Section 5, Annex 1: Terms of Reference

for the improvement and updating of the "Operational Coordination Center" Information System for monitoring and planning of service activities, its integration with other systems, including maintenance, support and training

No.	Specifications
1.	**Terms used in the terms of reference**
	- SI COC - "Operational Coordination Center" information system; - GIBP - General Inspectorate of the Border Police.
2.	**Requirements related to the development, maintenance and support of the information system to be offered**
	The purpose of the SI COC development and maintenance services is to ensure the achievement of the following objectives for the GIBP: o The functionality offered by SI COC will be aligned over time, depending on changing business needs; o The problems and incidents that will arise in the process of operating the SI COC IT system will be addressed, taken over and resolved in a timely manner, with minimal impact on the users' activity; o The difficulties encountered in the operation of SI COC will be able to be overcome correctly and in a timely manner, without affecting the operation of the IT system. For the achievement of these objectives the Supplier will provide support and maintenance services according to the requirements established in this specification. The supplier will describe the activities that will be carried out by him to respond to these requirements, presenting sufficiently detailed information on how he intends to provide the requested services at the required level. The offer for support and development services is to be based on the best practices in the field of project management and IT service management (example: ISO 20000, ITIL, SM ISO/CEI 14764:2005 - Information technology. Software maintenance, etc.) .
3.	**Support services for the SI COC IT system**
	The support services are provided by the Provider in order to identify and overcome the incidents produced as a result of the exploitation of the SI COC IT system, in order to solve the identified problems and for the correct and efficient use of the SI COC, by the users.

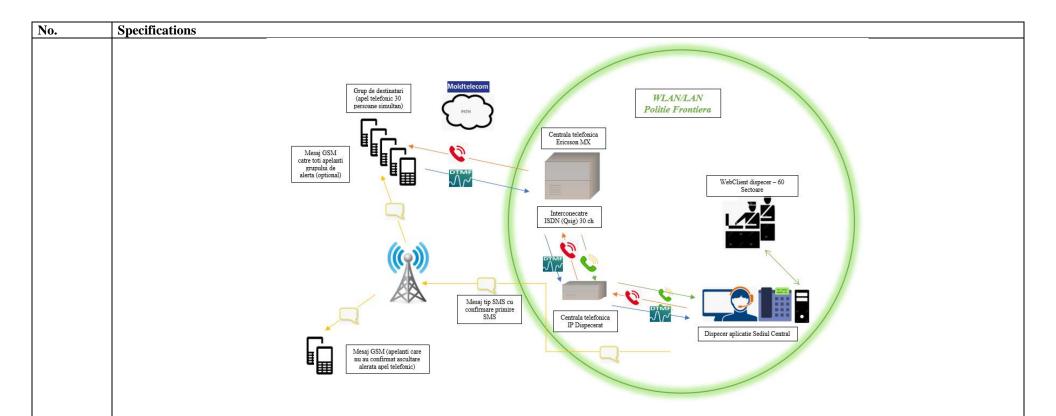| No.	Specifications
	A SI COC related incident is any event that affected or could have affected the normal operation of the IT system. A problem related to SI COC is a cause that led or may lead to the occurrence of an incident. A consultation request is an address from users to the Provider in order to obtain advisory support regarding the use, configuration and maintenance of the SI COC IT system. The support services are intended to ensure the timely use of SI COC at the quality parameters required by the GIBP. The quality parameters for the operation of the System are: • Availability - the ability of SI COC and its components to receive queries from authorized users and to respond in a timely manner to these queries; • Usability - the ability of SI COC to function correctly, delivering the expected services to the authorized users; • Performance - the SI COC's ability to respond to legitimate queries at established parameters; • Security - the SI COC's ability to ensure the confidentiality, integrity and availability of stored and managed data. SI COC support service requirements: 1. The provider will provide support to users in solving SI COC related incidents, arising in the case of normal use of the platform, without unauthorized interventions (example: errors in the application, problems at the level of system software, problems in external applications); 2. The provider will provide support services for solving the problems registered at the application level; 3. The provider will provide advisory support services for the use of SI COC by users; 4. The provider will provide administration services for the CentOS7 operating systems and the PostgreSQL database in the virtualization environment.
4.	**Maintenance services for the SI COC IT system**
	Maintenance services will be provided by the Provider in order to keep the applications up-to-date, with optimal operating parameters. For this purpose, the Provider may come up with updates and changes to the applications, as well as new versions. SI COC Updates are application-level changes, submitted to GIBP by the Provider, intended to improve the performance of the applications, remove problems, bugs and vulnerabilities known to the Provider. New versions (new releases) are software packages related to SI COC, submitted to GIBP by the Provider, which contain all changes previously made at the application level. Additionally, they may contain changes and updates, new application components that were not present in older versions. Maintenance service requirements for SI COC: a) The supplier will provide update services of SI COC and delivery of new versions;

