	M	External and internal Users will authenticate themselves in the *ITSS "CSA"* to review and handle the applications or statements received from *Multifunctional Centres for Service Provision or from the GCSD One-Stop Shop.*
FR 01.06	M	*The ITSS "CSA"* shall save the application/statement form only when all mandatory fields of the form have been completed.
FR 01.07	M	The incomplete application/statement form (that does not contain all the data necessary for its consideration) shall be deleted if it was not sent within one hour.
FR 01.08	M	The System shall generate a single identification number for the application/statement submitted for consideration.
FR 01.09	M	The System shall issue *the Applicant* a receipt (notification) about receiving the application/statement.

Identifier	Binding level	Description of Functional Requirements
FR 01.10	M	The System shall send the receipt (notification) about receiving the application/statement and their printable version to the Email address stated by the *Applicant* (or provided by *MPass*).
FR 01.11	M	The receipt about receiving the application/statement shall contain the single registration number, the date and time when it was received by the system.
FR 01.12	M	The time related to the receipt of application/statement will be retrieved from the State Time Stamping Service.
FR 01.13	M	Regardless of the way of submitting the application/statement (using traditional or electronic means), all applications/statements shall be processed through the same technological flows offered by the *ITSS "CSA".*
FR 01.14	M	The application/statement can be sent for consideration only if all electronic copies of the documents specified in the terms and conditions for service rendering and metadata related to them have been appended.
FR 01.15	M	*The Applicant/Declarant* shall have the possibility to sign digitally the electronic application/statement form and all the files appended thereto.
FR 01.16	M	*The ITSS "CSA"* shall allow checking the authenticity of the digital signature affixed on the application/statement form and on documents appended to the application.
FR 01.17	M	When submitting applications for services rendered for a fee, *the ITSS "CSA"* will allow settling the payment via MPay platform service.
FR 01.18	M	Depending on the configuration parameters of the electronic form used to submit a public service request, the *ITSS "CSA"* shall comprise all the data necessary to send the payment for processing.
FR 01.19	M	Upon launching the procedure for settling the payment online, *the ITSS "CSA"* shall deliver to MPay the parameters necessary to complete the Payment Order (Recipient's data, Payer's data, payment details, etc.).
FR 01.20	M	Following the settlement of the payment online, the *ITSS "CSA"* shall receive from MPay the details on the payment made, which will be inserted automatically into the content of the application form (the proof payment is inserted into the form).

6.3. UC02: Use Dashboard

The functional requirements intended to implement the *Dashboard* tool for *ITSS "CSA"* authenticated and authorised Users are displayed in Table 6.2.

Table 6.2. Functional Requirements for Use Case UC02

Identifier	Binding level	Description of Functional Requirements
FR 02.01.	M	*The ITSS "CSA"* shall deliver a *Dashboard* to authorised Users to notify them on important business events, enabling quick access to the event details and organising Users' activity.
FR 02.02.	M	The following categories of business events displayed on the *Dashboard* can be listed (available depending on the roles and rights assigned to the *ITSS "CSA"* authorised User):

Identifier	Binding level	Description of Functional Requirements
		• system notifications; • notifications on tasks received by the User to deal with; • notifications on workflows monitored by the User; • notifications on exceeding the deadline for carrying out the tasks assigned to the User; • notifications on the need to involve the User in the ITSS "CSA" workflows; • notifications on documents or processes pending the approval of Users with Decision-making roles; • notifications on the approvals of dates of the proposed agenda events; • other relevant events.
FR 02.03.	M	*The Dashboard* of the ITSS "CSA" User shall display only business events relevant to functionalities and data available for each authorised User depending on his/her rights and roles.
FR 02.04.	M	*The Dashboard* shall group the business events, having displayed them as indicators with aggregated values (example: Unread system notifications – 20; Documents for approval – 41; Documents which time-limit set for their execution has been exceeded – 25; Applications received – 5, etc.), which will contain hypertext reference to access the details (related records).
FR 02.05.	M	*The ITSS "CSA"* shall display detailed records of the *Dashboard* in specialised windows or fields on the User Interface main page, which will contain hypertext reference to access the details (case files, civil status acts, electronic forms, etc.).
FR 02.06.	M	*The ITSS "CSA"* shall provide each User with the functionality for individual configuration of the *Dashboard* appearance and content (configure the notification preferences, configure the areas with important content the authorised User is currently working with, the location of content categories on the *Dashboard).*

6.4. UC03: Receive notifications

The functional requirements for implementing the mechanism intended to receive notifications sent by the ITSS "CSA" *to* authorised Users are displayed in Table 6.3.

Table 6.3. Functional Requirements for Use Case UC03

Identifier	Binding level	Description of Functional Requirements
FR 03.01.	M	*The ITSS "CSA"* shall notify automatically any authorised User in case of registering a business event involving the action of the User or changing the status of processes he/she manages or monitors or the processes he/she is concerned with.
FR 03.02.	M	The authorised Users shall receive notifications to the Email address stated in their profile in the ITSS "CSA".
FR 03.03.	M	A copy of the notification shall be displayed on the User Dashboard.
FR 03.04.	M	The authorised User shall have the functionality to configure the preferences for receiving the notifications to the Email address.

Identifier	Binding level	Description of Functional Requirements
FR 03.05.	M	*The ITSS "CSA"* shall send the whole range of notifications intended for the authorised Users: • notification on opening/closing/reopening the case files on registering, changing, cancelling, transcribing or recovering civil status facts; • notification on the need to get involved in the *ITSS "CSA"* workflows; • notification on the delay of User action (exceeding the time-limit for checking the report, applying the decision, etc.); • notification on accepting/rejecting the case files on registering the civil status events; • notification on *ITSS "CSA"* operation issues; • other relevant notifications.
FR 03.06.	M	A notification sent via Email can comprise an appended file (example*: Case file refuse, Court judgement, etc.).*
FR 03.08.	M	*The ITSS "CSA"* shall allow sending notifications via Email in HTML or reach text Format.
FR 03.09.	M	The System can send specific notifications such as Warnings. The latter require some actions to be undertaken following the occurrence of certain events in other processes or sub-processes.
FR 03.10.	M	The warnings shall be generated both automatically and manually by the authorised Users.
FR 03.11.	M	The actions carried out following the warnings could be: • Deliberate refusal related to the person – the *ITSS "CSA" shall generate* and send a refusal message associated with the person data; • Deliberate refusal due to the situation – the *ITSS "CSA" shall generate* and send a refusal message due to the document data or due to an event (configurable for the User Interface with the System Administrator role) that has occurred; • Informing the *Applicant/Declarant – the ITSS "CSA"* shall generate a message to inform the Applicant/Declarant about the warning detected to address this issue; • Informing the *PSA GCSD Decision-makers* – the *ITSS "CSA"* shall generate a message to inform the Users – Decision-makers about the detected warning (the occurrence of an event linked to the registration logic or to an intervention need) requiring an advice or problem resolution; • Informing the *System Administrator – the ITSS "CSA"* shall generate a message to inform the System Administrators about the occurrence of technical problems; • Other actions and warnings detected throughout the review phase.
FR 03.12.	M	*The ITSS "CSA"* shall record all the reactions to warnings in the system log.

6.5. UC04: Register civil status facts

The functional requirements specifying the peculiarities of implementing the component intended for opening, closing and reopening the case files to register civil status facts are displayed in Table 6.4.

Table 6.4. Functional Requirements for Use Case UC04

Identifier	Binding level	Description of Functional Requirements
FR 04.01.	M	*The ITSS "CSA"* shall deliver electronic forms to be used for opening the case files to register civil status facts.
FR 04.02.	M	The case file to register civil status facts shall go through many processing stages, the initial stage dealing with the registration of facts with "draft" status.
FR 04.03.	M	A case may be opened manually by an User assigned with the internal User role (civil status officials) or external User role (DM/CO officials or LPA officials), having accessed the *ITSS "CSA"* corresponding functionality or automatically when receiving a final judgment on the dissolution of marriage, depriving of parental rights or enforceability of adoption, when making a new record on the birth/death confirming medical certificate, in other cases.
FR 04.04.	M	Regardless of how it was initiated, the case file to register civil status facts shall have the initial status "Draft".
FR 04.05.	M	Depending on the registration type and registration flow peculiarities, the *ITSS "CSA"* shall display the list of binding documents to be appended. Electronic documents with reference to civil status already entered into the system shall be acquired automatically.
FR 04.06.	M	*The ITSS "CSA"* shall allow adding all documents via UC05 and, where appropriate, append electronic copies of relevant documents to the case file.
FR 04.07.	M	Upon opening a registration case file, it will be required to identify the civil status acts of the person(s) registered previously in the SRP, by his/her(their) INDP. To this end, a query will be sent to the *SRP and* all the data identifying the person(s) and the civil status will be retrieved automatically.
FR 04.08.	M	*The ITSS "CSA"* shall have a mechanism to verify logically the registration; it shall not enable a registration to be made if the logic check failed (registration of a divorce without a marriage document, registration of a marriage when one of the spouses is already married).
FR 04.09.	M	If the logic check failed, the *ITSS "CSA"* shall issue a warning and channel the registration of facts to PSA GCSD Users assigned with decision-making roles.
FR 04.10.	M	*The ITSS "CSA"* shall check the case file completeness and the correctness of entered data.
FR 04.11.	M	*The ITSS "CSA"* shall allow introducing into the system the date and time of handing the civil status document.
FR 04.12.	M	When registering the change of the last Name and/or the First Name, the *ITSS "CSA"* shall have the functionality to convey (as per UC15) the registration case file to the User assigned with decision-making role for approval.
FR 04.13.	M	The authorised User responsible for the case file shall sign electronically the registration case.
FR 04.14.	M	*The ITSS "CSA"* shall log all the events on opening, closing and reopening the CSA registration case files.

Identifier	Binding level	Description of Functional Requirements
FR 04.15.	I	There is a special category of people – *"People with specific religious beliefs"* (people who refused to be issued an IDNP) for whom there is a separate registration scenario. During the technical design phase, the successful Bidder shall review the peculiarity of registering these categories of people and suggest solutions to optimise the flows.

6.6. UC05: Append document

The functional requirements related to the component of appending copies of documents to the application, statement or electronic case file for civil status facts registration are displayed in Table 6.5.

Table 6.5. Functional Requirements for Use Case UC05

Identifier	Binding level	Description of Functional Requirements
FR 05.01.	M	*The ITSS "CSA"* shall deliver functionalities to append electronic copies of relevant documents (both binding and optional) to the application, statement or case file registering civil status facts.
FR 05.02.	M	*The ITSS "CSA"* shall deliver a mechanism to input the metadata related to the digital documents appended to the application, statement or case file.
FR 05.03.	M	The nature of metadata related to the digital documents appended to the application, statement or case file shall be sufficient to define efficient queries for their retrieval.
FR 05.04.	M	All the documents appended to the case file shall be in PDF format.
FR 05.05.	M	*The ITSS "CSA"* shall have the functionality to configure the maximum size of appended documents.

6.7. UC06: Issue civil status documents

The functional requirements of the mechanism for issuing civil status documents are displayed in Table 6.6.

Table 6.6. Functional Requirements for Use Case UC06

Identifier	Binding level	Description of Functional Requirements
FR 06.01.	M	*The ITSS "CSA"* shall deliver a mechanism to issue civil status documents. Such documents (certificates, statements) shall be issued on an optional basis, upon the request deliberately stated in the standard application requiring services.
FR 06.02.	M	This mechanism shall be envisaged to issue the following documents: • Duplicate of the civil status certificate; • Statement from a civil status document; • Multilingual statement from a civil status document; • Civil status certificate; • Opinion to confirm or reject the change of the Last Name and/or First Name (is issued by the *GCSD*); • Opinion to cancel, rectify and/or supplement the civil status document;

Identifier	Binding level	Description of Functional Requirements
		• Explanatory certificate; • Opinion to the fact that the civil status document is missing; • Certificate of matrimonial capacity; • Explanatory documents F-28.
FR 06.03.	M	*The ITSS "CSA"* shall have the functionality to issue a statement (Personal records) for all civil status events of the person.
FR 06.04.	M	*The ITSS "CSA"* shall have the functionality to identify the previously registered *CSAs* from where all the data related to the CSD will be retrieved to the SRP.
FR 06.05.	D	The Applicants shall have access to an interface through which to require online the CSD, having authenticated themselves via MPass. There should be the possibility to require it via a dedicated interface of the *ITSS "CSA"* (displayed on the PSA Official WEB Page) or via an interface displayed on the *Public Services Portal* (http://servicii.gov.md).
FR 06.06.	M	The civil status document shall be issued on the basis of an application form.
FR 06.07.	M	*The ITSS "CSA"* shall provide an electronic form to complete the application, made available to authorised Users, such as *PSA Operator, PSA GCSD and CSO GCSD* (to enter/input the applications of citizens who visited the Civil Status Office or General Civil Status Division in person).
FR 06.08.	M	The ITSS "CSA" shall deliver a functionality to append a copy to the application requiring the issuance of a CSD.
FR 06.09.	M	The application forms for issuing a CSD submitted online must contain a digital signature (the digital signature shall be affixed via *MSign*) and the possibility to append a scanned document (power of attorney, mandate, etc.).
FR 06.10.	M	Regardless of the way of submitting the application for issuing a CSD (online or traditionally), the application processing flow will be the same.
FR 06.11.	M	*The ITSS "CSA"* shall deliver a functionality to generate the document related to the application requiring the issuance of a CSD.
FR 06.12.	M	For the applications submitted online to issue a CSD, the *ITSS "CSA"* shall generated and send automatically to the Applicant a document with the receipt regarding the received application, having a digital signature affixed on it.
FR 06.13.	M	*The ITSS "CSA"* shall deliver functionality for manual generation of a document related to the receipt requiring a CSD to be issued.
FR 06.14.	M	*The ITSS "CSA"* shall deliver to PSA GCSD Users and CSO GCSD assigned with relevant roles a mechanism to generate CSDs.
FR 06.15.	M	*The ITSS "CSA"* shall allow retrieving CSDs in a PDF file on which the PSA digital signature is affixed or imprinted.
FR 06.16.	M	The payment for the services provided for a fee shall be settled based on "Bills" (form approved by the *PSA*). The Developer shall configure under the *ITSS "CSA"* the "Bill" template approved by the *PSA*.
FR 06.17.	M	The Applicant shall have the option to pay for the rendered service via *MPay*.

Identifier	Binding level	Description of Functional Requirements
FR 06.18.	M	When the option to pay via MPay is selected, the *ITSS "CSA"* shall insert the bill in the receipt, having sent the latter to the *Applicant.*
FR 06.19.	M	*The ITSS "CSA"* shall wait for the payment confirmation from the *MPass*, and only after that it shall convey the application to the CSD consideration, preparing and issuance flow. The waiting time shall be configurable from the User Interface assigned with *System Administrator* role.
FR 06.20.	M	If the payment for the service is not settled within the established deadline, the *ITSS "CSA"* shall cancel the application.
FR 06.21.	M	Upon the issuance of a CSD printed on a form of strict accountability, the User shall insert the serial number of the form (as per the functional requirements specified in *UC13 – Managing the Forms of Strict Accountability*).
FR 06.22.	M	When a form of strict accountability is damaged in the process of printing the CSD, the authorised User shall have the functionality to introduce the serial number of the damaged form (as per the functional requirements specified in UC13 – *Managing the Forms of Strict Accountability*).

6.8. UC07: Search/view the Case content

The functional requirements necessary to define the information search queries within the content of the case file collection created in the process of registering civil status facts and managing the obtained results are displayed in Table 6.7.

Table 6.7. Functional Requirements for Use Case UC07

Identifier	Binding level	Description of Functional Requirements
FR 07.01.	M	*The ITSS "CSA"* shall deliver a mechanism to search the data and documents in the content of Case files created in the process of civil status fact registration.
FR 07.02.	D	*The ITSS "CSA"* shall deliver a mechanism for indexed search of electronic case files registering civil status events in the collection of data. The search mechanism shall use morphological means.
FR 07.03.	M	*The ITSS "CSA"* shall allow defining the following search targets (the search result will display a list of): • case files registering civil status events; • documents contained in the case files registering civil status events; • profiles of individuals; • the text of explanations included in the opinion or refusal; • electronic forms prepared and contained in the files.
FR 07.04.	M	*The ITSS "CSA"* shall deliver a flexible and efficient mechanism to define the search criteria.
FR 07.05.	M	When the formulated search criteria are too large or require too much time and too many resources to be enforced, the *ITSS "CSA"* shall not perform those queries, having required the User to narrow the area of searched values.

Identifier	Binding level	Description of Functional Requirements
FR 07.06.	M	The search results shall be displayed in orderly manner depending on the query relevance, in alphabetic order or according to the date of its creation/last update.
FR 07.07.	M	The User shall be able to define criteria for ordering and grouping the list content comprising the search results.
FR 07.08.	M	The System shall provide a mechanism for paging the search results to avoid overloading the WEB browser and data transmission channels.
FR 07.09.	M	The recordings of search results shall be marked (by specific colour or icon) depending on the nature or status of the information object retrieved/found.
FR 07.10.	M	*The ITSS "CSA"* shall deliver a functionality to refine the search in the list of results.
FR 07.11.	M	*The ITSS "CSA"* shall allow launching certain processes over the identified results or over a group of results such as: • launching the creation of a business event form to include the results in the form (example*: including a group of Users' profiles as authorised people in the case file*); • multiple deletion; • multiple electronic signing; • multiple approval or refusal; • other relevant actions.
FR 07.12.	M	*The ITSS "CSA"* shall display in the search results only the data that match the User's area of competence.
FR 07.13.	M	*The ITSS "CSA"* shall restrict the access to the search result details when the User who launched the search does not have access to the information objects required to be accessed.
FR 07.14.	M	*The ITSS "CSA"* shall allow exporting the Table with search results in CSV, RTF or PDF formats.

6.9. UC08: Register the change of Last Name and/or First Name

The functional requirements specifying the peculiarities for implementing the component intended to register the change of Last Name and/or First Name are displayed in Table 6.8.

Table 6.8. Functional Requirements for Use Case UC08

Identifier	Binding level	Description of Functional Requirements
FR 08.01.	M	*The ITSS "CSA"* shall furnish the mechanism for the applications to change the last Name and/or the First Name as per of Use Case *UC01*.
FR 08.02.	M	If no civil status acts have been preserved, the *internal User* shall have the functionality to initiate the process of recovering the registration of civil status facts.
FR 08.03.	M	The Developer shall implement the mechanism to register the conclusion on the change of the Last Name and/or the First Name.