No.	Specifications
	b) For this purpose, the Supplier will prepare the software packages and documentation related to updates and new versions; c) The implementation of all updates and new versions will be carried out according to the requirements established in the point "Management of changes" of these Terms of Reference.
5.	**Development services for the SI COC IT system**
	The development services are provided by the Provider at the request of the GIBP, in order to align the SI COC with the changing needs of the GIBP and related business processes. A modification/development request is an address from the GIBP to the Provider, in order to obtain changes to the SI COC functionalities or to deliver new functionalities for the IT system. A request from the GIBP will be considered as modification/development, only if the requested functionality is not provided by SI COC or is provided differently than requested by the GIBP. The last category does not include requests related to the correction of functionalities that present a problem related to SI COC (according to the definition above). Development Services Requirements for SI COC: 1. The Provider will provide modification and development services of SI COC. The scope of the changes will include at least: - changes for the presentation level of SI COC; - changes for the business logic level of SI COC; - changes for the data level of SI COC. 2. As part of the SI COC modification and development services, the Provider will perform: - receiving the change request with the description of the related functional specifications; - elaboration of the technical project related to the request and its coordination with the GIBP; - making changes and developments at the level of SI COC components; 3. The implementation of changes and developments at the system level will be carried out according to the requirements established in the point "Management of changes"; 4. The Provider will describe in his offer the model proposed for the management of modification and development requests and the methods applied to estimate the effort and the price submitted to the GIBP/IOM; 5. The information included in the offer must be sufficient to assess that the relationship between the Provider and GIBP in the process of providing development services will be transparent and fair; 6. The Provider shall provide development services for SI COC as part of SI COC operational maintenance and development services. Development services will include:

No.	Specifications
	- modification of the existing functionalities within the SI COC;
	- the implementation of new functionalities within the SI COC;
	7. Implementation/adjustment/modification:
	- automated generation of reports according to specific criteria (general report of the activity that includes the flow of state border crossings by people and means of transport, thematic report);
	- implementation of monitoring of radio stations, car GPS, thermal imaging cameras, video cameras, detection and alert devices (Defendec Smardek , photo traps, etc.), body camera, by viewing them depending on the criteria for access restriction to the respective components (by sector/user role);
	- the implementation of a new component for notifying the Border Police personnel, for alerting and notifying the personnel of the Border Police subdivisions;
	- automated generation of reports according to the criteria for calculating forces and means, time tables and service tasks;
	- systematizing the observations of the patrols by date, time, place, sector, map and at the same time making the connection between the incidents/events in which the same person or means of transport participated, the patrol that was at or transited a given sector, the GPS coordinates, the radio station or photo from alert devices, video sequences, with report generation by timeline in Word or PDF;
	- the establishment of the filter regarding the analysis of the in-service planning of forces and means (for each employee and means of equipment separately), the place of organization of the service (border sign and/or segments of the border sector, other landmarks and places), by types of patrols , activities and missions (stationary patrols, mobile patrols, patrol control, State Border verification, working with cooperation partners, genistic planning, etc.) , etc. , but also with the possibility of extracting the information recorded per subdivision following patrol reports (persons data, Name and Surname, document data, etc.) and means of transport observed (brand, registration number, etc.);
	- validation of the incidents to be entered into the SI COC;
	- updating the categories of information contained in the incident files;
	- development of the analysis and reporting module by including some standardized forms related to the necessary statistics, which are to be extracted from the system;
	- migration of depersonalized information regarding border records regarding persons, means of transport or documents detected during the control at the state border crossing;
	- the implementation of the application of the electronic signature on the service provisions, by all the actors foreseen, with the subsequent archiving of the document in the system or by authentication in the system by taking note of the service provision (login) ;