Identifier	Binding level	Description of Functional Requirements
FR 08.04.	M	The form to register the fact of changing the Last Name and/or the First Name shall comprise the following fields: • date of form registration and its registration number; • name of the CSB that registered the change of the Last Name and/or the First Name; • the Applicant's Last Name and First Name before the change and after the change, the date and place of birth, domicile; • references to the civil status facts, on the holder's name, to be subject to change following the change of the Last Name and/or the First Name; • serial number of the certificate issued with respect to the change of the last Name and/or the First Name; • other fields, as appropriate.
FR 08.05.	M	The certificate on the change of the last Name and/or the First Name shall include the fields as per the approved model of the CSD.

6.10. UC09: Modify the registration of Civil Status Facts

The functional requirements specifying the peculiarities for implementing the component intended to open, close and reopen the case files to modify the Civil Status Fact records are displayed in Table 6.9.

Table 6.9. Functional Requirements for Use Case UC09

Identifier	Binding level	Description of Functional Requirements
FR 09.01.	M	*The ITSS "CSA"* shall furnish the mechanism to identify and retrieve civil status facts from the SRP subject to change.
FR 09.02.	M	The Developer shall implement under UC09 the functional requirements FR 04.02. – FR 04.14.
FR 09.03.	M	*The ITSS "CSA"* shall allow registering mentions in the form where the amended fact was recorded.
FR 09.04.	M	When there is a need to issue the CSD after amending the fact registration, the *ITSS "CSA"* shall launch the flow for issuing the CSD as per the functional requirements of UC06.
FR 09.05.	M	*The ITSS "CSA"* shall allow amending more than one forms containing civil status facts, which refer to the same person under the same case file.
FR 09.06.	M	The authorised User responsible for the case file shall sigh electronically the fact of registration.
FR 09.07.	M	*The ITSS "CSA"* shall log all the events on opening, closing, reopening the case files to amend the records on civil status facts, the selected reason and basis.

6.11. UC10: Cancel the registration of Civil Status Facts

The functional requirements specifying the peculiarities for implementing the component intended to open, close and reopen the cases to cancel the registration of Civil Status Facts are displayed in Table 6.10.

Table 6.10. Functional Requirements for Use Case UC10

Identifier	Binding level	Description of Functional Requirements
FR 10.01.	M	*The ITSS "CSA"* shall furnish a mechanism to identify and retrieve from the *SRP* the form registering the civil status fact to be cancelled as per multiple criteria: form type, registration number, person, etc.
FR 10.02.	M	The Developer shall implement under *UC10* the functional requirements *FR 04.02 – FR 04.14*.
FR 10.03.	M	The form recording the fact shall be cancelled in the following cases: • two (repeated) civil status records were identified, which were prepared for the same fact (birth, death, divorce). The annulment shall take place via the annulment case file organised and approved by the PSA GCSD, • there is a recovered form of the registered civil status fact and the primary document has been identified, which was produced upon the registration of the same fact; • the annulment of the form registering a civil status fact, which was produced unlawfully or on the basis of fake documents, shall be done by courts.
FR 10.04.	M	*The ITSS "CSA"* shall allow creating links between case files (for instance, the case file for cancelling shall have a link to the case file it has cancelled and vice versa, and to the civil status fact registered correctly).
FR 10.05.	M	*The ITSS "CSA"* shall allow to record mentions in the form where the cancelled fact was registered.
FR 10.06.	M	The authorised User responsible for the case file shall sigh electronically the fact of cancelling.
FR 10.07.	M	*The ITSS "CSA"* shall log all the events of opening, closing, reopening the cancelling case files.

6.12. UC11: Transcribe the Civil Status Fact registered abroad

The functional requirements specifying the peculiarities for implementing the component intended to open, close and reopen the cases to transcribe the Civil Status Facts registered abroad are displayed in Table 6.11.

Table 6.11. Functional Requirements for Use Case UC11

Identifier	Binding level	Description of Functional Requirements
FR 11.01.	I	Transcribing the civil status facts represents a *UC04* peculiarity.
FR 11.02.	M	The Developer shall implement under *UC12* the functional requirements *FR 04.02 – FR 04.14*.
FR 11.03.	M	*The ITSS "CSA"* shall deliver the functionality to submit for approval to the User assigned with decision-making role, as per *UC15*.
FR 11.04.	M	*The ITSS "CSA"* shall allow registration of mentions in the form recording the transcribed fact.
FR 11.05.	M	The authorised User responsible for the case file shall sign electronically the fact of transcription.
FR 11.06.	M	*The ITSS "CSA"* shall log all the events of opening, closing, reopening the case files for transcription.

6.13. UC12: Restore the registration of Civil Status Facts

The functional requirements specifying the peculiarities for implementing the component intended to open, close and reopen the cases to restore the records of Civil Status Facts are displayed in Table 6.12.

Table 6.12. Functional Requirements for Use Case UC12

Identifier	Binding level	Description of Functional Requirements
FR 12.01.	M	The ITSS "CSA" shall deliver the functionality to search and identify a CSA in the SAIS (Archive Fund of Digitised Civil Status Acts) and SRP.
FR 12.02.	M	The Developer shall implement under *UC12* the functional requirements *FR 04.02 – FR 04.14*.
FR 12.03.	M	*The ITSS "CSA"* shall allow the registration of mentions in the form recording the recovered fact.
FR 12.04.	M	The authorised User responsible for the case file shall sign electronically the fact of CSA recovery.
FR 12.05.	M	*The ITSS "CSA"* shall log all the events of opening, closing, reopening the case files for recovery.

6.14. UC13: Manage forms of strict accountability

The functional requirements related to the mechanism of managing the forms of strict accountability by the *ITSS "CSA"* are displayed in Table 6.13.

Table 6.13. Functional Requirements for Use Case UC13

Identifier	Binding level	Description of Functional Requirements
FR 13.01.	M	*The ITSS "CSA"* shall allow the initiation of flows comprising documents of strict accountability within the system. The inventory card of such documents shall contain data on: • the Working Group composition; • the Working Group Decision (*DOMC Report* – appended document); • successful Bidder's data; • date of contract conclusion and its duration; • quantity of printed and delivered documents of strict accountability; • other relevant data.
FR 13.02.	M	*The ITSS "CSA"* shall offer a functionality to require forms of strict accountability. In its request, the internal or external User shall state the required type and quantity of documents of strict accountability.
FR 13.03.	M	*The ITSS "CSA"* shall have a mechanism for keeping records on the issued forms of strict accountability, by Applicants, serial number, type, date of distribution and purpose.
FR 13.04.	M	Based on the gathered data, the *ITSS "CSA"* shall generate reports on the distribution and use of forms of strict accountability.
FR 13.05.	M	*The ITSS "CSA"* shall have a mechanism to read the barcode imprinted on the forms of strict accountability.

Identifier	Binding level	Description of Functional Requirements
FR 13.06.	M	Upon the issuance of a CSD, the User shall introduce the serial number of the form of strict accountability, using the barcode reading devices.
FR 13.07.	M	*The ITSS "CSA"* shall offer a functionality to identify civil status documents and the profile of the person concerned based on the read barcode.

6.15. UC14: Generate documents and reports

The functional requirements of the mechanism to retrieve the documents and reports to be displayed in a way convenient for Users or to support the decision-making process are displayed in Table 6.14.

Table 6.14. Functional Requirements for Use Case UC14

Identifier	Binding level	Description of Functional Requirements
FR 14.01.	M	*The ITSS "CSA"* shall be able to provide a number of statistical and ad-hoc reports, so that the PSA Decision-makers could monitor the civil status events registration activity.
FR 14.02.	D	It is appropriate to have a platform serving as basis to generate reports, which is used to configure the dynamic generation of reports.
FR 14.03.	M	*The ITSS "CSA"* shall make available a standard number of configurable reports to PSA Decision-makers and authorise in an easy way the production of ad-hoc reports where necessary.
FR 14.04.	M	*The ITSS "CSA"* shall grant a range of documents to be generated on the basis of data contained in the case files registering civil status events and of data from the functional modules "CIVIL STATUS ACTS" and *the SRP modules*: • Application to issue a CSA; • Birth/death confirming medical certificate; • CSO Opinion; • Civil status documents; • Decision on establishing the Name; • Statement on a civil status event; • Other relevant documents.
FR 14.05.	M	*The ITSS "CSA"* shall have predefined (editable) templates for each type of document afferent to the case file review process containing civil status events.
FR 14.06.	M	*The ITSS "CSA"* shall deliver a mechanism to input the metadata related to digital documents appended to the application, statement or case file.
FR 14.07.	M	*The ITSS "CSA"* shall insert automatically the variable information in the document template afferent to the case file review process (shall populate the template content with information from the DB content).
FR 14.08.	D	*The ITSS "CSA"* shall allow issuing documents in electronic format related to the electronic case file review process, having affixed the PSA digital signature via the integration with the *HSM Private Signature Service*.
FR 14.09.	M	*The ITSS "CSA"* shall offer a range of reports intended to monitor the civil status event registration process:

Identifier	Binding level	Description of Functional Requirements
		• The number of CSD registered over a specified time period, the registration body and CSD type; • Proceeds collected over a specified time period, the registration body and CSD type; • The quantity of documents of strict accountability and the number of such documents that were spoiled, over a specified timeframe, the registration body and type; • The most frequent First Name (male/female); • The most frequent double First Name (male/female); • The least frequent First Name (male/female); • The number of newborns by parents' ethnic group (nationality) (mother/farther); • The youngest and the oldest father; • The youngest and the oldest mother; • The number of children born by minor parents; • The most frequent age at the time of marriage; • The oldest age at the time of marriage; • The list of countries and the number of marriages where Moldovan citizens register their marriage (transcription of the marriage certificate) for a definite timeframe; • The number of dissolved marriages registered during the same year with the marriage document; • The number of divorce documents prepared on the basis of common agreement of spouses without minor children; • The number of divorce documents prepared on the basis of common agreement of spouses with minor children; • The number of divorce documents prepared on the basis of court judgements; • The most frequent age at the time of marriage dissolution; • The list of countries and the number of divorces registered by Moldovan citizens (transcription of divorce certificates); • The number of deceased people structured by the body of act registration, gender, major/minor, children who died during the first week/year of life; • The average age of deceased people; • The list of foreign citizens who died and were registered on the territory of the Republic of Moldova; • The list of facts of marriage registered on the name of foreign citizens (one of the spouses); • The list of facts of divorce registered on the name of foreign citizens (one of the spouses); • The list of countries and the number of registered death of Moldovan citizens (transcription of death certificates); • The number of amendments operated in CSAs (as per the selected reason/basis); • The number of registered documents by the registration body, timeframe and type;

Identifier	Binding level	Description of Functional Requirements
		• The number of issued civil status documents: primary, duplicate, documents issued following the amendment, following the completion of the form registering the divorce, etc.; • Other reports identified over the review phase.
FR 14.10.	M	*The ITSS "CSA"* shall have a mechanism to define the range of reports and data available for each category of Users, depending on their assigned roles and rights.
FR 14.11.	M	A User who can view a report within the system shall be able to export it into an external editable file (.XLSX and .DOCX).
FR 14.12.	M	By default, the reports shall be retrieved in .PDF format.
FR 14.13.	M	Overall, the Developer shall implement up to 50 categories of predefined reports requested by the Beneficiary.
FR 14.14.	M	*The ITSS "CSA"* shall log all the events related to the report and document generation and printing.

6.16. UC15: Approve/reject a Case File

The functional requirements of the component intended for PSA Users assigned with decision-making roles *(CSO Head)* to approve or reject the electronic forms produced via the *ITSS "CSA"* are displayed in Table 6.15.

Table 6.15. Functional Requirements for Use Case UC15

Identifier	Binding level	Description of Functional Requirements
FR 15.01.	M	*The ITSS "CSA"* shall provide the authorised actors (*PSA Decision-makers*) with a mechanism to approve or reject the electronic case files requiring approval, which were preduced by authorised Users (*CSO Head)*.
FR 15.02.	M	The process of approval or rejection shall include producing a note, selecting the status (*Approved* or *Rejected*), its confirmation and applying the electronic signature of the User assigned with the role of file approval/rejection (*PSA Decision-maker*).
FR 15.03.	M	*The ITSS "CSA"* shall implement *MSign* to affix the electronic signature upon the approval/rejection of the electronic form.
FR 15.04.	M	When the electronic file has been approved, the *ITSS "CSA"* shall notify all relevant Users.
FR 15.05.	M	When the electronic case file was rejected, the workflow shall return to the previous stage (shall return the file to the User who sent it for a new preparation) and shall notify all relevant Users.
FR 15.06.	M	At the time when a form is sent for approval it can be amended only by the Decision-maker who shall approve it by applying repeatedly the electronic signature.
FR 15.07.	M	*The ITSS "CSA"* shall log all the events on the approval/rejection of electronic forms.
FR 15.08.	M	*The ITSS "CSA"* shall provide the authorised actors (assigned *with decision-making role*) with a differentiated mechanism to check the quality of data recorded by external *Users* to ensure the accuracy of stored data. The

Identifier	Binding level	Description of Functional Requirements
		quality checking process will be randomised. When detecting errors in the recorded data, the share of registered case files would increase and vice versa.

6.17. UC16: Generate Statistics and System Reports

The functional requirements of the report retrieval component with the aim to audit the *ITSS "CSA"* are displayed in Table 6.16.

Table 6.16. Functional Requirements for Use Case UC16

Identifier	Binding level	Description of Functional Requirements
FR 16.01.	M	*The ITSS "CSA"* shall be able to provide a number of management, statistical and ad-hoc reports so that the Users assigned with administrative roles can monitor the System operation and status.
FR 16.02.	M	The reports managed via *UC16* are intended for auditing purposes and do not include any reports related to business activities on civil status event registration and business events associated with it.
FR 16.03.	M	Such reporting is required for the entire system, including: • Nomenclatures and classifiers; • DB records; • User activity; • Access authorisations and security.
FR 16.04.	M	The reports shall be generated on the basis of the following logged events: • Successful authentication of Users; • Unsuccessful authentication of Users; • Notifications sent; • Actions on data (accessing, supplementing, amending, deleting).
FR 16.05.	M	The System shall allow for aggregated retrieval of reports or their breakdown per each specified User, Civil Status Body or institution (administration) assigned with the function to register civil status events or per certain groups of Users.
FR 16.06.	M	A User who views a report within the system shall be able to export it to an external editable file (PDF, XLS, CSV, and DOC).
FR 16.07.	M	The Developer shall implement up to 10 predefined audit reports requested by the *PSA*. For the audit reports that can be generated via the system means there is no need to implement in the *ITSS "CSA"* User interface.
FR 16.08.	D	To retrieve system reports and statistics relevant for *UC16* it is appropriate to use a platform dedicated to report configuration and generation.

6.18. UC17: Manage Users, Roles, Rights

The functional requirements of User administration component and configuring the access to the *ITSS "CSA"* User Interface and DB content are displayed in Table 6.17.

Table 6.17. Functional Requirements for Use Case UC17

Identifier	Binding level	Description of Functional Requirements
FR 17.01.	M	*The ITSS "CSA"* shall have a mechanism for retrieving the Users, their roles and rights from the *IRAMS*.
FR 17.02.	M	The access rights shall be managed via *IRAMS AIS Administrator*. Ranges of roles to be assigned to different User groups will be created on the basis of the list of access roles.
FR 17.03.	M	The connection, disconnection, reconnection, the change of rights shall be carried out via the *IRAMS AIS Administrator only*. *The ITSS "CSA"* shall retrieve the data about the rights of authenticated Users' access from the IRAMS.
FR 17.04.	M	*The ITSS "CSA"* shall store the Users' data retrieved from the IRAMS in the authorised User profile, and synchronise them upon each User authentication.
FR 17.05.	M	Under the Users' profiles the following categories of data would be managed: • User Last Name; • User First Name; • contact Email address; • contact phone number; • access login; • access Password; • authentication strategy (User+Password, electronic/mobile signature, authentication in two steps (2FA), LDAP, etc.); • active/deactivated account; • access term; • User's roles; • the Users replaced temporarily; • the replacing Users; • other relevant data.
FR 17.06.	M	An authorised User profile can be physically deleted only when it contains no logged events produced or data keyed in by that User.
FR 17.07.	M	*The ITSS "CSA"* shall display User interface and information content only on the basis of rights and roles held by the Users.
FR 17.08.	M	*The ITSS "CSA"* shall deliver a mechanism to register User interface components (resources) with the aim to provide a tool to define the Users' access rights to User interface. By component it is meant any modular entity of the application (form, menu, menu option, field, etc.), which detail level is sufficient to configure the access rights, workflow transitions and actions accessible to Users.
FR 17.09.	M	*The ITSS "CSA"* shall allow configuring the hierarchy of User interface components, the application basic models being at the root level, while the subordinated levels are not limited in their depth, the hierarchy being determined by their architecture.
FR 17.10.	M	Any component of ITSS "CSA" User interface shall contain data on its generic name, brief description, actions available to Users roles (business

Identifier	Binding level	Description of Functional Requirements
		events they can generate) that have access to User interface or action component.
FR 17.11.	M	Any component of ITSS "CSA" User interface shall contain data on statuses the data managed via the component can go through, the route transitions of component statuses (workflow configuration).
FR 17.12.	M	*The ITSS "CSA"* shall allow defining the authorisations related to actions (business events) available to Users with access to User interface components. The following action categories available to Users will be configured: • view records; • supplement records; • amend records; • delete records; • other relevant actions.

6.19. UC18: Manage Flows, Forms and Templates

The functional requirements of the component configuring workflows, electronic forms intended for inserting the data and document templates to be populated with data and generated by the ITSS "CSA" are displayed in Table 6.18.

Table 6.18. Functional Requirements for Use Case UC18

Identifier	Binding level	Description of Functional Requirements
FR 18.01.	M	*The ITSS "CSA"* shall have a mechanism to manage the programme resources (modules, electronic forms, menu options, buttons, etc.) for configuring the workflows and defining the rules for their processing for all scenarios related to electronic form preparation and processing associated with the registration of civil status events.
FR 18.02.	M	The workflow management should be carried out using the System graphical interface where the User usually works.
FR 18.03.	M	The workflows shall be defined by specifying the statuses an electronic form may go through and the processing steps (stages or workflow development stages carried out by Users assigned with specific roles).
FR 18.04.	M	A workflow shall be implemented as a set of activities through which a prepared electronic form goes through within the business processes carried out in a sequence.
FR 18.05.	M	The number of steps to be included in a flow shall not be limited. In this way the IT solution could be adaptable to the changes of work methodology with documents processed under the management procedure associated with the registration of civil status events.
FR 18.06.	M	A workflow should have associated a Coordinator (Supervisor). The Coordinator shall be able to receive warning messages (notifications) generated when rolling the corresponding flow. The User who launches a form for processing through a workflow shall be able to specify who the flow Supervisor is.