No.	Specifications
	- improving the daily activity record system for each employee in the subdivision;
	- revision of the employee planning process for shifts (3,4,5 or 8 hours);
	- reconfiguring the location of some buttons, as well as the possibility of excluding them;
	- revision of forms already existing in the system (disposition of work, schedule of the day);
	- modification of the access system of SI COC users according to a new algorithm, to "user role" is added:
	1. "shift manager" with personalized "user rights" (viewing the service provision, entering the report upon completion of the service, etc.);
	2. to the user "head of planning" and "deputy head of planning" are added "user rights" access to view the result of the service, from each "service provision" in the archive;
	- modification of some restrictions/processes in the planning system (service provisions, schedule of the day, exclusion of duplications in the daily schedule of R, LS, DT employees):
	- in the case of the employee transfer process, the possibility of accessing the person by the "head of planning"/"deputy head of planning" and including him in the list of personnel of the sector in the "area of competence of the BP" is desired;
	- for employees in the subdivision, the user "head of planning" will have the right to assign/modify the role and passwords for the users "deputy head of planning", "shift head" and "dispatcher";
	- viewing on the map of the itinerary of the patrol at the end of the service, according to the signal from the radio or GPS station;
	- the possibility to grant access to the "dispatcher" user within the sector to the "SI COC" Information System, so that he can view the Service Provisions in electronic format, 30 minutes before the start of the planned patrol service;
	- the development of the "Resource Management" department, by including new functions such as "disciplinary practice, leave records, professional training";
	- the possibility of applying the conventional signs, the tactical situation, as well as with the possibility of modification/deletion on the sector diagram;
	- the possibility to view authentications (IP, login / logout time), with search filter by ID, Name, Role.;
	- the possibility to delete the elements from the "sectors", "crossing points" compartment;
	- creation of a new compartment in the field of strategic management;
	- the integration and interoperability of the SI COC application database, in order to exchange data between the authority and other public institutions (National Police, Carabinieri, General Inspectorate for Migration). The integration of the entire application will be achieved by building intelligent endpoints, which will communicate both with each other and with the endpoints exposed by the systems already implemented within the listed institutions.

No.	Specifications
	8. Any development for the SI COC application software will be initiated based on a request from the GIBP. The request shall be accompanied by the functional specifications for the requested change. The implementation of any change related to SI COC will go through the change management process agreed with the GIBP; 9. For changes to the application software, the process will provide at least: - implementation in the GIBP testing environment of the execution of "unit testing " by the GIBP; - implementation in the GIBP test environment of execution of acceptance tests, with the involvement of SI COC users; - the implementation of the possibility of IS COC testing by GIBP users, as well as their training, in a safe environment, which meets the requirements of the technical and organizational measures for implementing the security and confidentiality regime of personal data, by making available an identical copy of SI COC, which does not contain official data/information with limited accessibility; - implementation in the production environment of the GIBP, according to the established change management procedure; final review and final acceptance of the change. 10. Development services additional to those included may be requested by GIP and offered by the Supplier based on additional agreements signed between the Parties, without changing the amount of the tariffs provided in the offer and maintaining them by aligning with the requirements stipulated in the specifications.
6.	**Development and integration services of the automated notification system for Border Police personnel (ANSP)**
	The need for the ANSP is generated by the requirement for operative intervention of the forces and means of the subdivisions of the Border Police in border crisis situations. The current complexity of the operational information process for BP employees and partner authorities creates a significant difficulty for operational coordination units. Minimizing the reaction time is possible by implementing an ANSP, which will ensure the organizational efficiency and immediate intervention of the employees of the BP subdivisions and partner authorities to ensure the implementation of unitary, coherent and continuous actions and measures: the integrity of the state border; compliance with the legislation in the field; order, public security and the normal conduct of legal activities in the border area and in other areas of interest; the safety of the population; preventing and combating illegal migration, cross-border crime, other illegal acts within the competence of the authorities in the integrated state border management system. The current requirements mainly describe the hardware and software needs of the ANSP for the proposed solutions to be based on the same aspect. However, it is necessary to take into account the need for bidders to rely as much as possible on the hardware, software and network equipment owned by the GIBP, so that in the end the product can be integrated into the Integrated Information System of Border Police (hereinafter SIIPF).

No.	Specifications

1.1. DESTINATION OF THE SYSTEM

The ANSP is intended for the optimization of the information time, in order to alert the staff of the BP subdivisions regarding the issuance of special signals and partner authorities, as well as the transmission of other information of a service nature.

ANSP objectives:
1) creation of a single automated system for alerting BP personnel;
2) reducing the reaction time of BP subdivisions, in specific and border crisis situations;
3) organizing effective collaboration and information exchange between BP subdivisions and partner authorities;
4) ensuring the process of accumulation, systematization, and permanent updating of employee data in order to maintain the ability to react.

The basic functions of the ANSP:
1) the formation of notification informational resources;
2) establishing an efficient automated system for alerting BP subdivisions (at tactical, operational and strategic levels) and partner authorities;
3) organizing the transmission and operational information of BP employees via analog or digital telephone lines, through a voice message;
4) prompt information processing;
5) ensuring the security and protection of information carried out at all stages of accumulation, storage and use of information resources;
6) ensuring the quality of information by creating and maintaining the components of the quality system, based on the procedural approach;
7) the possibility of interconnection with the existing informational resources of the BP;
8) monitoring of the alert of BP subdivisions by hierarchically superior subdivisions and system functionality;
9) record of alerts by period, by subdivision and by name, as well as the possibility of extracting statistical data regarding alerts.

1.2. SYSTEM DEFINITION AND STRUCTURE, CONDITIONS AND REQUIREMENTS OF OPERATION

ANSP will alert and notify the entities in each of the 60 subdivisions through operational coordination units (by levels). The requested system must allow the overall operation according to the block diagram (operational diagram) below:

No.	Specifications

ANSP will allow the following operating scenarios:

(a) Alerting at **the tactical level** - voice and/or SMS (text): in the event of a signal at the tactical level, the operational coordination unit in the sector will be able to generate a signal for all entities (personnel) in the sector through the available dispatcher or web-client software application on a PC (computer), so the staff in the sector will receive voice phone alerts on mobile or landline phones with the type of signal and its severity (green, yellow or red); for warning signals, the coordination operational unit will also send alarms, including SMS on mobile terminals, with the purpose of informing neighboring and hierarchically superior subdivisions, including cooperation partners.

(b) Alerting at **operational level –** voice and/or SMS (text):

-   in the case of a signal at the tactical level, the operational coordination unit in the Regional Coordination Center will be able to escalate a signal to all entities (personnel) of the subdivisions subordinate to the Regional Directorate (sections and services within the Regional Directorate) through the available software or web-client application on a PC (computer), so the staff will receive voice phone alerts on mobile or landline phones with the type of signal and its severity (green, yellow or red); for warning signals, the operational coordination unit will also send alarms, including SMS on mobile terminals, with the purpose of informing neighboring and hierarchically

No.	Specifications

	superior subdivisions, including cooperation partners;
	
	    - in case of a signal at the operational level, the operational coordination unit in the Regional Coordination Center will be able to escalate a signal for all entities (personnel) of one of the subdivisions or several subdivisions of the Regional Directorate (departments, services and Border Police Sectors of the Regional Directorate) through the software or web-client application available on a PC (computer), thus the staff will receive voice telephone alerts on mobile or landline phones with the type of signal and its severity (green, yellow or red); for warning signals, the coordination operational unit will also send alarms, including SMS on mobile terminals, with the purpose of informing neighboring and hierarchically superior subdivisions, including cooperation partners.
	
	    (c) Alerting at **strategic level** - voice and/or SMS (text):
	
	    - in case of a signal at the tactical level, the operational coordination unit in the Operational Coordination Center will be able to escalate a signal to all entities (personnel) of the subordinate subdivisions of the GIBP (directorates, sections and services within the GIBP) through the available software or web-client application on a PC (computer), so the staff will receive voice phone alerts on mobile or landline phones with the type of signal and its severity (green, yellow or red); for warning signals, the operational coordination unit will also send alarms, including SMS on mobile terminals, with the purpose of informing neighboring and hierarchically superior subdivisions, including cooperation partners;
	
	    - in the case of a signal at the operational level, the operational coordination unit in the Operational Coordination Center will be able to escalate a signal to all entities (personnel) of one of the subdivisions or several subdivisions of the BP (GIBP subdivisions, regional subdivisions and GIBP subordinate ones) through the software application or web-client available on a PC (computer), thus the staff will receive voice telephone alerts on mobile or landline phones with the type of signal and its severity (green, yellow or red); for warning signals, the coordination operational unit will also send alarms, including SMS on mobile terminals, with the purpose of informing neighboring and hierarchically superior subdivisions, including cooperation partners.
	
	    - in the case of a signal at a strategic level, the operational coordination unit in the Operational Coordination Center will be able to escalate a signal for all entities (personnel) of one of the subdivision or several subdivisions of the BP (GIBP subdivisions, regional and subordinate subdivisions of the GIBP or Border Police Sectors) through the software or web-client application available on a PC (computer), thus the staff will receive voice phone alerts on mobile or landline phones with the type of signal and its severity (green, yellow or red); for warning signals, the operational coordination unit will also send alarms, including SMS on mobile terminals, with the purpose of informing neighboring and hierarchically superior subdivisions, including cooperation partners.
	
	    All alerting and voice notification telephone calls generated by operational coordination units (tactical, operational or strategic) from the software application or web-client available on a PC (computer) will be made through the technical solution offered, interconnected with the IP telephone exchange of the institution (Mitel MX-ONE) and with the provider Moldtelecom via ISDN PRA(30B+D) Q.SIG protocol – minimum 30 simultaneous channels.

No.	Specifications

The voice alarm and SMS operational coordination unit must present a non-blocking architecture and have the possibility of further interconnection and integration, including its upgrades and extensions, with the integrated information systems of the Border Police, as well as USER-type applications in platforms GooglePlay and IOS.