Identifier	Binding level	Description of Functional Requirements
FR 18.07.	M	The Developer shall configure the electronic form processing flows intended to prepare all business events related to the registration of persons' civil status events.
FR 18.08.	M	*The ITSS "CSA"* shall provide a mechanism to configure the electronic forms necessary for preparing the documents related to the registration of civil status events (statuses and transitions thereof).
FR 18.09.	M	*The ITSS "CSA"* shall provide mechanisms to configure document (and report) templates related to the documents generated on the basis of prepared electronic forms (the templates shall have a well-defined structure allowing to modify the appearance and content of the retrieved document).
FR 18.10.	M	The Developer shall configure and implement electronic forms and templates to generate the entirety of documents specific for the registration of civil status events, specified in Chapter *5.1. Information Objects.*
FR 18.11.	M	The Developer shall configure within the application up to 20 document templates to be generated by the ITSS "CSA".

6.20. UC19: Manage metadata

The functional requirements necessary for managing the *ITSS "CSA"* metadata are displayed in Table 6.19.

Table 6.19. Functional Requirements for Use Case UC19

Identifier	Binding level	Description of Functional Requirements
FR 19.01.	M	*The ITSS "CSA"* shall have a mechanism to manage nomenclatures, classifiers comprising the metadata intended for configuring the System and managing the civil status event registration process.
FR 19.02.	M	The classifiers managed by the *PSA* will be taken over in full, as well as other official classifiers of the Republic of Moldova, as appropriate.
FR 19.03.	M	The rights to make changes in the PSA internal classifiers implemented in the SRP and in the official ones shall be limited.
FR 19.04.	M	For the system of nomenclatures and internal metadata, the IT solution shall deliver a mechanism for their dynamic definition and administration (it should offer the possibility to dynamically add categories of nomenclatures/classifiers and their content).
FR 19.05.	M	*The ITSS "CSA"* shall not allow deleting any category of metadata if they are used at least in on DB entry.
FR 19.06.	M	*The ITSS "CSA"* shall provide a mechanism for versioning the metadata values and setting the time period afferent to the validity of metadata values.
FR 19.07.	M	The Developer shall configure the automatic update of classifiers through the retrieval of the list of available classifiers managed by the PSA, checking the latest updates, retrieving the data of the updated classifier and synchronising the values in the *ITSS "CSA"* as per the functional requirements *FR 23.09*.

Identifier	Binding level	Description of Functional Requirements
FR 19.08.	M	*The ITSS "CSA"* shall allow configuring linear and hierarchical classifiers (where some values may have parent values).
FR 19.09.	M	*The ITSS "CSA"* shall provide a mechanism to export and import the classifiers from User Interface in XML and CSV format. The rights to import and export shall be assigned to Users with the role of *System Administrator*.
FR 19.10.	M	*The ITSS "CSA"* shall deliver a mechanism to configure from the User Interface with the role of *System Administrator* a list of mandatory documents, terms and costs related to them, facilities, additional services depending on the type of CSA and the registration flow peculiarity. After having selected the type of CSA and the deadline, the *ITSS "CSA"* shall determine automatically the cost (if any, or calculated as per the granted facilities) and additional services suggested for ticking-off.

6.21. UC20: Other Administration Activities

The functional requirements for *ITSS "CSA"* administration activities are displayed in Table 6.20.

Table 6.20. Functional Requirements for Use Case UC20

Identifier	Binding level	Description of Functional Requirements
FR 20.01.	M	*The ITSS "CSA"* shall allow the administrative roles to take over, display and reconfigure the System operation parameters and settings.
FR 20.02.	M	*The ITSS "CSA"* shall allow the Users with *System Administrator* role to configure the access to WEB services provided by external IT Systems the *ITSS "CSA"* interacts with.
FR 20.03.	M	*The System Administrator* shall have a specialised interface to access and review the *ITSS "CSA"* system logging events.
FR 20.04.	M	*The ITSS "CSA"* shall deliver an interface intended for monitoring the current operation.
FR 20.05.	M	*The System Administrator* shall be able to generate *ITSS "CSA"* back-ups *and* restore the System functionality on their basis.
FR 20.06.	M	*The ITSS "CSA"* shall provide *the System Administrator with the* functionalities necessary to ensure the IT solution smooth operation.
FR 20.07.	M	*The System Administrator* shall have the functionality to configure the share of verification and the rating mechanism for each LPA/DM/CO institution separately, depending on the share of identified errors.

6.22. UC21: Logging Events

The functional requirements of the component for logging business events produced during the *ITSS "CSA"* operation are displayed in Table 6.21.

Table 6.21. Functional Requirements for Use Case UC21

Identifier	Binding level	Description of Functional Requirements
FR 21.01.	M	The IT System shall contain a mechanism for logging all business events related to the System use.
FR 21.02.	M	*The System Administrator* shall be able to configure all strategies for logging the business events via Use Case *UC21*
FR 21.03.	M	*The ITSS "CSA"* shall have a mechanism to filter and search the logged events.
FR 21.04.	M	The following categories of events shall be logged: • User authentication; • User logout; • Adding/modifying/deleting/accessing a record; • Business events specific for the *ITSS "CSA"* ; • Generate/access reports; • DB query; • Other specific business events.
FR 21.05.	M	The logged events shall save the following categories of data (depending on the nature of the logged event): • identifier of the User who generated the event; • category of the logged event; • the time of event logging; • *the ITSS "CSA"* module that generated the business events; • the record affected by the business events; • the action undertaken by the User.
FR 21.06.	M	*The ITSS "CSA"* shall log exhaustively all business events that have occurred.
FR 21.07.	M	*The ITSS "CSA"* shall log each access via MConnect, using the Government logging service *MLog*.

6.23. UC22: Send Notifications

The functional requirements for the component notifying the *ITSS "CSA"* Users are displayed in Table 6.22.

Table 6.22. Functional Requirements for Use Case UC22

Identifier	Binding level	Description of Functional Requirements
FR 22.01.	M	Depending on the User (data for configuring his/her profile), the WEB notification service shall apply one out of three notification strategies: • notification via Email; • notification on the Dashboard of authorised Users via intra-system messages; • both categories mentioned above.
FR 22.02.	M	Depending on the *ITSS "CSA"* configuration resources, the WEB notification service shall send a notification to relevant Users when a transition occurs within the IT application.
FR 22.03.	M	The notification shall contain reference for accessing the relevant resource/form, which business event generated the notification (valid for the notifications stored in the User's Dashboard).

Identifier	Binding level	Description of Functional Requirements
FR 22.04.	M	The authenticated Users (regardless of the roles held) shall be able to configure their preferences in terms of notification means.
FR 22.05.	M	The authorised Users shall receive notifications on business events related to their job duties (the need to approve the form, changes in personal records, etc.).
FR 22.06.	M	*The System Administrator* shall have the functionality to prepare forms and send notifications to a group of people.
FR 22.07.	M	The actors involved in the business processes related to the registration of civil status events shall be able to receive notifications at their Email address in case of business events prepared via *UC04* or in case of notifications prepared by the *System Administrator*.
FR 22.08.	D	*The ITSS "CSA"* shall notify *the System Administrator* on any issues affecting the IT System performance and availability.
FR 22.09.	D	*The ITSS "CSA"* shall notify the Users via the Government notification service *MNotify*.

6.24. UC23: Synchronise Data

The functional requirements for data synchronisation procedures processed by the ITSS "CSA" *with* external IT System DBs are displayed in Table 6.23.

Table 6.23. Functional Requirements for Use Case UC23

Identifier	Binding level	Description of Functional Requirements
FR 23.01.	M	*The ITSS "CSA"* shall use data from external systems of CPAs and state institutions of the Republic of Moldova via COI (Common Object Interface) and via Government Interoperability Platform *MConnect*.
FR 23.02.	M	*The ITSS "CSA"* shall carry out synchronisation actions with the *State Register of Population aimed at* receiving data about people in the process of identification and registration of civil status events.
FR 23.03.	M	*The ITSS "CSA"* shall derive data on civil status acts from the functional contour *"CIVIL STATUS ACTS" of the SRP* with the aim to register civil status facts. The data used from the functional contour *"CIVIL STATUS ACTS" of the SRP* shall be stored by the *ITSS "CSA"*.
FR 23.04.	M	*The ITSS "CSA"* shall complete, update or make a record on cancelling the civil status documents stored in the functional contour *"CIVIL STATUS ACTS" of the SRP*.
FR 23.05.	M	*The ITSS "CSA"* shall respond to the electronic request submitted by the CNAS IS on the new registrations of birth to initiate subsequently the process of granting a childbirth allowances or on the new registrations of death of retired people.
FR 23.06.	M	*The ITSS "CSA"* shall receive courts judgements with relevance to civil status events conveyed by the Integrated File Management Programme (IFMP) and initiate automatically the relevant processes (for example, initiating the registration process of Divorce Certificate based on the Court judgement on dissolution of marriage). The following documents shall be

Identifier	Binding level	Description of Functional Requirements
		received from the IFMP, initiating automatically a case file to register the CSA: • judgment on the dissolution of marriage; • judgment confirming the fact of birth/death; • judgment confirming the registration of birth/death; • judgment on depriving of parental rights; • judgment on enforceability of adoption; • notary decision on citizens' divorce.
FR 23.07.	M	For certain documents and data received, the *ITSS "CSA"* shall be able to perform certain automatic actions, such as: • Initiating the process of divorce registration following the receipt of the Court Judgement on the dissolution of marriage; • Initiating the process of birth registration following the receipt of the birth confirming medical certificate; • Initiating the process of civil status document issuance following the receipt of an application; • other relevant actions.
FR 23.08.	M	All synchronisation events and, especially, those of accessing personal data via the procedures described by functional requirements *FR 23.02 - FR 23.07* shall be logged via *MLog*.
FR 23.09.	M	*The ITSS "CSA"* shall synchronise automatically, via *IRAMS,* the configured classifiers with the classifiers implemented in the SRP.

7. Non-functional requirements of the IT System

This Part of the Terms of Reference shall set the requirements towards non-functional characteristics the *CSA ITSS* shall have. The IT solution, which is the subject-matter of this procurement, shall match the non-functional requirements set as it is described below.

7.1. Agreements on drawing up Non-functional Requirements

The non-functional requirements set in this document are marked using the following agreement:

- all requirements are indexed with two values: **X** and **Y**, where **X** represents the category of requirements described in Table 7.1; and **Y** is the single identifier of requirements in the categories it is part of;
- for each requirement the binding level is shown: **M** – mandatory requirement to be implemented, **D** – desirable/optional requirement to be implemented, and **I** – informative requirement.

Table 7.1. Categories of requirements comprised by the Scope of Work

Value	Meaning	Interpretation
LIPR	Requirements for licensing and intellectual property	The requirements refer to the rights of intellectual property related to *the ITSS "CSA"* and software components necessary for the ITSS "CSA" operation.
ARH	Architecture requirements	The requirements refer to architecture matters for conceptualizing the *ITSS "CSA".*
DEL	Requirements regarding the deliverables	The requirements refer to deliverables to be submitted by the *ITSS "CSA" Developer.*
FLEX	Flexibility requirements	The requirements refer to the flexibility of adjusting the *ITSS "CSA"* to new needs.
GMS	Requirements regarding the defect liability period, maintenance and post-implementation support	The requirements refer to the features of operational maintenance and post-implementation development services for the *ITSS "CSA"* required under this Procurement.
INT	Interoperability requirements	The requirements refer to the interoperability framework of the *ITSS "CSA".*
SLA	Requirements regarding the level of services offered	The requirements refer to quality parameters set for defect liability period, maintenance and post-implementation support services.
MG	Project management requirements	The requirements refer to the Project Management issues during the *ITSS "CSA"* design, development, implementation, commissioning and operation.
PERF	Performance requirements	The requirements refer to the *ITSS "CSA"* operation performance.
RC	Resilience and continuity Requirements	The requirements refer to *the ITSS "CSA"* capacity to respond to critical events and quick restoration of its functionalities.
SEC	Security requirements	The requirements refer to information security aspects the *ITSS "CSA"* shall comply with.
SR	Scalability requirements	The requirements refer to scalability properties of the *ITSS "CSA"* when the number of Users increases, as well as the number of transactions or the volume of data processed.

Value	Meaning	Interpretation
MR	Maintenance requirements	The requirements refer to maintenance matters of *ITSS "CSA"* post-delivery.
PR	Platform requirements	The requirements refer to the technological platform required for the *ITSS "CSA".*
UI	User Interface requirements	The requirements refer to User Interface the *ITSS "CSA"* shall deliver *to* Authorised Users.
ISR	Implementation services requirements	The requirements refer to services rendered during the *ITSS "CSA"* implementation and commissioning.
PIR	Post-implementation requirements	The requirements refer to defect liability period and *ITSS "CSA"* post-implementation maintenance services.

The bid submitted by the Bidder shall meet all the binding requirements.

The bid submitted by the Bidder shall get competitive advantage for each desirable/optional requirement assumed.

The informative requirements are intended to offer more data to ensure better understanding of the context of other requirements.

7.2. Requirements on Licensing and Intellectual Property

The PSA shall have all the rights necessary for using the ITSS "CSA" without a time limit, as all as all software components necessary for *ITSS "CSA"* smooth operation.

Table 7.2. contains detailed requirements related to licensing and the rights of intellectual property related to *the ITSS "CSA"* and software components necessary for the System smooth operation.

Table 7.2. The licensing requirements and those related to intellectual property

ID	Binding level	Requirement
LIPR 001	I	*The PSA* shall ensure the following operation environment for the *ITSS "CSA"*: • production environment; • testing environment.
LIPR 002	M	The Bidder shall include in its bid licences for all software products type COTS necessary to implement and operate the *ITSS "CSA"* in those three environments made available by the *PSA*. Here the following are displayed: operating systems, DBMSs, software, utility libraries, and other system software.
LIPR 003	M	The quantity of licenses offered shall allow accessing and using the *ITSS "CSA"* (in any environments it is operated) by at least 1500 nominal Users, and unlimited by external systems. No restriction shall be imposed on the number of documents, transactions or the way of accessing the *ITSS "CSA"* (example: *limitations upon concurrent access*).
LIPR 004	M	The quantity of licenses provided shall allow accessing the APIs exposed by the ITSS "CSA" by any application and external system.
LIPR 005	M	The Bidder shall convey to the *PSA* all the rights over the developments, adjustments, configurations and customisations carried out to implement *the ITSS "CSA"* as per the requirements. Those can be related to third licensed software products or can be components developed under the Project.

ID	Binding level	Requirement
LIPR 006	M	Any data stored under the DBs related to the *ITSS "CSA"* shall be the PSA property. Access to those data throughout the whole contracting period of the Supplier/Provider and beyond it shall be subject of requirements and of information confidentiality clauses.
LIPR 007	M	The Bidder shall submit its proposed licensing model for the *ITSS "CSA"* that must meet the requirements LIPR 001 – LIPR 006. The Bidder shall describe the proposed licensing model, arguing why it is the optimal one for the *PSA*. The Bidder shall submit a comparative analysis with other licensing models offered, as a rule, for the proposed solution.

7.3. Requirements for System Architecture

The ITSS "CSA" Architecture shall be aligned with the *PSA* needs in terms IT System flexibility and maintenance. *The Public Services Agency* opts for an open, modular Architecture based on interoperable components. These principles shall be visible at all levels of *ITSS "CSA"* Architecture.

7.3.1. General requirements of the *ITSS "CSA"* Architecture

Table 7.3. contains detailed general non-functional requirements set for the *ITSS "CSA"* Architecture.

Table 7.3. General requirements set for the *ITSS "CSA" Architecture*

ID	Binding level	Requirement
ARH 001	M	The ITSS "CSA" Architecture shall be based on open standards.
ARH 002	M	The ITSS "CSA" Architecture shall be service oriented (SOA).
ARH 003	M	The ITSS "CSA" Architecture shall have an integrated design developed with the use of filed-related best practices (example*: Architecture principles and aligned reference architectures TOGAF 9.1*).
ARH 004	M	The ITSS "CSA" Architecture shall be client-server type, organised in three vertical levels at least, clearly divided so that each superior level depends on its inferior level only.
ARH 005	M	The ITSS "CSA" Architecture shall be adapted during the System implementation and operation within the virtualised environments.
ARH 006	M	The IT System features with the Architecture focused on implementation in virtualised environments are as follows: aware of latency, aware of component failures, parallelisable, aware of resource use.
ARH 007	M	Communication among all System components is carried out in a secured way, using to this end internal interfaces of System components.

7.3.2. Requirements for the *ITSS "CSA"* Architecture Presentation Level/Layer

The Architecture Presentation Level is responsible for ensuring the User interaction with the *ITSS "CSA"* business functions. This Architecture level manages the way how the Users access and use the IT System functions both with the aim to exercise their job duties and for administrative purposes.

The ITSS "CSA" is to be accessed by the employees of healthcare facilities, mayoralties, Diplomatic Missions and Consular Offices, *PSA* GCSD and its territorial offices (Civil Status Bodies). In addition, the *ITSS "CSA"* shall communicate with other *PSA* systems or with third parties systems via external applied interfaces (specifications

related to *the ITSS "CSA" interoperability*) with the aim to use data. The external systems that need civil status data shall access the SRP (via COI or MConnect, following the approval of the corresponding legal framework).

Table 7.4. comprises detailed non-functional requirements set for the *ITSS "CSA"* architecture presentation level.

Table 7.4. The ITSS "CSA" Architecture Presentation Level

ID	Binding level	Requirement
ARH 008	M	*The ITSS "CSA"* shall allow a User to make use of one client application to access all business functions for which he/she has been authorised. Exceptions shall be granted for roles with privileged rights.
ARH 009	M	There should be possible to roll the client application in standard operating environments or with minimum configurations to be carried out by the Beneficiary (example*: system standard software only*).
ARH 010	M	The WEB browser shall be the default client application for the *ITSS "CSA".*
ARH 011	M	The ITSS "CSA" shall be compatible with at least two of the widely used WEB browsers (Microsoft Internet Explorer/Microsoft Edge, Mozilla FireFox, Google Chrome, Opera and Safari).
ARH 012	M	The presentation level shall not implement business rules, except for the validation of data inputs.

7.3.3. Requirements for the level of business logics of the ITSS "CSA" Architecture

The level of business logics of the ITSS "CSA" Architecture shall implement basic functionalities of the IT System. The level of business logics comprises the one required to exercise the *PSA* duties via *the ITSS "CSA".* The business logics shall be responsible for accessing, processing and transforming the data from the application, for managing the business rules, having ensured the data consistency and accuracy.