1.3. TECHNICAL REQUIREMENTS of ANSP (hardware and software)

The following describes the main hardware equipment and software that form the basis of the voice and SMS alarm coordination operational unit:

1.1.1 Server-type computer for ANSP;
1.1.2 Server-type application for ANSP;
1.1.3 Client type application for ANSP;
1.1.4 WebClient type application for ANSP;
1.1.5 IT solution for ANSP interconnection.

1.1.1. Hardware requirements:

Description	Amount
• Desktop type with the following minimum features: • Intel Core i7 processor; • Graphics card Intel UHD Graphics 630; • Memory 16GB DDR4; • Hard disks: 2 x SSD 512Gb • DVD±RW, Media reader 7-in-1; • Ports: USB 3.1 Gen2, 4 x USB 3.1 Gen1; • Video output ports: VGA, DisplayPort and HDMI; • Network port: ethernet / Gbit ; • Operating system: Microsoft Windows 11 Pro 64 bit English; • Monitor: minimum 23" IPS, Backlight , FHD (1920x1080), 16:9, Brightness: 250cd/m2, Contrast Ratio : 1000:1, Response time: 6 ms, minimum viewing angle 178 degrees; • Speakers 2.0 SP-HF160, minimum 4W RMS;	1

1.1.2. Requirements for the server application of ANSP;

No.	Specifications	
	Description	**Amount**
	The application will have the following minimum features: • Operation in licensed Windows 10 operating environment /64 bit; • all-in-one " type : Audio, SMS, email, all in one platform; • Services provided: audio messages to the telephone station, SMS through integration with the application Bulk SMS from provider , recipient email, PUSH notification; • Operation in tandem with the telephone station 30 simultaneous voice channels; • Receives the DTMF signals from the telephone exchange, for establishing the listening times of the alarm messages to the recipient; • Allows up to: 150 audio channels, 8 SMS channels, 8 email channels, 30 PUSH channels (IOS/Android); • Equipment: 30 audio channels, 4 SMS channels, 1 email channel; • Equipment: for sending SMS, email, audio message using multiple platforms: Import from Excel, Read Email, Read SMS, Socket TCT , Socket WEB, Read Serial Port, Read Local File, Read FTP File or add manually by the user; • Equipped with TTS (text to speech) software in Romanian for recording predefined alarm messages or new ones; • Equipped for sending SMS messages (4 simultaneous channels), e-mail, audio message (30 simultaneous channels) to multiple destinations with up to 9000 numbers and 60 call groups of 3 subgroups each; • Equipped to connect at least one operational coordination unit at the strategic level and 59 operational coordination units at the operational and tactical level; • The possibility of upgrading for client-type alarm applications (IOS/Android); • The possibility of upgrading for voice commands (in Romanian) using the phone call; • It allows staggered operation hours according to the time zone established by prefix number.	1

1.1.3. Requirements for the ANSP client application;

	Description	Amount
	The application will have the following minimum features: a) Operation in LAN, Windows operating environment by connecting to the application with username and password;	60

No.	Specifications	
	b) Manage the app:	
	c) General administrator – create/delete/modify user and user types ;	
	d) Tactical level administrator – add/delete/modify the persons and data of subordinate staff;	
	e) Operational level administrator: – add/delete/modify persons and personnel data within the regional subdivision and subordinate subdivisions; – modify the structural scheme within the regional subdivision and subordinate subdivisions by adding a new subdivision or changing the existing structure.	
	f) Strategic level administrator: – add/delete/modify persons and GIBP personnel data; – amends the structural scheme within the Border Police subdivision and subordinate subdivisions, by adding a new subdivision or changing the existing structure; – add type voicemails; – set alarm types: low, medium, high for each Client.	
	g) initiate predefined voice alerts for groups and/or users;	
	h) initiate customized voice alerts through the TTS application or IP phone for groups and/or users;	
	i) initiate predefined SMS alerts for groups and/or users;	
	j) customized SMS alerts for groups and/or users;	
	k) initiate predefined email alerts for groups and/or users;	
	l) customized email alerts for groups and/or users;	
	m) escalate alerts for all entities (personnel) depending on the hierarchical level;	
	n) receives detailed reports on: the listening of the alert message by the recipients, according to the hierarchical level ;	
	o) allows setting a minimum duration of listening to the message so that the message is considered delivered, but not less than 50% of the duration of the message;	
	p) issues detailed and total reports by categories of messages;	
	q) initiate scheduled messages via SMS, Mail, IP phone (Year/Month/Day/Hour/Min/repetitive);	
	r) sets personalized messages according to data from the centralized directory (name, phone, e-mail and personalized information: information 1 , information 2 and information 3;	
	s) set alert groups and destinations.	

No.	Specifications	

1.1.4. WebClient type application for ANSP;

Description	Amount
WebClient dispatcher application will have the following minimum features: • Operation in WAN/LAN through "web access" type connection to the voice and SMS dispatcher application with user and password ; • Three types of alarms available by "typing" directly in the available application: low, medium, high for each Client. Initiation from the web application available from pre-defined voice and/or SMS alarm calls (pre-defined settings per sector functionality) for all users at sector level;	1

1.1.5 ANSP interconnection IT solution;

Description	Amount
IP IT system with TDM capability that will serve ANSP with the following minimum features: • Modular server base type construction with maximum dimensions of 2U in a 19" rack, in which to install the requested equipment interfaces; • Non blocking with a BHCA of at least 99%; • Equipped with a processor with at least Core E500 677 Mhz , 1G RAM, SRAM 512 Kb and SD card for backup of at least 8G and at least two LAN interfaces; • Equipped with IP-TDM conversion interface with up to 250 dynamically allocated channels; • Equipped with at least 2 IVR channels, with the possibility of upgrading up to 80 simultaneous channels in order to extend the solution; • The computer system will be equipped with an integrated switch that supports Layer 2 and port mirroring of at least 8 Gbit ports with dynamic PoE of at least 15 watts/port, QoS ; • It will be compatible with SIP communication standards (Session Initiated Protocol) and H.323 which can offer up to 800 SIP/H.323 extensions in the future; • Equipped with at least 30 standard SIP licenses, for the requested quantity and for communication with ANSP; • To be compatible with the following ISDN BRI and PRI communication standards that can offer up to 150 ISDN channels in the future; • It will include at least one ISDN PRI interface (30B+D) with Q.SIG protocol (slave) for interconnection with	1

No.	Specifications
	the existing Ericsson MX institutional telephone station on at least 30 simultaneous channels; • It will include at least a TAPI 2.0 license (CTI 3party) for the communication of CDR / SMDR information with ANSP; • It will provide CLIP FSK / DTMF facility for external and internal lines; • The IT system will support the function of integrating mobile phones into the system (mobility extensions). Initially, a minimum of 4 licenses will be offered with the possibility of expanding up to 800 mobile extensions; • It will offer the facility of organizing remote video conferences with up to 100 simultaneous video participants; • IP terminal from the same manufacturer will be included with the IT system for native interconnection and good operation, with a minimum 70 x 60 mm illuminated LCD display and a minimum resolution of 165 x 125 px , a minimum of 32 memory keys with LEDs and Keys fast: Diaries, Voicemail , Message waiting, conference, built-in switch with Gb 2-Port, 10BASET/100BASETX/1000BASE-T, Full, Duplex/ Half-Duplex , Auto Negotiation , Codec G.711, G.729A, G.722 (Wideband) , supports headset via RJ11/USB, encryption, system directory 1000 numbers/group directory/personal directory for 600 phones, call history and functional call recording, XML interface - possibility of integration with other applications, 802.1x conversation security: IEEE802.1x Authentication (EAPMD5, EAPOL Forwarding), SIP & RTP Encryption , possibility of integration with Microsoft Outlook
7.	**The level of services related to SI COC (service level)**
	The level of support and maintenance services establishes the requirements regarding the parameters at which these services must be provided by the Supplier. The level of support services The parameters that characterize the level of support services are the following: - Response Time (RT) - is the time in which the Provider will react to a support request, diagnose the situation and establish the necessary actions to be taken for resolution; - Solution Time (ST) - is the objective time in which the Provider is expected to undertake the actions in his area of responsibility to fully resolve the users' request. Support and maintenance requests are classified in terms of their importance to GIBP. The importance for the GIBP is assessed according to the impact (produced or probable) of the event that generated the need to place the request for support services on the quality

No.	Specifications
	parameters for the operation of the SI COC. **Table 1. Classification of the importance of support requests** | Classification	The impact on quality parameters for the operation of applications
Critical	*Availability',* the IT system is unavailable to all or most users. Important transactions need to be completed as soon as possible (from 15 min. to max. 1 hour). *Usability'.* key business functions cannot be used. There are no alternative procedures and functionality. *The performance',* the response time to user queries make the IT system practically unavailable. *Security',* there are major risks of compromising the confidentiality, integrity, or availability of data.
High	*Availability',* the IT system is unavailable for a good part of the users. Important transactions and operations are required to be completed by the beginning of the next day. *Usability',* key business functions can be used to a limited extent. *Performance',* the response time to user queries significantly affects the performance of key business processes. *Security',* there are high risks of compromising the confidentiality, integrity, or availability of data.
Ordinary	*Availability',* the IT system is unavailable for some users. Transactions and operations must be executed in the next three days. *Usability',* the business functionality of the system can be used to a limited extent. *Performance',* the response time to user queries moderately affects the performance of business processes. *Security',* there are risks of compromising the confidentiality, integrity, or availability of data.	