The level of business logics is accessed by the presentation level to make the IT System business functions available to Users. Likewise, it can make available those functions to external IT applications via specialised interfaces, which, likewise, are component parts of the level of business logics.

SOA-type Architecture implies a high level of granularity of component blocks for business logics. Each logical block provides its functions via internal or/and external interfaces. Those can be accessed by other components of business logics, components of the presentation level or external systems.

Table 7.5. comprises specifications for non-functional requirements set for the level of business logics of the ITSS "CSA" Architecture.

Table 7.5. The requirements set for the level of business logics of the ITSS "CSA" Architecture

ID	Binding level	Requirement
ARH 014	M	The level of business logics shall be fully independent relative to the presentation level and the applications accessing the level of business logics directly (via specialised applied interfaces).
ARH 015	D	The level of business logics shall have an absolutely modular Architecture based on reusable components and interface abstracts. It is not required to have identical functionalities held by different components at this level (example*: data access*).
ARH 016	D	The level of business logics must contain and have bounded "*business workflow*" and "*business entity*" type components.

ID	Binding level	Requirement
ARH 017	D	The components of "*business entity*" shall be accessed via the components of "*business workflow*".
ARH 018	M	Business entities shall be clearly identified at the level of business logics and encapsulated in components of "*business entities*".
ARH 019	M	The components of "*business entity*" shall be service-minded and contain all data and business logics afferent to the business entity, necessary for carrying out business operations, applying the relevant business rules and for maintaining the integrity and accuracy of data held.
ARH 020	M	The components related to the level of business logics shall communicate amongst them via dedicated internal interfaces/functions (*tight coupling*).
ARH 021	M	The components related to the level of business logics shall be accessible for external applications via external applied interfaces only defined to this end.
ARH 022	M	The Architecture of the level of business logics shall allow for concurrent access to *ITSS "CSA"* objects and functions.

7.3.4. Requirements for data level of the ITSS "CSA" Architecture

The ITSS "CSA" data are stored and accessed at this Architecture level. The data are accessible via DBMS. The data integrity rules are defined at the DBMS level. The data level shall ensure that the latter would be made available to authorised entities only and that data integrity and veracity would be provided.

The data level shall ensure the data necessary *for the ITSS "CSA"* to deliver the functionalities and business services requested by the PSA. The requirements for the data level of the ITSS "CSA" Architecture are displayed in Table 7.6.

Table 7.6. The requirements for the data level of the ITSS "CSA" Architecture

ID	Binding level	Requirement
ARH 023	M	The data model implemented and supported by the ITSS "CSA" shall correspond to the description referred to in Point *5.1 Information Objects of the ITSS "CSA".*
ARH 024	M	*The ITSS "CSA"* shall support an integrated data model for the reference information.
ARH 025	M	The designed data model shall ensure the possibility to migrate the data from the IT Systems currently operated by the *PSA*.
ARH 026	M	The ITSS "CSA" data shall be made available via the components contained by the level of business logics only.
ARH 027	M	The data stored under the *ITSS "CSA"* shall be neutral and independent relative to the level of business logics.
ARH 028	M	The data Architecture shall be optimised to allow for quick access to data to carry out transactions and generate statistics and analysis reports. The generation of analysis reports shall not affect the performance of transactional operations of the IT System.
ARH 029	M	The data model implemented shall be documented in details. The documentation must contain both the technical description of the data level (example: *XSD*) and the semantic description (*association of data structure at the business entity and properties thereof*). The semantic description of data

ID	Binding level	Requirement
		shall be available to Users within the System, as appropriate (example*: configuring reports*).
ARH 030	M	Each registration of the information object shall have a single identification number at the system level. The algorithm for assigning the single identification number shall be configurable within the System and shall allow for identifying the corrupted records.
ARH 031	M	The System Architecture shall ensure data integrity and correctness upon their simultaneous accessing and changing by several entities (Users, internal processes, external applications).

7.3.5. Requirements for the technological level of the ITSS "CSA" Architecture

The software and hardware components necessary to roll the *ITSS "CSA"* are placed at this Architecture level. The former are part of higher levels (the level of data, the level of business logics and the level of presentation).

The Architecture technological level shall ensure availability and accessibility of System components. The requirements set for the technological level of the ITSS "CSA" Architecture are displayed in Table 7.7.

Table 7.7. The requirements set for the technological level of the ITSS "CSA" Architecture

ID	Binding level	Requirement
ARH 032	M	The System Technological Architecture shall have a pretty high level of resilience to failures and contain no SPOF.
ARH 033	M	The Technological Architecture shall ensure the rational and balanced use of resources for processing.

7.4. Requirements for the Technological Platform

The Technological Platform consists of software and hardware components necessary to ensure the operating environment where the *ITSS "CSA"* is to be used. The Technological Platform shall include: development platforms and programming languages the IT System Code has been developed in, DBMSs, operating systems on which basis System components can be rolled, programme specific provision necessary to be installed for accurate rolling of the IT System, hardware platform on which the System components are rolled, etc.

To have a scalable, flexible and easy maintainable system, there should be a minimum level of dependence of the System relative to the Technological Platform on which its components are being rolled.

7.4.1. General requirements relative to the Technological Platform of the *ITSS "CSA"*

Table 7.8. comprises general non-functional requirements set for the Technological Platform of the *ITSS "CSA".*

Table 7.8. The general requirements set for the Technological Platform of the *ITSS "CSA"*

ID	Binding level	Requirement
PR 001	M	The Platform Technologies included in the *ITSS "CSA"* Architecture shall be technologies widely known and implemented in the Republic of Moldova. It is required that at least three other Providers render maintenance and solution development services on the respective platforms on the local market.

ID	Binding level	Requirement
PR 002	M	The ITSS "CSA" components shall be independent relative to the technological platform they are rolled (except for the cases when such requirements result explicitly from the current Terms of Reference).
PR 003	M	The System Architecture shall be optimised for rolling in such environments as *Cloud Computing*. The features of a system with the Architecture focused on implementing Cloud Solutions are as follows: aware of latency, aware of component failures, parallelisable, aware of resource use.
PR 004	M	The technologies available at the Technological Platform level shall be homogenous (minimum number of different technologies; *example: the same operating systems for middleware and database*).
PR 005	M	*The ITSS "CSA"* shall support setting, amending, processing, storing and accessing the text in Unicode format.
PR 006	M	The Bidder shall indicate in its bid full and extensive information on technological platforms supported by its application and the relevant constraints.

7.4.2. Requirements for the presentation level of the *ITSS "CSA"* Technological Platform

This Part comprises the requirements related to *ITSS "CSA"* presentation level technologies. Table 7.9 displays all specific requirements set for the presentation level of the *ITSS "CSA"* Technological Platform.

Table 7.9. The requirements for the presentation level of the *ITSS "CSA"* Technological Platform

ID	Binding level	Requirement
PR 007	M	*The ITSS "CSA"* shall be accessible for any authorised ITSS "CSA" User connected to the *PSA* corporate network, using standard computers available at the work place (desktop computers, notebooks, tablets, printers, etc.).
PR 008	M	There should be the possibility to print out all the visualisations and reports generated by the ITSS "CSA" on the stated page format. *The ITSS "CSA"* shall dimension automatically the output documents to frame them into the format stated by the User (example*: A2/A3/A4/A5, portrait/landscape, etc.*). There should be one or more options for the output document types (example*: PDF, XML, XLS, DOC etc*).

7.4.3. Requirements for the level of business logics of the ITSS "CSA" Technological Platform

This Part comprises the requirements related to technologies present at the *ITSS "CSA"* level of business logics. Table 7.10 comprises all requirements specific for the level of business logics of the *ITSS "CSA"* Technological Platform.

Table 7.10. The requirements for the level of business logics of the *ITSS "CSA"* Technological Platform

ID	Binding level	Requirement
PR 010	M	The components forming the level of business logics shall be developed in modern programming languages, widely accepted in the industry and, especially, in the ICT sector of the Republic of Moldova (example*: Java, PHP, PSA.NET, C#, etc.*).

ID	Binding level	Requirement
PR 011	M	The technologies present at this level shall allow integrating the components that already have been or will be developed by *the Public Services Agency* through the applied interfaces made available.

7.4.4. Requirements for the level of data of the ITSS "CSA" Technological Platform

This Part comprises the requirements related to technologies present at the level of *ITSS "CSA" data*. Table 7.11 comprises all requirements specific for the level of data of the ITSS "CSA" Technological Platform.

Table 7.11. The requirements for the level of business logics of the ITSS "CSA" Technological Platform

ID	Binding level	Requirement
PR 012	M	The Provider shall ensure a mechanism for storing the data for the *ITSS "CSA".*
PR 013	M	Where appropriate, t*he Bidder* shall identify additional needs to ensure the System lawfulness and performance (additional licences, equipment for data storage, etc.).
PR 014	M	*The ITSS "CSA"* shall be compatible with the DBMSs currently used by the *PSA*.

7.4.5. Requirements for the technological level of the ITSS "CSA" Technological Platform

This Part comprises the requirements related to technologies used by the *ITSS "CSA"* Platform. Table 7.12 comprises the requirements specific for the technologies of the ITSS "CSA" Technological Platform.

Table 7.12. The requirements for the technologies of the ITSS "CSA" Technological Platform

ID	Binding level	Requirement
PR 015	M	All System components (example*: operating system, middleware, DBs*) shall have the possibility to be rolled in virtualised environments on virtualisation platforms Microsoft Hyper-V Server 2012 R2 and newer.
PR 016	M	The Bidder shall include in its bid detailed information on the recommended Technological Platform (within the limits of available alternatives/options), taking into account the PSA needs defined in this Scope of Work. In the case of successful offer, the latter will be taken as basis for setting the Technological Platform afferent to the *"PSA" ITSS*.

7.5. The Interoperability Requirements

The ITSS "CSA" interoperability represents the characteristics of the IT System to communicate with other IT applications. The system Architecture shall define the interfaces to be in place between the *ITSS "CSA"* and other systems held by *PSA or* by Moldovan Public Authorities. Table 7.13 defines the requirements regarding the interoperability characteristics of the *ITSS "CSA"* required by *the Public Services Agency*.

Table 7.13. The requirements for the *ITSS "CSA"* interoperability framework

ID	Binding level	Requirement
INT 001	M	All the interfaces exposed by the ITSS "CSA" shall be based on open standards. All the message flows between the *ITSS "CSA"* and external entities shall be carried out by using open standards.
INT 002	M	*The ITSS "CSA"* shall have the capacities to implement interfaces via MConnect.
INT 003	M	Upon implementation, the ITSS "CSA" shall be integrated with the following internal systems: • State Register of Population (shall deliver and use data). • SAIS (the Digitised Archive Subsystem). Currently *SAIS* has no functional API developed for accessing the data. To use *SAIS* data it would be required to develop initially those Web services or queries in the *SAIS database*, which would enable accessing the data. *SAIS* will serve only as a static source of archive data without being updated with new data; • *IRAMS* (Information Resource Access Management System)
INT 004	D	Upon implementation, the *ITSS "CSA"* shall be integrated with the following external systems: • MPass; • MSign; • MNotify; • MLog; • PSP; • IFMP.
INT 005	M	All the interfaces provided by the *ITSS "CSA"* will interact with external applications either instantaneously or scheduled through specialised jobs.
INT 006	M	The "PSA" ITSS shall have the capacities to define new standard interfaces for accessing all key business functions of the System (example: generate documents, generate transactions, access information about business entities stored within the ITSS "CSA"). The respective interfaces shall allow managing the business entities, applying all relevant business rules and using all properties related to business entities.
INT 007	M	*The "PSA" ITSS* shall have the capacities to define new interfaces for accessing external systems, using open standards. These interfaces shall be available for use within the System functions upon implementing the ITSS "CSA" functionalities.
INT 008	D	*The "PSA" ITSS* shall have standard interfaces for exporting the data to such tools as *Data Warehouse*.
INT 009	M	All System interfaces shall be properly documented (example*: using the Web Services Description Language Model*).
INT 010	D	*The ITSS "CSA"* shall have specific capacities similar to *ESB solutions*. These capacities could be used for *ITSS "CSA"* integration with external systems, as well as for its interoperability with external systems without involving the *ITSS "CSA"* in the information exchange flows.
INT 011	M	The ITSS "CSA" interoperability capacity shall be aligned with the identification and metadata system defined by the standards specific for CSAs.

The ITSS "CSA" shall take into account the aspects related to IT technologies used and the industry initiatives in force on the territory of the Republic of Moldova. The relevant requirements to this end are specified in Table 7.14.

Table 7.14. The requirements regarding the aspects related to ICT and initiatives thereof

ID	Binding level	Requirement
INT 012	M	*The ITSS "CSA"* shall integrate with Government Interoperability Platform *MConnect* to use data from external IT Systems (example*: retrieving data from other state registers*).
INT 013	M	*The ITSS "CSA"* shall use *MPass* platform service as a mechanism for User authentication via electronic signature or mobile identities.
INT 014	M	*The ITSS "CSA"* shall use *MSign* platform service as an infrastructure for using the electronic signature.
INT 015	M	*The ITSS "CSA"* shall use *MLog* platform service as a mechanism to log critical business events.
INT 016	M	*The ITSS "CSA"* shall use *MNotify* platform service as a mechanism to notify the Users.
INT 017	M	*The ITSS "CSA"* shall integrate with the Public Services Portal (https://servicii.gov.md) with the aim to interact with citizens (take over the orders of civil status documents, etc.).

7.6. Performance Requirements

The ITSS "CSA" shall have the capacity to timely process the transactions carried out by the ITSS Users as per the workload resulting from the activity of the PSA GCSD and its territorial services, Mayoralties, Diplomatic Missions and Consular Offices in the area of civil status events registration. Table 7.15 exposes the performance requirements set for the *ITSS "CSA".*

Table 7.15. Performance requirements for the *ITSS "CSA"*

ID	Binding level	Requirement
PERF 001	M	The response time to a transaction query from an external User/service shall not exceed 3 seconds (it does not relate to the report generation).
PERF 002	M	*The ITSS "CSA"* shall be able to manage up to 250 concurrent sessions (connections of Authorised Users and external systems) with the possible scalability up to 1000 concurrent sessions in the process of subsystem scale-up.
PERF 003	M	The Bidder shall include in the *ITSS "CSA"* administration and operation guidelines the information on processes that may affect/decrease the *ITSS "CSA"* performance and its recommendations on concurrent rolling of those processes (example*: it is not recommended to roll the X process for generating daily reports concurrently with the Y process for generating back-ups*).
PERF 004	M	Reports generation and accessing the information with the aim to carry out business analyses shall not affect the System operating performance at the level of transaction processing. The System documentation shall identify the reports with significant impact on performance and formulate recommendations for the Bidder regarding the generation of the respective reports so that the *ITSS "CSA"* performance indicators are not influenced.
PERF 005	M	The Bidder shall indicate in its bid the minimum guaranteed values for *ITSS "CSA"* performance features with reference to the recommended technological platform.

ID	Binding level	Requirement
PERF 006	M	*The ITSS "CSA"* shall have the capacity to process at least 20 000 transactions a day.

7.7. Flexibility Requirements

The ITSS "CSA" shall have the capacity to be adjusted over time to new needs generated by the PSA activity. It is desirable this to be done by adjustments to system configurations (without amending the programme code), in this way minimising the adjustment costs to be borne by the *PSA*. Table 7.16 comprises flexibility requirements to be met by the *ITSS "CSA".*

Table 7.16. Flexibility requirements set for the ITSS "CSA"

ID	Binding level	Requirement
FLEX 001	M	*The ITSS "CSA"* shall allow configuring the visualisations and forms intended for Users. The IT System shall allow setting new forms for Users to access the *ITSS "CSA"* business logics.
FLEX 002	M	*The ITSS "CSA"* shall allow configuring the existing reports (example: adjusting data sets, reformatting).
FLEX 003	M	The ITSS "CSA" shall allow adding and configuring reports and statistics (example: defining data sets, formatting reports, defining the calculated fields).
FLEX 004	M	*The ITSS "CSA"* shall allow configuring the KPIs and the ways of their graphical presentation on the *Dashboard*.
FLEX 005	M	*The ITSS "CSA"* shall allow configuring the automatic generation of reports. The automatic generation shall be carried out at certain events rolled in the System or at certain time periods. The generated reports will be stored within the System or sent to email addresses or to identified Users.
FLEX 006	M	*The ITSS "CSA"* shall allow defining and configuring business entities stored within the System (example*: defining new properties*) via appropriate adjustment of the *ITSS "CSA" data model*.
FLEX 007	D	*The ITSS "CSA"* shall allow configuring the envisaged roll of system procedures (jobs) depending on time parameters or on certain events rolled within the System. *The ITSS "CSA"* shall allow installing and configuring new system procedures.
FLEX 008	M	The ITSS "CSA" shall allow defining and configuring new business flows and adjusting the existing flows as appropriate (example: operation sequence, transforming the property status of business entities, generated documents and records, notifications, the roles involved and operations allowed, etc.).
FLEX 009	M	*The ITSS "CSA"* shall allow for defining and managing the reference regulatory information used within the System. The data source for reference information could be internal or external (example*: external DB, external WEB service, external file, etc.*).
FLEX 010	M	The ITSS "CSA" potentially variable information (*example: different parameters, constants, ways of data storage, ways of connection with external services, classifiers, etc.*) shall be configurable and require NO repeated compilation of the solution or direct interventions in the database.

		There should be the possibility to carry out the changes concerned in User Interface convenient for Administrators.
FLEX 011	D	*The ITSS "CSA"* shall allow for integrating the components developed by the *PSA under* other IT application development projects. These components shall have access to public functions and properties of System components.
FLEX 012	M	*The ITSS "CSA"* shall allow for defining the statuses an information object or an electronic form may have. The access rights shall allow for defining the operations permitted to the User, depending on statuses admitted for the information object (the IT System shall have a mechanism to detect the conflicts when statuses for which the rights were set have been changed).

7.8. The Requirements for User Interface and Ergonomics

The IT System interface shall be User-friendly, easy and intuitive. The time required for training with the aim to use the *ITSS "CSA"* shall be minimal. Users shall have access to support information any time to foster accurate use of facilities provided by the *ITSS "CSA".* Table 7.17 comprises the requirements regarding the fitness characteristics t*he ITSS "CSA"* shall meet.