No.	Specifications	
	Low	*Availability',* the IT system is unavailable for a limited number of users. There are no transactions and operations that must be executed within three days.
		Usability', the business functionality of the IT system is insignificantly affected. There are alternative procedures and functionality.
		Performance', response time to user queries is higher than usual. The development of business processes is not affected.
		Security', there are minor risks of compromising data confidentiality, integrity, or availability.

When placing a request for support and maintenance services, the GIBP determines the classification for them. The GIBP will attach brief information to explain the classification performed. The GIBP will be able to reclassify the requests placed, depending on the changes in the context of the requests.

- The supplier will provide support services between Monday - Friday between 09:00 and 18:00;

- The level of support services provided by the supplier and the duration of resolving support requests must correspond to the requirements specified in table 2.

Table 2. Support request Solution time

compulsoriness	Classification of the request placed by the IGPF	Response Time (TR)	Solution Time (TS)
Yes	Critical	4 hours	1 working day
Yes	High	6 hours	2 working days
Yes	Ordinary	8 hours	3 working days
Yes	Low	2 days	Best Effort*

∗ *The provider will make every effort to process the request for services as quickly as possible by operating normally. The time limit for resolving the request will be communicated, agreed, and accepted by the GIBP.*

∗ *Subsequent changes to the time limit are allowed only with the consent of the GIBP.*

No.	Specifications
8.	**Level of maintenance services**
	SI COC maintenance service level requirements : 1. The provider will apply a policy of minimizing the frequency of issuing updates at the application level. The policy applied by the Provider will allow the application of new updates on a monthly basis. Exceptions may be updates intended to remove critical and security issues; 2. The supplier will communicate to the GIBP its schedule for issuing updates and new versions. For updates, the Supplier is to notify the GIBP at least 7 days in advance. For new versions, the Supplier is to notify the GIBP at least 1 month in advance; 3. In order to maintain the SI COC in a functional state, the Supplier can carry out maintenance work at the level of IT components related to the IT system. The type of maintenance works, their period and duration are established and coordinated in advance with the GIBP.
9.	**Level of development services**
	Requirements for SI COC development services: 1. The supplier will react to a development request from the GIBP within a maximum of one working day; 2. The supplier will come with the budget estimates and the solution concept in a maximum of 10 working days; 3. The supplier will deliver the solution in the time agreed with the GIBP, applying the "The Best effort" principle; 4. The Supplier shall allow the GIBP to set priorities for development requests and their subsequent review. The review of the priorities of the requests will make it possible to review the terms of delivery of the solutions by the Supplier.
10.	**Management of support services**
	Requirements for support services management: 1. The provision of services by the Provider will be done considering the ISO 20000 standards and the ITIL set of practices. The provider must have the ability to interact with the GIBP according to established best practices. It must also have internal processes and capabilities to perform operationally according to the practices mentioned in the field; 2. The support services will be provided based on a Service Provision Agreement (SPA), which will be annexed to the Contract signed between the Parties. The agreement will establish the level of support and maintenance services, based on the requirements included in this specification; 3. The Provider will have a Customer Support Center to which all requests from users will be directed. The work schedule and organization of the Support Center's activity must ensure the provision of support and maintenance services at the level established in this specification;

No.	Specifications
	4. The supplier must be able to demonstrate the timely access of the Support Center to certified and qualified specialists by the manufacturers of the application solutions provided; 5. Support services will be provided remotely. If necessary, the Supplier's specialists will travel to the GIBP headquarters; 6. For the provision of support and maintenance services, the supplier will make available to the GIBP an application platform, accessible to the GIBP via the Internet network. The application platform will be adequately secured. All interactions between the Supplier and the Beneficiary in the provision of support and maintenance services will be carried out through the respective platform; 7. The supplier will monitor the quality of the support and maintenance services and will react to the admitted deviations in order to prevent them; 8. The supplier will present reports to the GIBP regarding the services provided and their level. The reports will also contain information on the actions undertaken by the supplier or planned, in order to improve the quality of services; 9. The supplier will submit to the GIBP on a monthly basis the act of acceptance of the support and maintenance services. The act of acceptance will contain the volume and amount of services provided. The act of acceptance will be accompanied by the report on the services provided and their level.
11.	**Change management**
	All changes applied to SI COC applications in the context of the provision of support and maintenance services will be managed according to a mature change management process. Requirements for change management: 1. In its offer, the Supplier will include information on the proposed approach for the management of changes at the application level; 2. The supplier will propose the GIBP the change management procedure related to the applications. The procedure will be coordinated and accepted by the GIBP; 3. The change management procedure must provide at least the following activities under the supplier's responsibility: - testing changes in the GIBP test environment; - preparation of the change implementation plan; - preparation of the "Roll back" plan in case of failed changes; - the preparation of the technical documentation related to the changes, including: the purpose of the changes, affected components, the implementation guide, the application guide of the Roll back plan, the follow -up guide of the changes; - preparing the detailed technical documentation related to the changes (the documentation will include the description of the