Table 7.17. The requirements set for *ITSS "CSA"* User Interface

ID	Binding level	Requirement
UI 001	M	All the business functions accessible to *ITSS "CSA"* Users shall be made available through graphical User Interfaces.
UI 002	M	*The ITSS "CSA"* shall have User-friendly, intuitive and suitable interfaces for Users assigned with non-administrator and administrator roles. The information necessary to Users with the aim to carry out job duties shall be visible and accessible. The ITSS "CSA" User Interface shall have unique styles of graphical design. The graphical elements and texts shall be used consistently from the standpoint of significance associated thereto.
UI 003	M	All User interfaces shall be developed at least in Romanian.
UI 004	M	The User Interface elements shall comply with Level A *0* requirements of *Web Content Accessibility Guidelines (WCAG) 2*.
UI 005	M	The User Interface shall be optimised for desktop PCs or notebooks with the resolution of 1360x768.
UI 006	M	For the most important functionalities, the *ITSS "CSA"* shall have the possibility to adjust the User Interface (shall deliver responsive interfaces) depending on the device used (notebook, desktop PC, tablet, smartphone).
UI 007	M	*The ITSS "CSA"* shall allow intermediate saving of the work done and of operations initiated by the User (automatically or at User's request).
UI 008	M	*The ITSS "CSA"* shall have an integrated function for searching data. The procedures for data and records retrieval shall be carried out via simple search (specifying search series) or via complex search allowing for more accurate filtering of the information (QBE forms). Regardless of the nature of the information searched, the User shall use the same query and data retrieval for any part of User Interface of the IT product.
UI 009	M	In addition to the search module implemented on the basis of QBE principle that would give the possibility to define complex queries visually, the User

ID	Binding level	Requirement
		Interface shall provide for the possibility to refine the search results by filtering the information in the list of search results.
UI 010	M	Indexed values (values from Classifiers, Nomenclatures) shall have the option to be filtered by picking up the value from predefined lists. For numerical types of fields or calendar data there should be the possibility to filter as per the exact value of the searched feature (example: ***01.04.2018****- all records with a specified date*) or by logical criteria (example*: **<31.12.2017** – all records with the date older than 31.12.2017, **>31.12.2017** – all records with the date more recent than 31.12.2017*).
UI 011	M	Also, it should be granted the possibility to filter the results according to the mask (*for example, filtering by IDNP*) as per the sample: **098151224*** - all the records that begin with the series of characters "**098151224**", ***ESCU** - all the records that end with the series of characters "**ESCU**" or ***URCAN*** - all the records that comprise the series of characters "**URCAN**" in their content.
UI 012	M	The content of any table comprising results shall have the possibility to be exported in any of the following format: DOC/DOCX, XLS/XLSX and PDF.
UI 013	M	*By default, the ITSS "CSA"* shall allow appending files to information objects or references to the files stored on server / WEB for all information objects. This functionality shall be used by Users depending on access profile settings. The appended cards shall comprise a series of attributes: date of creation, date of changing, responsible person, size.
UI 014	M	*The ITSS "CSA"* Users shall have access to *context-sensitive help* in all System interfaces.
UI 015	M	When using the functions to define and configure reports, the Users shall be able to access the dictionary of data stored within the System.

7.9. Maintenance Requirements

In order to make the *ITSS "CSA"* available to business Users at the aggregated level, the ITSS shall be maintained and monitored on a continuous basis. The IT System shall allow identifying proactively the issues and preventing them via easy unrolled operating maintenance activities at the level of all System components. Table 7.18 comprises the requirements regarding the maintenance features related to the *ITSS "CSA".*

Table 7.18. *ITSS "CSA"* maintenance requirements

ID	Binding level	Requirement
MR 001	D	*The ITSS "CSA"* shall have mechanisms to monitor the load and operation level of all key components (example*: components of business logics levels and data levels*).
MR 002	D	The ITSS "CSA" shall generate notifications when the performance of its components is degrading (example: the response time to User's queries exceeds two seconds).
MR 003	M	All the errors and exemptions in the ITSS "CSA" operation shall be recorded.
MR 004	M	*The Bidder* shall list the means to be used in the process of *ITSS "CSA"* trouble-shooting.
MR 005	M	*The Bidder* shall prepare means facilitating the *ITSS "CSA"* administration functions:

ID	Binding level	Requirement
		• starting the System components; • restarting the System components; • setting the DB and content file back-ups; • restoring the *ITSS "CSA"* functionalities on the basis of the indicated back-up.
MR 006	M	The Source Code of the *ITSS "CSA"* shall be developed as per the recommendations for writing a Source Code easy to maintain, namely: well structured, accompanied by comments, suggestive variables, etc.
MR 007	M	The ITSS "CSA" Architecture shall allow the PSA to implement in a simplified way the changes at the System level. The segment affected by changes shall be minimal, while the components to be tested following the operated changes shall be clearly identifiable.
MR 008	M	*The ITSS "CSA"* shall allow defining and rolling the tasks envisaged for operating maintenance activities (example*: archiving historical data*, *preparing data for comprehensive reports, etc.*).
MR 009	M	The ITSS "CSA" Architecture shall allow implementing new versions provided by the Bidder without affecting the existing configurations, the components implemented by the *PSA* and interfaces implemented for interacting with external IT Systems.
MR 010	M	There should be possible to roll easily the *ITSS "CSA"* from the production environment in other operating environments and vice-versa in order to ensure System testing and development processes. The ITSS "CSA" relevant documentation shall describe this process.
MR 011	M	*The ITSS "CSA"* shall have procedures for processing all errors generated. The errors occurring during the System operation shall be recorded and made available for subsequent analysis with the aim to improve the quality of the IT solution.

7.10. Scalability Requirements

While operating the *ITSS "CSA"* it is possible that the number of transactions processed and of concurrent Users increases or decreases substantially from one time period to another. To ensure rational use of processing resources, the IT System shall be easily scalable (up and down). Table 7.19 comprises the requirements regarding the scalability characteristics related to the *ITSS "CSA".*

Table 7.19. Scalability requirements of the *ITSS "CSA"*

ID	Binding level	Requirement
SR 001	M	*The ITSS "CSA"* shall allow increasing the processing capacity without interrupting its operation. To this end, the System shall support horizontal expansion of processing capacity (example*: adding new server hubs and balancing the load*).
SR 002	D	There should be the possibility to configure the *ITSS "CSA"* for automatic scaling at the level of key components (*lag sensitive*). The System scaling shall be done both up and down.
SR 003	M	*The ITSS "CSA"* shall have the possibility to serve an unlimited number of transactions, provided that the processing and data storing resources are

ID	Binding level	Requirement
		allocated properly. The resources shall be allocated horizontally (new servers without increasing the performance of the servers already in place).

7.11. Security Requirements

The ITSS "CSA" shall allow carrying out proper checks of information security risks during the System operation. The implemented security measures shall be aligned with security policy approved within the PSA and ensure preventing, detecting and reacting properly to security incidents.

The ITSS "CSA" shall implement a "*Multi-layered security*" approach at the System level and have the capacity to be integrated in the PSA institutional model for information security management (based on the set of standards ISO 27000).

This part sets the requirements regarding security characteristics related to the System requested by the PSA.

7.11.1. Requirements for Security Architecture

This Part comprises the requirements related to security Architecture implemented for the *ITSS "CSA".* Table 7.20 comprises all security Architecture requirements set for the *ITSS "CSA".*

Table 7.20. The security Architecture requirements set for the *ITSS "CSA"*

ID	Binding level	Requirement
SEC 001	M	The ITSS "CSA" Architecture shall be designed by using *"Secure by design"* approach.
SEC 002	M	The ITSS "CSA" security Architecture shall be documented at the technical level.
SEC 003	M	The documentation shall contain details regarding the implemented security model, components presented and the role of each component from the security standpoint.
SEC 004	M	The documentation shall contain specifications regarding the placement of *ITSS "CSA"* components at the network level and the Bidder's recommendations regarding the access rules at the network level required to be set by the *PSA* to ensure secured access to all System components (example*: communication matrix among services*).
SEC 005	M	All System processes related to ITSS "CSA" components shall be rolled with minimum privileges necessary to fulfil the assigned tasks.
SEC 006	M	All the access credentials used by the application shall be configurable in administrative interfaces. *The ITSS "CSA"* shall not contain hard-coded access credentials.
SEC 007	M	*The ITSS "CSA"* shall not contain stored open-type access credentials at the level of its components (DB, configuring files).
SEC 008	M	All *ITSS "CSA"* exposed interfaces shall be accessed having applied reliable authentication methods (example*: X.509 Certificate*).
SEC 009	M	The access to functions provided to non-authenticated Users (exposing services on the PSA official WEB Page) shall be checked with means of protection against service overloading by one or several network hubs.

ID	Binding level	Requirement
SEC 010	M	All fields of forms completed by Users must be validated by type both for the client and for the server.
SEC 011	M	The ITSS "CSA" shall be secured against OWPSA Top 10 vulnerabilities (2017).
SEC 012	M	*The ITSS "CSA"* shall ensure the confidentiality of data sent-received via communication channels.
SEC 013	M	The Users' actions shall be recorded in electronic logs.
SEC 014	D	The System shall deliver a regular signal indicating its operating status.

7.11.2. Requirements for Authentication Mechanism

This Part comprises the requirements regarding the authentication mechanism to be implemented under the *ITSS "CSA".* Table 7.21 comprises all the requirements to be met by the *ITSS "CSA"* authentication mechanism.

Table 7.21. The requirements for the *ITSS "CSA"* authentication mechanism

ID	Binding level	Requirement
SEC 015	M	*The ITSS "CSA"* shall allow for its functions to be accessed only after successful authentication of the User. *The ITSS "CSA"* shall grant support for at least the following authentication methods: based on ID and Password, Windows authentication (integration with *Active Directory*), authentication in two steps (2FA), *MPass*. *The ITSS "CSA"* shall allow the Users to change their individual passwords.
SEC 016	M	*The ITSS "CSA"* shall allow the Users to register their profile information as well (example*: ID, Password, name, First Name, Email, etc.*).
SEC 017	M	Users' passwords shall be protected. The password protection method shall ensure the possibility to intercept, infer or recover it.
SEC 018	M	*The ITSS "CSA"* shall use the API displayed by IRAMS to implement the password management procedures.
SEC 019	D	*The ITSS "CSA"* shall allow for differentiated use of password policies for different types of Users.
SEC 020	M	*The ITSS "CSA"* shall allow locking, deactivation and suspension of User accounts at the level of application.
SEC 021	M	*The ITSS "CSA"* shall be integrated with guiding service implemented within the PSA (the PSA uses *MS Active Directory*) for internal Users. *The ITSS "CSA"* will implement authentication mechanisms for external Users. Upon setting a new User account, the *ITSS "CSA"* shall have the option to select from the list of Users available under the guiding service.
SEC 022	D	*There* should be the possibility to integrate the *ITSS "CSA"* with external services such as "ISP" (*Identity Services Providers*). To this end, the open standards *and* protocols shall be used (example*: SAML*). The authentication methods shall be supported with the involvement of an external ISP, namely: • ID and password; • X.509 Certificates; • OPR (One Time Password).

ID	Binding level	Requirement
SEC 023	M	When using mobile applications, the access shall be granted based on User's access credentials and on a single key set in the configuration of client application. Communication with *ITSS "CSA"* server shall be encrypted.
SEC 024	D	*The ITSS "CSA"* shall allow for differentiated application of authentication methods, depending on the accessed resources (example*: default ID and password, additional OPR for administrative interface*).
SEC 025	M	*The ITSS "CSA"* shall allow for setting the number of simultaneous connections to be initiated by a User.
SEC 026	M	*The ITSS "CSA"* shall allow for setting the time for ending the User's sessions in case of inactivity.
SEC 027	M	*The ITSS "CSA"* shall have efficient mechanisms to prevent the unauthorised taking over of active sessions initiated by authorised Users.
SEC 028	M	The working session in the *ITSS "CSA"* shall be locked upon the User's request or automatically upon the expiry of User's session.

7.11.3. Requirements for the Authorisation Mechanism

This Part comprises the requirements related to authorisation mechanism to be implemented under the *ITSS "CSA".* Table 7.22 comprises all the requirements set for the *ITSS "CSA"* authorisation mechanism.

Table 7.22. The requirements for *ITSS "CSA"* authorisation mechanism

ID	Binding level	Requirement
SEC 029	M	The ITSS "CSA" shall allow for granular management of the rights of access to its objects and the possible actions on them (example: business entities, properties of business entities, electronic forms, menus, reports, and actions aimed at creating/viewing/updating/deleting, etc.).
SEC 030	M	The authorisation method within the System shall be based on the principle "*everything which is not allowed is forbidden*".
SEC 031	M	*The ITSS "CSA"* shall allow defining groups of Users and roles, and User association with those groups and roles.
SEC 032	M	*The ITSS "CSA"* shall allow for granting the rights of access at the level of explicit User, group and role. A group of Users may comprise several subgroups/roles. A User may be associated with one or several groups and roles, and the User's rights of access are determined cumulatively.
SEC 033	M	The ITSS "CSA" shall allow for granting rights of access based on business rules (example: amending a document only when the User is the author or when the operation is performed within a certain time period, status or context).
SEC 034	M	*The ITSS "CSA"* shall allow for temporary assignment of rights held by a User to another User. This assignment shall be done by preserving or suspending the rights held by the User who is temporarily assigned the rights.
SEC 035	D	*The ITSS "CSA"* shall allow for segregating the administrative activities (example: Administrator 1 makes the changes, Administrator 2 confirms them).
SEC 036	M	*The ITSS "CSA"* shall deliver visualisations and reports regarding the configured access rights. The latter shall be parameterised depending on at least the

ID	Binding level	Requirement
		following criteria: group of Users/roles, User ID, business entity, property afferent to business entity, allowed actions.
SEC 037	M	*The ITSS "CSA"* shall have capabilities to authenticate and authorise the Users through the PSA IRAMS.
SEC 038	M	The authorisation mechanism implementation matters related to *ITSS "CSA"* Users will be carried out under the *ITSS "CSA"* and IRAMS, depending on their peculiarities.

7.11.4. Requirements for the validation mechanism of data inputs/outputs

This Part comprises the requirements related to the validation mechanism of data inputs/outputs comprised by electronic forms provided by the *ITSS "CSA".* Table 7.23 comprises all requirements for the validation mechanism of data inputs/outputs comprised by electronic forms provided by the *ITSS "CSA".*

Table 7.23. The requirements for validation mechanism of data inputs/outputs comprised by electronic forms provided by the *ITSS "CSA"*

ID	Binding level	Requirement
SEC 039	M	*The ITSS "CSA"* shall have appropriate mechanisms to prevent the manipulation of input data (received from Authorised Users, received from external applications).
SEC 040	M	All the changes targeting critical and sensitive data under the *ITSS "CSA"* shall be carried out via specialised forms and documents, as per the workflow defined for these categories of documents (example*: correcting the data in an issued civil status document*).
SEC 041	M	*The ITSS "CSA"* shall carry out full and independent validation of data on the level of presentation, the level of business logics, and the level of data with the aim to ensure data integrity, completeness and correctness.
SEC 042	M	All data displayed within the *ITSS "CSA"* shall be accompanied by a security marking as per a classifier set to this end under the *ITSS "CSA".*
SEC 043	M	The confidential data shall not be insecurely stored and accessed under the *ITSS "CSA"* (example*: log files, caching*).
SEC 044	M	The ITSS "CSA" shall have mechanisms providing additional protection to particularly confidential data (example: masked display of data, storing encrypted data, repeated authentication of Users, etc.).
SEC 045	M	*The ITSS "CSA"* shall have routine procedures to verify and detect possible corruption of data integrity relations.
SEC 046	M	*The ITSS "CSA"* shall have appropriate mechanisms to prevent any manipulation of data stored in an application.

7.11.5. Requirements for Logging and Auditing Mechanism

This Part comprises the requirements intended to implement an event logging and security auditing mechanism under the *ITSS "CSA".* Table 7.24 comprises all requirements set for the logging and auditing mechanism provided by the *ITSS "CSA".*

Table 7.24. The requirements for the logging and auditing mechanism of the *ITSS "CSA"*

ID	Binding level	Requirement
SEC 047	M	*The ITSS "CSA"* shall have audit components to collect and manage the audit records in a centralised manner for each IT System module.
SEC 048	M	The audit component shall allow for granular configuration of audit policy.
SEC 049	M	*The ITSS "CSA"* shall allow for setting audit policy at the level of object / business entity and at the level of a logged event.
SEC 050	M	The ITSS "CSA" shall allow for setting specific characteristics of events to be logged (example: produced over a certain time period, a certain value of business entity property).
SEC 051	M	*The ITSS "CSA"* shall allow for auditing any event at the level of any object or business entity within the IT System.
SEC 052	M	Each audit record shall contain at least: • the time the event occurred; • the event subject (User ID); • the affected object or business entity; • the event that occurred; • IP address of the source that initiated the event.
SEC 053	M	The audit records shall not comprise confidential business information (example*: passwords introduced during the failed authentication attempt*s).
SEC 054	M	Errors that may occur during the process of logging the audit records shall not affect the System smooth operation.
SEC 055	M	The audit component shall use the System set at the operating system level where the audit component is rolled.
SEC 056	M	The audit component shall have a mechanism to archive the historical audit records. There should be the possibility to parameterize the archiving process (frequency, data time period, archiving format, destination etc.).
SEC 057	D	*The ITSS "CSA"* shall be able to generate automatically notifications to people responsible for carrying out certain security events as per the configurations set.
SEC 058	D	Based on open standards, there should be the possibility to integrate the audit component with SIEM (*Security Incident and Event Management*) solutions to take over the audit records produced within the System by the respective solutions.
SEC 059	M	*The ITSS "CSA"* shall allow for fixing historical versions of data considered as extremely sensitive.
SEC 060	M	The activities carried out to change statuses and responsible for records shall be logged.
SEC 061	M	*The ITSS "CSA"* shall have suitable tools for accessing and processing the logged events, including filtering the audit records by any field held and their export in usual format. The System audit tools could be used also to import archives containing audit files to do occasional analyses.
SEC 062	M	*The ITSS "CSA"* shall have reliable mechanisms to protect the integrity of logged audit records.
SEC 063	M	The critical business events could be logged in parallel via *MLog.*

ID	Binding level	Requirement
SEC 064	M	*The ITSS "CSA"* shall deliver a mechanism to configure business events to be logged alternatively via *MLog*.

7.11.6. Requirements for Exemption and Error Management Mechanism

This Part comprises the requirements related to the exemption and error management mechanism under the *ITSS "CSA".* Table 7.25 comprises all the requirements set for the exemption and error management mechanism provided by the *ITSS "CSA".*

Table 7.25. The requirements for exemption and error management mechanism provided by the *ITSS "CSA"*

ID	Binding level	Requirement
SEC 065	M	*The ITSS "CSA"* shall record in a centralized manner all exemptions and errors generated by its components.
SEC 066	M	When an error occurs, the *ITSS "CSA"* shall display a generic error message for the User. The message may comprise the error code and a single error identifier to facilitate the involvement of support services.
SEC 067	M	*The ITSS "CSA"* shall have the tools necessary for analysing and processing the records related to exemptions and errors.
SEC 068	D	*The ITSS "CSA"* shall be able to generate automatically notifications to responsible people when certain errors occur in the operation of System components.

7.12. Resilience and Continuity Requirements

This Part sets the requirements regarding the continuity and resilience characteristics of the *ITSS "CSA"* requested by the PSA.

Table 7.26. The requirements for *ITSS "CSA" resilience capacities*

ID	Binding level	Requirement
RC 001	M	*The ITSS "CSA"* shall have implemented tools to carry out the procedures for automatic generation of back-ups and management of historical back-ups.
RC 002	M	*The ITSS "CSA"* shall have mechanisms to ensure data integrity when failures occur at the level of any of its components.
RC 003	M	*The ITSS "CSA"* shall have mechanisms for quick recovery of System availability and accessibility when continuity incidents occur.
RC 004	M	The ITSS "CSA" Architecture shall be resilient to failures of components and have no SPOF.
RC 005	M	*The ITSS "CSA"* shall have mechanisms to ensure data integrity when accidental failures occur at the level of any of its components.
RC 006	M	*The ITSS "CSA"* shall have mechanisms for quick recovery of System availability and accessibility when continuity incidents occur.

8. Requirements for implementing the *ITSS "CSA"*

This Chapter sets the requirements regarding the phases and deliverables of the *ITSS "CSA"* Implementation Project. The purpose of these requirements is to ensure that the *Bidder* will deliver an IT solution that meets all the specifications set, while its operation in the production environment is confirmed at a reasonable level of certainty.

The requirements defined in this Chapter are binding. *The Bidder* shall specify for each requirement how it is supposed to be implemented (when the requirement refers to planned measures after the Contract conclusion) or shall submit the requested information (if the requirement is applicable at the stage of bid submission). The bid must contain also pertinent and sufficient information regarding the *Bidder* capacity to meet the requirements defined in this Chapter.

8.1. General Requirements set for ITSS "CSA" Implementation

This Part comprises general requirements for organising and carrying out the *ITSS "CSA"* Implementation Project.

Table 8.1. General requirements for implementing *the ITSS "CSA"*

ID	Binding level	Requirement
ISR 001	M	The ITSS "CSA" design, development and implementation shall last eight months at most after the Contract conclusion.
ISR 002	M	*The Bidder* shall describe in its bid the proposed approach in terms of organising the *ITSS "CSA"* Project Implementation. *The Bidder* shall argue why the proposed approach is the most appropriate to support the *ITSS "CSA"* implementation strategy selected by the *PSA* by the deadline set.
ISR 003	M	The approach proposed by the Bidder for organising the *ITSS "CSA"* Project Implementation shall be independent from the implementation of other applications and components under the future PSA application architecture.
ISR 004	M	The approach proposed by the Bidder shall ultimately ensure that the *ITSS "CSA"* implementation would go through key stages set in the Terms of Reference and produce the deliverables requested therein.

8.2. Project Management Requirements

During the *ITSS "CSA" Project Implementation*, the Project management activities shall produce a series of deliverables to be coordinated and agreed with the *PSA* and ensure smooth unrolling of Project works.

8.2.1. General Requirements

The general requirements for organising the *ITSS "CSA"* Project Implementation Management framework are displayed in Table 8.2.

Table 8.2. General requirements for organising the *ITSS "CSA"* Project Implementation Management Framework

ID	Binding level	Requirement
ISR 005	M	*The Bidder* shall be responsible for managing the Implementation Project as per the Project Work Plan and practices agreed jointly with the *PSA*.

ID	Binding level	Requirement
ISR 006	M	*The Bidder* shall be responsible for identifying and mobilising the resources necessary to carry out the activities assigned to him/her comprised by the Project Management Plan at the agreed quality level.
ISR 007	I	*The PSA* shall be responsible for all procedures and administrative aspects related to Project launch, organising the in-house Project Team, preparing the ICT environment necessary for *ITSS "CSA" implementation*.
ISR 008	M	The Project shall be managed by using a well-known methodology or standard in the project management area (example*: PRINCE 2, PMBOK, etc.*).
ISR 009	M	The Bidder shall include in its bid the draft Document on Project initiation (*PID / Project Charter*). The Document shall clearly mention at least the following: • Project management Organigram, including: Project Director, Project Committee, the roles of Project Team members from the Provider's side, the roles of Project Team members from the *PSA side*; • Key duties shall be defined for each role within the Project; • Practices applied for Project interaction and collaboration, including: managing the Project Plan; detailed planning of Project activities; resource managing; communication plan; change management, risk management, managing the quality of deliverables; monitoring and reporting the progress; managing the exemptions; managing the Project library.
ISR 010	M	*Both the PSA and the Bidder* shall designate its Project Manager to manage the appropriate Project Team (*PSA's* and *Bidder's).*
ISR 011	M	The Bidder's Project Manager shall have the authority necessary to carry out Project activities and bear primary responsibility for producing and submitting the Project deliverables in compliance with the established quality terms and conditions.
ISR 012	M	*The Bidder* may appoint one or several Team Leaders to facilitate the process of communication and collaboration with the PSA Team, depending on their area of competence.
ISR 013	M	If the *Bidder* is represented by an association or subcontracts another company to get involved in Project implementation, the roles and responsibilities of all members of the association/subcontractor shall be clearly specified.
ISR 014	I	*The PSA and UNDP-Moldova* may contract external consultants/experts to be delegated quality assurance function for the overall Project.
ISR 015	D	*The Bidder* shall prove the maturity of practices applied for *ITSS "CSA"* implementation by submitting the relevant as perity certificates (example*: ISO 9001, ISO 20000, ISO 27001, etc.*).

8.2.2. Requirements for Project Management activities

The requirements for Project Management activities aimed at implementing the *ITSS "CSA"* are displayed in Table 8.3.

Table 8.3. The requirements regarding the key activities for Project Management

ID	Binding level	Requirement
ISR 016	M	For Project Management, the *Bidder* shall carry out at least the following activities: • Developing and agreeing with the *PSA* the **Project Initiation Document**. Making the necessary adjustments as appropriate; • Developing and agreeing with the *PSA* the **Project Plan**. Making the necessary adjustments as appropriate throughout the Project implementation period; • Developing detailed Work Plans; • Coordinating the activities as per the detailed Work Plan; • Implementing the Communication Plan; • Preparing Weekly Project Progress Reports; • Keeping the Project Management Registers throughout the Project implementation period. Binding registers: Register of deliverables, Register of risks, Register of changes, Register of communications/press releases, Register of events; • Organising the Project Management meetings as per the agreed Communication Plan; • Submitting the final reports for each phase and the supporting presentations during the Project Management meetings at the end of each phase; • Closing the Project main phases and submitting the acceptance documents to the *PSA*; • Placing the Project Management deliverables in the Project library.

8.2.3. Requirements for Project Management deliverables

The requirements related to deliverables resulting from carrying out the Project Management activities are displayed in Table 8.4.

Table 8.4. The requirements for Project Management deliverables

ID	Binding level	Requirement
ISR 017	M	All communications and deliverables under the Project Management activities shall be prepared in Romanian and, upon need, in English.
ISR 018	M	For Project Management the *Bidder* shall deliver at least the following deliverables: • Project Initiation Document; • Project Plan and amendments thereof; • Detailed Project Work Plans (example: sprints, iterations); • Supporting presentations for kick-off meetings and for other Project Management meetings; • Project weekly progress reports and Project registers maintained and updated as per the Project Initiation Document. • Phase final reports to comprise at least the following information: general presentation of the completed phase, submitting the Project

ID	Binding level	Requirement
		Plan for the next period; risk analysis; setting the Project issues; registration the Project quality level. • Reports on exemptions to comprise at least: the description of reasons for Project deviations; the produced impact, solutions suggested and their general impact on the Project, options recommended by the Project Manager or by the Provider.

8.2.4. Acceptance Criteria for Project Management deliverables

The acceptance criteria for the deliverables resulting from Project Management activities are displayed in Table 8.5.

Table 8.5. The acceptance criteria for deliverables resulting from Project Management activities

ID	Binding level	Requirement
ISR 019	M	Deliverables resulting from Project Management activities shall be accepted when: • Deliverables are timely submitted to the *PSA*; • *The PSA* has no objections regarding the deliverables completeness and correctness.

8.3. Phases of ITSS "CSA" Project Implementation

The Project phases shall meet the Technical Regulation **"Software life cycle "RT 38370656 – 002:2006** (Published: 23.06.2006 in the Official Gazette No. 95-97 Article No. 335). The activities mentioned under each phase represent the minimum requirements. The indicated deliverables and their acceptance criteria are binding. As per the requirements referred to in Section 8.1, the Bidder shall specify in its bid the implementing phases and the produced deliverables. Each phase shall define the objectives, responsible people and the tools used to carry out the envisaged activities. Each phase shall be planned and coordinated with the PSA. The Project timeline must include the submission of documents to the PSA for approval. The timeframe for reviewing and verifying the deliverables by the PSA shall correspond to the rules set by the in-house standards of the institution.

8.3.1. Review Phase: key activities

This Part comprises the requirements regarding the Analysis Phase key activities under the *ITSS "CSA"* development and implementation processes. Table 9.6 comprises the requirements regarding the Analysis Phase key activities.

Table 8.6. The requirements regarding the Analysis Phase key activities

ID	Binding level	Requirement
ISR 020	M	The *Bidder* shall validate the business needs for the *ITSS "CSA"* under the business analysis phase. To this end, *the Bidder* shall carry out the following activities: • revise/analyse the business requirements; • analyse the relevant business processes; • analyse the reporting processes; • revise/analyse the reporting requirements;

ID	Binding level	Requirement
		• organise workshops between the *PSA* and *Bidder* tackling the analysis of business processes; • analyse the Users and their roles under the *ITSS "CSA";* • identify the data sources; • analyse the current software, hardware and network infrastructure. • The works shall be carried out by interviewing the responsible individuals from business and IT Subdivisions, and by analysing the relevant documentation.

8.3.2. Review Phase: deliverables

This Part comprises the requirements regarding the Analysis Phase deliverables under the *ITSS "CSA"* development and implementation processes. Table 8.7 comprises the requirements regarding the Analysis Phase deliverables.

Table 8.7. The requirements regarding the Analysis Phase deliverables

ID	Binding level	Requirement
ISR 021	M	Following the business analysis, the Provider shall submit as a deliverable *SRS* that represent a review report of the situation "As-Is" of business processes, which may contain clarifications and proposals relative to the Terms of Reference for the *ITSS "CSA".*
ISR 022	M	The time required for preparing the *SRS* shall not exceed one month after the start of the Project.
ISR 023	I	Based on the prepared *SRS*, the *PSA* can accept adjustments to functional and non-functional specifications as per the Terms of Reference.

8.3.3. Review Phase: Deliverables Acceptance Criteria

This Part comprises the requirements regarding the acceptance criteria for the deliverables submitted during the Analysis Phase under the ITSS "CSA" development and implementation processes. Table 8.8 comprises the requirements regarding the acceptance criteria for the deliverables submitted during the Analysis Phase.

Table 8.8. The requirements regarding the acceptance criteria for the deliverables submitted during the Analysis Phase

ID	Binding level	Requirement
ISR 024	M	Acceptance of deliverables submitted during the Analysis Phase of the Project shall be carried out as per the following criteria: • Deliverables are submitted to the *PSA*; • *The PSA* submitted a positive opinion and has no objections regarding the completeness and correctness of deliverables; • The deliverables Acceptance Protocol has been signed by both Parties.

8.3.4. Technical Design Phase: key activities

This Part comprises the requirements regarding the key activities of the ITSS "CSA" Technical Design Phase. Table 8.9 comprises the requirements regarding the key activities of the Technical Design Phase.

Table 8.9. The requirements regarding the key activities of the Technical Design Phase

ID	Binding level	Requirement
ISR 025	M	During this stage the *Bidder* shall develop the technical design for the *ITSS "CSA" (SDD)* as per the functional and non-functional specifications. *The Bidder* shall carry out at least the following: • define the system architecture and its levels (peculiarities for implementing the presentation level, application level, data level and technological level); • define the technical peculiarities for the *ITSS "CSA"* search Architecture level; • review and describe the scenarios and workflows. Following the business review, the successful Bidder shall describe the existing business processes (BPA development) and propose options for reengineering and optimisation of workflows (BPR development); • define the detailed data model afferent to the *ITSS "CSA";* • map the data model with the currently existing data sources within the PSA; • define the basic peculiarities of *ITSS "CSA"* User Interface; • define the customisations to be carried out using the native capacities of the proposed solution; • define the developments to be performed; • define technical specifications for the applied interfaces of the *ITSS "CSA"* necessary to integrate with external systems.

8.3.5. Technical Design Phase: deliverables

This Part comprises the requirements regarding the deliverables of the of the ITSS "CSA" Technical Design Phase. Table 8.10 comprises the requirements regarding the Technical Design Phase deliverables.

Table 8.10. The requirements regarding the Technical Design Phase deliverables

ID	Binding level	Requirement
ISR 027	M	After the technical design, *the Bidder* shall deliver **the Software Design Description (*SDD*)**. It is a guiding document containing the activities aimed at developing the *ITSS "CSA"* that contains detailed description of the following visions: • description of technology and methods for *ITSS "CSA"* implementation*;* • data structures and constraints thereof; • architecture of IT System and its components with detailed description of all architectural visions for the *ITSS "CSA";* • description of the interaction way of System components; • *ITSS "CSA"* User Interface that covers the design of all User Interface components; • *ITSS "CSA"* functionalities comprising detailed description of all scenarios and implementation algorithms for the ITSS "CSA" functionalities.

ID	Binding level	Requirement
ISR 028	M	The time required for preparing the *SDD* shall not exceed one month and a half after the start of the Project.

8.3.6. Technical Design Phase: acceptance criteria of deliverables

This Part comprises the requirements regarding the acceptance criteria for the deliverables submitted during the ITSS "CSA" Technical Design Phase. Table 8.11. comprises the requirements regarding the acceptance criteria for the deliverables submitted during the Technical Design Phase.

Table 8.11. The requirements regarding the acceptance criteria for the deliverables submitted during the Technical Design Phase

ID	Binding level	Requirement
ISR 029	M	Acceptance of the Technical Design Phase is conditioned by the delivery of *SDD* to the PSA, and the PSA responsible people have no objections regarding its completeness and correctness.
ISR 030	M	Acceptance of the Technical Design Phase shall end when the Acceptance Protocol is signed by both Parties.

8.3.7. Development/Configuration Phase: key activities

This Part comprises the requirements regarding the key activities carried out during the ITSS "CSA" Development/Configuration Phase. Table 8.12 comprises the requirements regarding the key activities of the *ITSS "CSA"* Development/Configuration Phase.

Table 8.12. The requirements regarding the key activities of the Development Phase.

ID	Binding level	Requirement
ISR 031	M	During this phase the *Bidder* shall configure and adjust (in case there are solutions or universal platforms in place) or develop and configure (when the IT System shall be developed from scratch) the ITSS "CSA" as per the SDD specifications. *The Bidder* shall carry out at least the following activities: • install the production, testing and training environments of the *ITSS "CSA"* (Operating System/DBMS/applications, etc.); • develop, roll and configure *the ITSS "CSA"* as per the *SDD;* • roll the ITSS "CSA" components in the prepared operating environments.
ISR 032	M	The ITSS "CSA" Development/Configuration Phase shall not exceed six calendar months.

8.3.8. Development/Configuration Phase: deliverables

This Part comprises the requirements regarding the deliverables submitted during the ITSS "CSA" Development Phase. Table 8.13 comprises the requirements regarding the deliverables submitted during the Development Phase.

Table 8.13. The requirements regarding the deliverables submitted during the Development Phase.

ID	Binding level	Requirement
ISR 033	M	*The Bidder* shall develop and configure the *ITSS "CSA"* components as per the functional and non-functional specifications in the: • production environment; • testing/training environment.
ISR 034	M	*The Bidder* shall prepare and deliver full technical documentation afferent to the implemented components as per the current PSA Methodology.
ISR 035	M	*The Bidder* shall deliver the plan and testing scenarios and test the *ITSS "CSA"* components, carrying out: • unit testing; • integration testing; • stress testing; • load testing.

8.3.9. Development/Configuration Phase: acceptance criteria of deliverables

This Part comprises the requirements regarding the acceptance criteria for the deliverables submitted during the *ITSS "CSA"* development/configuration phase. Table 8.14 comprises the requirements regarding the acceptance criteria for the deliverables submitted during the *ITSS "CSA"* development/configuration phase.

Table 8.14. The requirements regarding the acceptance criteria for the deliverables submitted during the development/configuration phase

ID	Binding level	Requirement
ISR 036	M	*The ITSS "CSA"* components shall be implemented and configured as per the functional and non-functional specifications in the following environments: • production environment; • testing/training environment.
ISR 037	M	Full technical documentation afferent to the *ITSS "CSA"* implemented components shall be delivered.
ISR 038	M	The Beneficiary has no objections or comments regarding the deliverables quality.
ISR 039	M	The deliverables Acceptance Protocol of the development/configuration phase shall be signed by the Bidder and the PSA.

8.3.10. Acceptance Testing Phase: key activities

This Part comprises the requirements regarding the key activities carried out during the *ITSS "CSA"* Acceptance Testing Phase. Table 8.15 comprises the requirements regarding the key activities carried out during the Acceptance Testing Phase.

Table 8.15. The requirements regarding the key activities carried out during the Acceptance Testing Phase

ID	Binding level	Requirement
ISR 055	M	During this phase all ITSS "CSA" components are implemented and configured as per the functional and non-functional specifications.

ID	Binding level	Requirement
		The ITSS "CSA" is made available and is operational in all environments it was implemented. *The Bidder* shall organise the System acceptance testing. To this end, the Bidder shall carry out at least the following activities: • define the testing strategy and procedures; • prepare detailed testing plans, including testing scenarios; • receive the detected errors and remove/address them; • prepare the plan with the final testing results, including the status of all identified errors.
ISR 056	M	The coverage of *ITSS "CSA" capacities* with unit tests shall be at least 90%.

8.3.11. Acceptance Testing Phase: deliverables

This Part comprises the requirements regarding the deliverables of the ITSS "CSA" Acceptance Testing Phase. Table 8.16 comprises the requirements regarding the deliverables of the Acceptance Testing Phase.

Table 8.16. The requirements regarding the deliverables of the Acceptance Testing Phase

ID	Binding level	Requirement
ISR 057	M	*The Bidder* shall deliver the acceptance testing plan to the PSA for coordination and acceptance;
ISR 058	M	*The Bidder* shall deliver testing *scenarios* for all categories of tests (*unit testing, integration testing, stress testing, load testing, etc.*) to the PSA for coordination and acceptance.
ISR 059	M	*The Bidder* shall deliver the Report on *ITSS "CSA"* testing results to the PSA for coordination and acceptance.

8.3.12. Acceptance Testing Phase: acceptance criteria of deliverables

This Part comprises the requirements regarding the acceptance criteria for the deliverables submitted during the ITSS "CSA" Acceptance Testing Phase. Table 8.17 comprises the requirements regarding the acceptance criteria for the deliverables submitted during the ITSS "CSA" Acceptance Testing Phase.

Table 8.17. The requirements regarding the *ITSS "CSA"* acceptance criteria

ID	Binding level	Requirement
ISR 060	M	*The Bidder* shall carry out all the planned tests as per the Test Plan and the final testing results are acceptable by the ITSS "CSA".
ISR 061	M	The deliverables shall be accepted if no critical misalignments and less than three major misalignments have been detected.
ISR 062	M	The acceptance shall be dated with the day when all the misalignments detected upon delivery have been remedied.
ISR 063	M	The ITSS "CSA" Acceptance Protocol shall be signed by the Bidder and the PSA.

8.3.13. Training and Documentation Phase: launching constraints

This Part comprises the constraints to be met for launching the training activities in using the *ITSS "CSA".* Table 8.18 comprises all the constraints to be met for launching the *PSA* staff training *in* using the *ITSS "CSA".*

Table 8.18. The requirements regarding the constraints to be met for launching the training activities in using the *ITSS "CSA"*

ID	Binding level	Requirement
ISR 064	I	*The Bidder* shall ensure all the facilities necessary for organising the training of *PSA* Users *in* operating the ITSS "CSA" : • training class/room; • work stations connected to the network; • technical equipment necessary for training.
ISR 065	M	*The Bidder* shall ensure: • the environment for training (testing) prepared; • supporting materials for training (in Romanian); • tests for checking the training effectiveness (in Romanian).

8.3.14. Training and Documentation Phase: key activities

This Part comprises the requirements regarding the key activities to be carried out during the *ITSS "CSA"* Training and Documentation Phase. Table 8.19 comprises the requirements regarding the key activities to be carried out during the Training and Documentation Phase.

Table 8.19. The requirements regarding the key activities to be carried out during the Training and Documentation Phase

ID	Binding level	Requirement
ISR 066	M	*The Bidder* shall develop and deliver training programmes for all relevant categories of PSA Users.
ISR 067	M	*The Bidder* shall determine jointly with the *PSA* the **Plan for organising the training sessions**.
ISR 068	M	*The Bidder* shall carry out Users' training as per the Training Plan and Programmes agreed with the *PSA*. The training sessions shall be conducted in Romanian.
ISR 069	M	*The Bidder* shall provide training to a target group of Users – trainers who shall provide support and continue the training after the *ITSS "CSA"* is commissioned.

8.3.15. Training and Documentation Phase: deliverables

This Part comprises the requirements regarding the deliverables submitted during the *ITSS "CSA"* Training and Documentation Phase. Table 8.20 comprises the requirements regarding the deliverables submitted during the Training and Documentation Phase.

Table 8.20. The requirements regarding the deliverables submitted during the Training and Documentation Phase

ID	Binding level	Requirement
ISR 070	M	The Training and Documentation Phase implies providing the following categories of deliverables: • training regarding business operation of the *ITSS "CSA"* (the Users with non-administrator role); • training for *ITSS "CSA"* administration and configuration (the Users with administrator role); • full guides for all categories of *ITSS "CSA"* Users to be used for *ITSS "CSA"* operation and administration.
ISR 071	M	*The Bidder* shall prepare and deliver at least the following *ITSS "CSA" supporting* documents: • *ITSS "CSA"* Technical Architecture Document; • ITSS "CSA" Administration Guide; • *ITSS "CSA"* Users' Guide; • ITSS "CSA" Installation Guide; • Guide for operational configuration and maintenance of all *ITSS "CSA" components;* • Guides for Developers within the limit of components admitted for internal development by the *PSA*; • Supporting materials for training the Users with non-administrator and administrator roles.
ISR 072	M	The Guides shall be complete, detailed and updated for all groups of Users.
ISR 073	M	The Guides for the Users with administrator role shall be in Romanian. Other documentation shall be in Romanian (mandatorily), Russian or English. The Romanian version is mandatory for all categories of deliverables.
ISR 074	M	*The Bidder* shall deliver the Guides in electronic format. The Guides shall be convenient to be accessed and navigated, and the information – easy to identify.
ISR 075	M	*The Bidder* shall prepare and deliver the following categories of operating guidelines for the *ITSS "CSA"*: • Guide for removing the defects detected in the *ITSS "CSA";* • Manual for *ITSS "CSA"* installation and configuration; • Training materials for *ITSS "CSA"* Administrators; • Guides for making back-ups and restoring the *ITSS "CSA";* • Documentation of the process of data archiving and restoring from the *ITSS "CSA" Archive*; • *ITSS "CSA"* security documentation.
ISR 076	M	*The Bidder* shall deliver the Source Code and libraries related to the developments prepared for the *ITSS "CSA".* The Source Code shall contain sufficient comments to be easily understood by the *PSA staff*.

8.3.16. Training and Documentation Phase: acceptance criteria

This Part comprises the requirements regarding the acceptance criteria for the deliverables submitted during the *ITSS "CSA"* Training and Documentation Phase. Table 8.21 comprises the requirements regarding the acceptance criteria for the deliverables submitted during the *ITSS "CSA"* Training and Documentation Phase.

Table 8.21. The requirements regarding the acceptance criteria for the deliverables submitted during the Training and Documentation Phase

ID	Binding level	Requirement
ISR 077	M	*The Bidder* shall conduct all training sessions as per the Plan agreed jointly with the *PSA*.
ISR 078	M	The ITSS "CSA" documentation shall be complete and delivered in the form requested by the PSA.
ISR 079	M	The Source Code for the developments carried out for the *ITSS "CSA"* shall be delivered.
ISR 080	M	Libraries necessary for the compilation of the Source Code or for the ITSS "CSA" operation shall be delivered.
ISR 081	M	The Acceptance Protocol for training and documentation shall be signed by the Provider and the PSA.

8.3.17. Commissioning Phase: key activities

This Part comprises the requirements regarding the key activities for ITSS "CSA" commissioning. Table 8.22 comprises the requirements regarding the key activities aimed at ITSS "CSA" commissioning.

Table 8.22. The requirements regarding the key activities during the Commissioning Phase

ID	Binding level	Requirement
ISR 082	M	*The Bidder* shall suggest its approach for ITSS "CSA" commissioning (example: *sequentially*, *big-bang*, *parallel rolling*, *pilot*) and justify that approach.
ISR 083	M	*The Bidder* shall take part in all stages for ITSS "CSA" commissioning. To this end, *the Bidder* shall carry out at least the following actions: • develop the plan for commissioning (*cut-over plan*); • develop the roll-back plan (*where applicable*); • update the data sets generated/modified in the current systems after carrying out the procedures aimed at populating with initial data; • grant support to the execution of the plan for commissioning; • remove quickly the errors and defections that occurred in the *ITSS "CSA" operation*.

8.3.18. Commissioning Phase: deliverables

This Part comprises the requirements regarding the deliverables submitted during the ITSS "CSA" commissioning. Table 8.23 comprises the requirements regarding the ITSS "CSA" commissioning.

Table 8.23. The requirements regarding the deliverables submitted during the ITSS "CSA" commissioning

ID	Binding level	Requirement
ISR 084	M	*The Bidder* shall prepare and coordinate with the *PSA the* **Plan for ITSS "CSA" commissioning**.
ISR 085	M	*The ITSS "CSA"* has been commissioned.

8.3.19. Commissioning Phase: acceptance criteria

This Part comprises the requirements regarding the acceptance criteria for the deliverables submitted during the ITSS "CSA" commissioning. Table 8.24. comprises the requirements regarding the acceptance criteria for the deliverables submitted during the ITSS "CSA" commissioning.

Table 8.24. The requirements regarding the acceptance criteria for the deliverables submitted during the ITSS "CSA" commissioning

ID	Binding level	Requirement
ISR 086	M	*The ITSS "CSA"* shall be made available and be operational for all PSA Authorised Users.
ISR 087	M	The Protocol for accepting the *ITSS "CSA"* commissioning has been signed by the Bidder and the *PSA*.

8.3.20. Testing in Production Phase of the *ITSS "CSA"*

This Part comprises the requirements regarding the period for *ITSS "CSA"* testing in production. Table 8.25 comprises the requirements regarding the period for *ITSS "CSA"* testing in production.

Table 8.25. The requirements regarding the period for *ITSS "CSA"* testing in production

ID	Binding level	Requirement
ISR 088	M	*The Bidder* shall grant its on-site support for a three-month period after commissioning with the aim to fix/address the errors and operation deficiencies of the *ITSS "CSA"*. Over this period the ITSS "CSA" is considered to be tested in production.
ISR 089	M	During the period of testing the *ITSS "CSA"* in production, *the Bidder* shall carry out development activities to remove the errors and deficiencies, analyse the logging records to prevent some eventual issues, carry out adjustments to User Interface and to critical modules of the *ITSS "CSA"*.

8.3.21. Final Acceptance Phase of the *ITSS "CSA"*

This Part comprises the requirements regarding the *ITSS "CSA"* final acceptance. Table 8.26 comprises the requirements regarding the *ITSS "CSA"* final acceptance.

Table 8.176. The requirements regarding the *ITSS "CSA"* final acceptance

ID	Binding level	Requirement
ISR 090	M	The final acceptance of the *ITSS "CSA"* shall be registered based on the **Final Acceptance Protocol** signed by the *Bidder* and the *PSA*, provided the following conditions have been met: • the period for testing in production has expired; • all errors, deficiencies and major/serious (level 1) issues have been removed; • there are less than 10 errors and major/serious (level 2) issues to be removed; • none of testing scenarios could corrupt data integrity.
ISR 091	M	An error or issue afferent to the *ITSS "CSA"* is considered of level 1 if it locks or makes it difficult to use the IT System key functionalities. An error or issue afferent to the *ITSS "CSA"* is considered of level 2 if it locks or makes it difficult to use the functionalities for which there are alternative options (workarounds).

9. Requirements for Warranty, Maintenance and Post-implementation Support

The goal pursued by the *ITSS "CSA"* maintenance and post-implementation support services is to fulfil the following *Public Services Agency* objectives:

- Functionality provided by the ITSS "CSA" shall be timely aligned with the PSA changing business needs;
- Incidents and issues occurring during the *ITSS "CSA"* operation shall be timely addressed with minimum impact over the *PSA* activity;
- Difficulties encountered in the *ITSS "CSA"* operation shall be timely and correctly addressed without affecting the IT System operation.

To attain those objectives, the Bidder shall provide maintenance and post-implementation support services as per the requirements defined in this Scope of Work.

The Bidder shall describe the activities to be carried out to respond to those requirements, by submitting sufficiently detailed information about how it intends to render the requested services at the expected level, as well as the information regarding its technical, organisational capacities and competence, confirming its capability to render the requested services at the expected level.

The PSA expects that the offer for maintenance and post-implementation support services is based on best practices in the area of Project and IT service management (example*: ISO 20000, ITIL, etc.*).

9.1. General requirements for defect liability period, maintenance and post-implementation support

This Part comprises general requirements for defect liability period, maintenance and post-implementation support for the ITSS "CSA". Table 9.1 comprises all general requirements for defect liability period, maintenance and post-implementation support for the ITSS "CSA".

Table 9.1. General requirements for defect liability period, maintenance and support

ID	Binding level	Requirement
PIR 001	M	As part of the initial Contract for delivering and implementing the *ITSS "CSA", the Bidder* shall render defect liability, maintenance and support services for the IT System applications delivered over a 12-month period from the date of final acceptance of the IT System.
PIR 002	M	The price of the initial Contract for the development and implementation of the *ITSS "CSA"* shall include all defect liability, maintenance and post-implementation support services, except for the services of additional development beyond the *SRS and SDD* objectives.
PIR 003	M	The price of the initial Contract for the development and implementation of the *ITSS "CSA"* shall include granting by the Provider, upon the Beneficiary request, of 100 man-days of development services as specified in these Terms of Reference.
PIR 004	M	All the errors detected in the *ITSS "CSA"* operation during the defect liability period shall be remedied at the expense of the *Bidder* (those activities shall not be considered as development activities and not included in those 100 man-days of development services rendered during the defect liability period, support and maintenance).

ID	Binding level	Requirement
PIR 005	M	After a year of rendering defect liability, maintenance and post-implementation support services, the *PSA* may require to prolong the period of service rendering. *The Bidder* shall be required to accept subsequent rendering of services, for at least five years, under the conditions resulting from these Terms of Reference and bid estimates (example*: services level, services price, etc.*).

9.2. Specifications of maintenance and post-implementation support services

Here the types of requested maintenance and post-implementation support services are defined. Any further reference to those terms shall have the meaning stated under this part. The PSA requirements for each type of services shall be defined as well.

9.2.1. Support services for the *ITSS "CSA"* during the defect liability period

The support services shall be rendered by the Bidder *in* order to overcome the incidents produced during the *ITSS "CSA"* operation to address the issue detected and ensure proper and efficient use of the *ITSS "CSA"* by the PSA.

An incident afferent to the *ITSS "CSA"* is any event that has affected or could have affected the smooth operation of the IT System. An issue afferent to the *ITSS "CSA"* is the cause that has led or could have led to the occurrence of an incident.

An advice request is an application submitted by the *PSA* to the Bidder in order to obtain the consulting support during the ITSS "CSA" use, configuration and maintenance.

The support services are intended to ensure the use of the *ITSS "CSA"* in line with the quality parameters necessary for the *PSA*. The quality parameters for the *ITSS "CSA"* operation are as follows:

- **Availability** – the IT System capacity and the capacity of its components to receive queries from authorised entities and timely respond to those queries;
- **Suitability for use** – the IT System capacity to function properly/correctly/orderly, having delivered the expected services to authorised Users and entities;
- **Performance** – the IT System capacity to respond to lawful queries under the established parameters;
- **Security** – the IT System capacity to ensure confidentiality, integrity and availability of stored and managed data.

This part shall define the requirements for support services, using the aforementioned terminology. Table 9.2 comprises the requirements of support services to be rendered by the *Bidder* during the period of defect liability, maintenance and support.

Table 9.2. The requirements regarding the support services for the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 006	M	*The Bidder* shall grant support to the *PSA* in addressing the incidents related to the *ITSS "CSA",* regardless of the causes that led to the occurrence of the incident (example*: errors in the application, issues at the software level, issues in external applications*). To this end, depending on the peculiarity of each incident, the *Bidder* may undertake the following actions:

ID	Binding level	Requirement
		• receive from the *PSA* information about the incident that occurred and the context thereof; • localise the incident and identify the immediate actions to be undertaken to mitigate the incident impact; • identify the incident causes and define the actions necessary to be undertaken to remove the incident; • guide the *PSA* to undertake the actions aimed at mitigating the incident impact and address it within the established deadline; • present detailed information to the *PSA* regarding the incident causes, the rationale behind the actions undertaken and actions planned to prevent repeated occurrence of similar incidents; • consider the need to register any new issue related to the *ITSS "CSA"* (if the issue has been recorded, the *Bidder* shall manage it as per the requirements related to support services for problem resolution).
PIR 007	M	*The Bidder* shall render support services to address the issues recorded at the level of applications. To this end, depending on the peculiarity of each separate case, the *Bidder* can undertake the following actions: • receive and collect the information related to the issue, symptoms, effects, specific conditions; • analyse and localise the issue at the level of *ITSS "CSA"* components, identify interdependencies that contribute to the problem occurrence or are affected by it; • identify temporary solutions to mitigate the issue effects and guide the *PSA* in order to apply them; • identify solutions for the issue, ensure regular communication with the PSA regarding the progress made in identifying the solutions; • if the solutions are related to configuration of applications, the *PSA* shall be guided to implement them; • if the solutions imply changes at the level of the *ITSS "CSA"* programme code, they shall be applied by the Bidder *and* implemented under the maintenance services within the established deadline.
PIR 008	M	*The Bidder* shall render consulting support services in the operation of the *ITSS "CSA"* by the PSA. To this end, depending on the peculiarity of PSA consulting needs, the Provider can undertake the following actions: receive advice requests from the *PSA* and the information related to the context under which it needs advice; identify solutions and validate them within testing environments of the *Bidder*; provide full and accurate answers on how the *PSA shall react during the ITSS "CSA" operation*, as per the advice request.

9.2.2. Maintenance services for the *ITSS "CSA"* during the defect liability period

Maintenance services shall be rendered by the Bidder with the aim to maintain the applications within the optimal operation parameters. To this end, *the Bidder* may bring updates and changes in applications and new releases.

Updates for the *ITSS "CSA"* are changes carried out at the level of applications, conveyed to the *PSA* at the Bidder's initiative, with the aim to remove the problems, errors and vulnerabilities known to the *Bidder*.

N*ew releases* are software packages related to the *ITSS "CSA",* conveyed to the PSA at the Bidder's initiative that contain all the changes carried out previously in applications. In addition, they may comprise changes and updates, new components not included in the previous/old releases.

Table 9.3 comprises the requirements of maintenance services to be rendered by the *Bidder* during the defect liability period.

Table 9.3. The requirements regarding maintenance services for the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 009	M	*The Bidder* shall render, as appropriate, update services for the *ITSS "CSA"* and deliver new releases.
PIR 010	M	To this end, the *Bidder* shall prepare software packages and documentation afferent to updates and new releases.
PIR 011	M	All updates and new releases shall be implemented as per the requirements referred to in point "*Change Management*" of this Scope of Work.

9.2.3. Development services for the *ITSS "CSA"* during the defect liability period

Development services shall be rendered by the Bidder upon the PSA request with the aim to align the *ITSS "CSA"* with the PSA changing business needs (upgrading/improving the system, adjusting the system when the regulatory-legal framework has been amended, customizing the software aimed at ensuring its functioning capacity under the changed conditions (environment) or which are subject to change, specifying the corresponding programme documents and its reprogramming to improve the functional characteristics and other software attributes).

A request for change /development is an application submitted by the *PSA* to the Bidder with the aim to get changes at the level of ITSS "CSA" functionalities or with the aim to deliver new functionalities for the IT System.

A request from the *PSA* shall be considered a change/development only when the requested functionality has not been delivered by the ITSS "CSA" or it has been delivered differently than requested by the *PSA*. The last category does not include the requests related to the corrections brought to functionalities, which represent an issue in the *ITSS "CSA"* operation (according to the aforementioned definition).

Development services that exceed the amount of 100 man-days per annum shall be paid by the PSA in addition to the Contract sum, depending on the volume of services rendered.

Table 9.4 comprises the requirements of development services to be rendered by the *Bidder* during the defect liability period.

Table 9.4. The requirements regarding development services for the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 012	M	*The Bidder* shall render change and development services for the *ITSS "CSA".* The change area shall include at least: • changes to the presentation level of the *ITSS "CSA";* • changes to the business logics level of the *ITSS "CSA";* • changes for the data level of the *ITSS "CSA".*
PIR 013	M	As part of change and development services for the *ITSS "CSA", the Bidder* shall carry out the following: receive request for change with the description of functional specifications thereof;

ID	Binding level	Requirement
		develop the *SRS+SDD* afferent to the request and coordinate them with the PSA; render the change and development services in the *ITSS "CSA"* components.
PIR 014	M	Implement the changes and developments at the system level as per the requirements referred in Part "*Change Management*".
PIR 015	M	*The Bidder* shall describe in its bid the proposed model for change management and development request and the methods applied to estimate the effort and price to be submitted to the *PSA.* The information included in the bid shall be sufficient, as well as transparent and correct, to appraise the *Bidder* and *PSA* relationship while rendering the development services.
PIR 016	M	*The Bidder* shall grant development services for the *ITSS "CSA"* as part of operational maintenance and development services for the *ITSS "CSA".* The development services shall include: • amending the existing functionalities of the *ITSS "CSA";* • implementing new functionalities for the *ITSS "CSA".*
PIR 017	M	Any development for the applied software afferent to the *ITSS "CSA"* shall be initiated as per a request submitted by the *PSA*. The request shall be accompanied by functional specifications for the demanded change. The implementation of any changes related to the *ITSS "CSA"* shall go through the change management process agreed with the PSA. To do the changes at the software level, the process shall include at least: • implementation in the PSA testing environment, having performed a unit testing by the PSA; • implementation in the PSA testing environment and carrying out acceptance tests, having involved the *ITSS "CSA"* Users; • implementation in the PSA production environment as per the established change management procedures; • final revision and acceptance of changes.
PIR 018	M	*The Bidder* shall include in its bid 50 man-days for development services to be rendered during the 36 months of post-implementation warranty.
PIR 019	M	*The Bidder* shall include in its bid 50 man-days for development services per year, for the post-warranty period.
PIR 020	M	Additional development services could be requested by the PSA and provided by the Bidder based on additional agreements concluded by the Parties.

9.3. Service level related to the ITSS "CSA"

The level of post-implementation maintenance and support services shall define the requirements regarding the parameters according to which those services shall be rendered by the Bidder.

9.3.1. Support services

Parameters that describe the level of support services:

- **Response time** is the time for the *Bidder* to react to a support request, diagnose the situation and determine the actions necessary to be undertaken to address the issue;

- **Resolution time** is the objective time during which the *Bidder* is expected to take actions in the area of its competence to address the PSA request in full.

The *PSA* requests for post-implementation maintenance and support services shall be classified according to their importance for the *PSA*. The importance for the *PSA* is determined depending on the event impact (produced or eventual) that generated the need to place the request on the quality parameters for the *ITSS "CSA"* operation.

Table 9.5 comprises the classification of PSA requests *depending on their importance*.

Table 9.5. Classification of PSA requests *depending on their importance*

Classification	Impact on quality parameters for application operation
Critical	*Availability*: the IT System is not available for all or most Users. Important transactions are necessary to be performed ASAP (in several hours). *Suitability for use*: key business functions cannot be used. There are no alternative procedures and functionalities. *Performance*: the response time to User's queries makes the IT System operation impossible. *Security*: there are major risks that data confidentiality, integrity or availability would be compromised.
High	*Availability*: the IT System is not available for a large part of Users. Important transactions and operations are necessary to be performed by the beginning of the next day. *Suitability for use*: the use of key business functions is limited. *Performance*: the response time to User's queries affects the key business processes significantly. *Security*: there are high risks that data confidentiality, integrity or availability would be compromised.
Common	*Availability*: the IT System is not available for some Users. There are pending transactions and operations to be carried out within the next three days. *Suitability for use*: the use of System key business functions is limited. *Performance*: the response time to User's queries affects moderately the key business processes. *Security*: there are risks that data confidentiality, integrity or availability would be compromised.
Low	*Availability*: the IT System is not available for few Users. There are no pending transactions and operations to be carried out within the next three days. *Suitability for use*: the IT System business functionality is affected insignificantly. There are alternative procedures and functionalities in place. *Performance*: the response time to User's queries is higher than the regular one. Business processes are not affected. *Security*: there are minor risks that data confidentiality, integrity or availability would be compromised.

When placing a request for post-implementation maintenance and support services, the *PSA* shall set the request classification. The *PSA* shall append brief information to explain that classification. The *PSA* shall be able to reclassify the placed requests, depending on the changes that occurred in the request context.

The Bidder shall render support services during the business days as per the Moldovan legislation in force, from 08:00 through 18:00.

The level of support services rendered by the Bidder shall meet the requirements specified in Table 9.6.

Table 9.6. Duration of addressing the PSA support requests

ID	Binding level	Classification of the request placed by the PSA	Response time	Resolution time
PIR 021	M	Critical	5 minutes	60 minutes
PIR 022	M	High	60 minutes	End of the day
PIR 023	M	Common	24 hours	3 days
PIR 024	M	Low	3 days	The best effort*

**The Bidder* shall make the effort to address the request for services ASAP, working regularly. The time limit for addressing the request shall be communicated and accepted by the PSA. Further changes of the deadline shall be allowed only with the *PSA* acceptance.

9.3.2. Maintenance services

The parameters describing the level of maintenance services for the *ITSS "CSA"* rendered by the Bidder during the defect liability period are displayed in Table 9.7.

Table 9.7. Requirements for maintenance services of the *ITSS "CSA"* during the post-implementation period

<table>
<tr><th>ID</th><th>Binding level</th><th>Requirement</th></tr>
<tr><td>PIR 025</td><td>M</td><td>The Bidder shall apply a policy to minimise the frequency for issuing the application updates. The policy applied by the Bidder shall allow the PSA to use the new updates on a monthly basis, save the updates intended to remove the critical issues and the ITSS "CSA" security updates.</td></tr>
<tr><td>PIR 026</td><td>M</td><td>The Bidder shall apply a non-binding policy in terms of implementing the application new releases. The policy applied by the Bidder shall allow the PSA to use the application new releases every three years.</td></tr>
<tr><td>PIR 027</td><td>M</td><td>The Bidder shall communicate to the PSA its schedule for updates and new releases. For the updates, the Bidder shall notify the PSA at least one month in advance. For the new releases, the Bidder shall notify the PSA at least six months in advance.</td></tr>
<tr><td>PIR 028</td><td>M</td><td>To maintain the ITSS "CSA" in good order, the Bidder can carry out maintenance works at the level of IT System components. The type of maintenance works and the Bidder commitments regarding their coordination with the PSA, the timeframe and duration thereof are set in the Table below:
<table>
<tr><th>Type of maintenance works</th><th>Notification of the Beneficiary</th><th>Timeframe and duration of works</th></tr>
<tr><td>Common maintenance works</td><td>5 days in advance.</td><td>Shall be carried out beyond the guaranteed period of availability for the ITSS "CSA". The duration of works shall not exceed 4 hours.</td></tr>
<tr><td>Major maintenance works</td><td>10 days in advance.</td><td>Shall be carried out beyond the guaranteed period of availability for the ITSS "CSA". The duration of works shall not exceed 24 hours.</td></tr>
</table></td></tr>
</table>

ID	Binding level	Requirement		
		Urgent maintenance works	Notifying immediately as the need for such work evolved.	Shall be carried out any time. The duration of works shall not exceed 2 hours.

9.3.3. Development services

Parameters describing the level of development services rendered by the Provider for the *ITSS "CSA"* during the defect liability period are displayed in Table 9.8.

Table 9.8. Requirements for development services for the *ITSS "CSA"* during the post-implementation period

ID	Binding level	Requirement
PIR 029	M	*The Bidder* shall react to any development request submitted by the *PSA* in three days at most.
PIR 030	M	*The Bidder* shall prepare the budget estimates and the solution design in ten days at most.
PIR 031	M	*The Bidder* shall deliver the solution within the timeframe agreed with the PSA, applying the principle *"the best effort"*.
PIR 032	M	*The Bidder* shall allow the *PSA* to define the priority of development requests and revise them accordingly. This should enable the Bidder to revise also the terms for delivering the solutions.

9.4. Management of Support Services

The manner of organising the support services for the *ITSS "CSA",* including the post-defect liability period, is described in the non-functional requirements displayed in Table 9.9.

Table 9.9. Non-functional requirements for the management of support services for the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 033	M	The Bidder shall render the services to the *PSA*, taking into account the *set of practices of ISO 20000* standards and *ITIL v3.0*. *The Bidder* shall have the capacity to interact with the PSA as per the defined best practices. Likewise, it shall have internal processes and capacities to render the services in compliance with the aforementioned industry practices.
PIR 034	M	The support services shall be rendered based on a SLA to be appended to the Contract signed by the Parties. The Agreement shall determine the level of post-implementation maintenance and support services on the basis of requirements included in this Scope of Work.
PIR 035	M	*The Bidder* shall have a Client Support Centre to receive all the requests submitted by the *PSA*. The Centre work schedule and activities shall ensure rendering the post-implementation maintenance and support services at the level defined in this Scope of Work.

ID	Binding level	Requirement
PIR 036	M	*The Bidder* shall be able to demonstrate the Centre timely access to qualified professionals certified by the producers of delivered applied solutions.
PIR 037	M	There shall be the possibility to provide remote support services. Where necessary, the *Bidder* professionals shall visit the *PSA headquarters*.
PIR 038	M	To render post-implementation maintenance and support services, *the Bidder* shall make available to the *PSA* an applied platform via the Internet. The applied platform shall be properly secured. All the interactions between the *Bidder* and the *PSA* to render post-implementation maintenance and support services shall be carried out via that platform.
PIR 039	M	*The Bidder* shall monitor the quality of post-implementation maintenance and support services and react to any detected deviations to prevent them.
PIR 040	M	*The Bidder* shall submit monthly reports to the PSA regarding the services rendered and their level. The reports shall comprise information on the actions undertaken by the Bidder or those planned with the aim to improve the quality of services.
PIR 041	M	On a quarterly basis, the *Bidder* shall submit the Acceptance Protocol of post-implementation maintenance and support services to the PSA. The Protocol shall contain the amount of work and the sum charged for the services rendered. The Protocol shall be accompanied by a report on the services rendered and their level.
PIR 042	M	The payment for post-implementation maintenance and support services shall be settled on a quarterly basis, after the services were rendered based on the Acceptance Protocol and the report on the services rendered.

9.5. Change Management

All the changes made to *ITSS "CSA"* applications *in the* context of rendering post-implementation maintenance and support services shall be managed as per a mature change management process. Table 9.10 comprises the requirements set for organising the change management for the ITSS "CSA".

Table 9.10. Requirements for change management of the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 043	M	In its offer the *Bidder* shall include information regarding its approach in dealing with change management for applications.
PIR 044	M	*The Bidder* shall suggest the *PSA* the change management procedure related to applications. The procedure shall be coordinated and accepted by the PSA.
PIR 045	M	The change management procedure shall cover at least the following activities to be carried out by the *Bidder*: • testing the changes in the PSA testing environment; • preparing the plan for implementing the changes; • preparing the roll-back plan in case of failed changes; • preparing technical documentation related to changes, including: the purpose of changes, the affected components, Guide for implementation, Guide for using the roll-back plan, Guide for change follow-up;

ID	Binding level	Requirement
		• preparing detailed technical documentation related to changes (the documentation shall include change description, the affected components, installation guidelines, the roll-back plan in case of failed changes, follow-up procedures to ensure proper implementation of changes); • updating the User documentation and technical documentation related to applications and submitting them to the PSA; • delivering software packages related to changes; • delivering the files containing the Source Code afferent to changes (the authenticity and integrity of software packages and Source Code shall be ensured by affixing the Provider's digital signature - code signing); • reacting immediately when errors were detected in the changes implemented and their correction as soon as possible.
PIR 046	M	In the process of *ITSS "CSA"* operational maintenance and development, *the Bidder* shall perform a range of changes related to *ITSS "CSA"* components (system components and applied software). All the changes made by the Bidder in the *"PSA" ITSS* shall be implemented as per a jointly agreed process for change management. The changes that have significant impact on the parameters of quality of the *ITSS "CSA"* shall be authorised by the PSA. The binding elements for such type of changes shall include: • testing in the testing environment; • the plan for implementing the changes; • the roll-back plan; • revise post-implementation services. *The Bidder* shall keep records on all the changes related to the *ITSS "CSA"* in a separate Register of changes. The *PSA* shall have access to read that Register.

9.6. Quality Assurance

The quality of post-implementation maintenance and support services affects directly the operation of *ITSS "CSA"* by the PSA. *The Bidder* shall be able to prove that those services are rendered at the agreed upon quality level. Table 9.11 comprises the requirements regarding the quality of post-implementation support services for the ITSS "CSA".

Table 9.11. Requirements regarding the quality of post-implementation maintenance and support services for the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 047	M	*The Bidder* shall submit, at the beginning of the year, a Quality Assurance Plan for post-implementation maintenance and support services. The Plan shall contain performance indicators for services, the risks that may affect the performance indicators, the preventive actions implemented to manage the risks and the measures aimed to mitigate the residual risks. The Plan submitted by the Bidder shall be subsequently accepted by the PSA. The Quality Assurance Plan shall be revised by the Bidder at least on an annual

ID	Binding level	Requirement
		basis or when significant deviations in service delivery from the defined level have been detected.
PIR 048	M	*The Bidder* shall include in its offer information regarding its approach as a Quality Assurance Plan for post-implementation maintenance and support services.
PIR 049	M	*The Bidder* shall carry out yearly audits of its capacities to render post-implementation maintenance and support services at the established level. The audits shall be conducted by entities that are independent from the *Bidder*. The applied audit methodology shall be aligned with the industry best practices (example*: SAS 70, ITIL, ISACA standards, etc.*). The audit reports shall be submitted to the PSA, together with action plans to remedy the shortcomings found by the Auditor.
PIR 050	M	*The Bidder* shall devise and a Quality Assurance Plan for *ITSS "CSA" operating maintenance services* and maintain it updated. The Plan shall tackle the following categories of risks: **operating risks** (the *Bidder* may lose the capacity to render services at the established level, there could be risks at the level of internal processes of the *Bidder*); **technological risks** (risks that may affect the availability, accessibility, performance and security of the *ITSS "CSA"*).
PIR 051	M	The Quality Assurance Plan must contain detailed information about the identified risks, the measures to be implemented by the Bidder to prevent them, the residual risks and the actions planned should the residual risks occur.
PIR 052	M	The Quality Assurance Plan shall be updated at least annually or upon making any major change in the ITSS "CSA" components, processes related to *ITSS "CSA" maintenance*. *The Bidder* shall submit the updated Quality Assurance Plan to the PSA.
PIR 053	M	When submitting its offer, the *Bidder* shall describe how the Quality Assurance Plan for services will be devised. The offer shall be granted competitive advantage if the *Bidder* appends to it a Quality Assurance Plan, and the latter meets the *PSA needs*.

9.7. Performance Guarantees

The Bidder shall guarantee to render maintenance and support services during the post-implementation period as per the SLA signed with the PSA. Table 9.12 comprises the requirements for guaranteeing the quality of maintenance and support services rendered by the Bidder during the post-implementation period related to the *ITSS "CSA".*

Table 9.12. Requirements for guaranteeing the quality of maintenance and support services rendered during the post-implementation period related to the *ITSS "CSA"*

ID	Binding level	Requirement
PIR 054	D	*The Bidder* shall submit a Bank Guarantee Letter related to the post-implementation maintenance and support services to be rendered at the established level.

PIR 055	D	The bank guarantee sum shall represent 10% of the value of services rendered. The Bank Guarantee Letter content shall be coordinated with and accepted by the PSA.

9.8. Termination of the Contract

When the Parties decide not to prolong the contract for post-implementation maintenance and support services, the *PSA* activity shall not be affected. The *PSA* shall have the possibility to contract another Provider or to take over the *ITSS "CSA"* support and maintenance.

Table 9.13 comprises the requirements related to the conditions for terminating the contractual relations between the *Bidder* and the *PSA regarding* the maintenance and support services for the *ITSS "CSA"* during the post-implementation period.

Table 9.13. Requirements for terminating the contract for maintenance and support services for the *ITSS "CSA"* during the post-implementation period

ID	Binding level	Requirement
PIR 056	M	When it is envisaged to close the contract for post-implementation maintenance and support services, *the Bidder* shall provide at least: • all Source Codes (or configuration files for COTS) related to the *ITSS "CSA"* to the PSA. • the provided Source Codes/configurations shall be those based on which the ITSS "CSA" components were produced and are rolled in the PSA production environment at the time of contract closure (the authenticity and integrity of the aforementioned files shall be confirmed by the affixed Bidder's digital signature); • all documentation afferent to the *ITSS "CSA"* shall be updated and submitted to the PSA; • all records related to PSA requests fulfilled by the Bidder (related to incidents, problems, consulting/advice, changes, developments, etc.) shall be exported in the format agreed with and submitted to the PSA (example*: CSV, XLS*, etc.); • the Bidder shall preserve for a year all the records produced while rendering services, the Source Codes and documentation afferent to the *ITSS "CSA".*
PIR 057	M	Over a calendar year after the expiry of the support Contract, the *Bidder* shall be eager to cooperate with third parties authorised by the PSA with the aim to render post-implementation maintenance and support services to the PSA. To this end, the *Bidder* shall ensure at least delivering any information held that might help improving the quality of services.
PIR 058	M	*The Bidder* shall include in its bid information on the proposed approach regarding the termination of post-implementation support and maintenance services, taking into account the PSA requirements and needs.
PIR 059	M	The Contract signed on the basis of this procurement bid shall last for 12 months. Any of the Parties may require the termination of the signed Contract. To this end, the Party that would like to terminate the Contract shall notify the other Party about its intention at least six months in advance.
PIR 060	M	All the data stored in the DBs related to the *ITSS "CSA"* shall be the property of the *PSA*.