No.	Specifications
	changes, the affected components, the installation instructions, the rollback plan in case of failure, the follow-up procedures up to ensure the correct implementation of the changes)',
	- updating the user documentation and the technical documentation related to the applications and submitting it to the GIBP;
	- providing the software packages related to the changes; providing the files containing the source code related to the changes (the authenticity and integrity of the software packages and the source code must be ensured with the application of the supplier's digital signature - code signing),
	- immediate reaction in case of detection of errors in the implemented changes and their correction in the shortest possible time;
	4. In the process of operational maintenance and development of the SI COC, the Supplier is to carry out a series of changes at the level of the related components of the SI COC (system components and application software). All changes made by the Bidder at the level of the System will be implemented according to a jointly agreed process for change management. Changes that may have a significant impact on the quality parameters of the SI COC service will be authorized by the GIBP. Mandatory elements for this type of changes will be:
	- testing in the test environment; the change implementation plan;
	- Roll back plan; post-implementation review.
	The supplier will keep track of all changes related to SI COC in a Register of changes. GIBP will have read access to this Register.
12.	**Other criteria and requirements**
	The supplier must guarantee the provision of the maintenance and support services granted according to the maintenance and support contract signed with the GIBP.
	If the parties decide not to extend the contract for support and maintenance services, the work of the GIBP shall not be affected. The GIBP must have the ability to contract with another Provider or take over internally the support and maintenance of the SI COC.
	Requirements for termination of the contract for the provision of maintenance and support services:
	1. If the contract for support and maintenance services is expected to be terminated , the Supplier must ensure at least:
	- all related SI COC source codes are transmitted to the GIBP;
	- the transmitted source codes/configurations must be those on the basis of which the SI COC components were produced that are run at the time of termination of the contract in the GIBP production environment;
	- all related SI COC documentation is updated and sent to GIBP;
	- all records related to GIBP requests made on the part of the Supplier (for incidents, problems, consultancy, changes, developments, etc.) are exported in a mutually agreed format (example: CSV, XLS, etc.) and sent to GIBP;

No.	Specifications
	- The supplier will keep for a period of one calendar year all the records produced during the provision of services, the source codes and the related SI COC documentation; 2. For a period of one calendar year after the expiration of the support contract, the Supplier will be willing to cooperate with third parties authorized by GIBP, in order to provide support and maintenance services to GIBP. for this purpose, the Provider will at least ensure the provision of any information held that would help improve the services; 3. The supplier will include in its offer information regarding the proposed approach for the termination of support services and maintenance, taking into account the requirements and needs of the GIBP; 4. The contract signed on the basis of this tender is to be for a period of 7 months. Any of the parties can at any time request the termination of the signed contract. For this purpose, the party wishing to terminate the contract shall notify the other party of its intention at least 3 months in advance. The final product (SI COC) consists of the software and documentation artifacts of the system as well as the knowledge transfer to the system owner and administrator. Artifacts delivered for SI COC: a) The complete source code of the modules and components necessary to compile the delivered program product; b) The final product packaged for easy installation in the proposed technological environment; c) Updated and completed technical task; d) Modifying and supplementing the User's (Content Administrator's) manual; e) All materials related to the training of SI COC users; f) All artifacts copied on electronic media.
13.	**Server-type processing and storage unit for SI COC**
	The equipment offered as part of the purchase must be new, high-quality, mass-produced, from renowned manufacturers, well-known internationally in the IT field. The equipment configuration must consist of components from the same manufacturer and ensure optimal operation.

compound	Minimum required parameters	The amount
Type	International brand name	
Type	Rack mount 19", 1U, SFF	1
Processor, min	2 x Base frequency: 2.10 GHz, Turbo Boost 3.30 GHz, 12-Core/24-Threads/120W, Cache 18 MB L3	
RAM, min	8 x 16GB (1x16GB) Dual Rank x4 DDR4-3200 CL22 Registered ,	
HDD, min	2x 960 GB SSD RI, 2 x 1.2 TB SAS 10K HDD factory pre-installed, Hot-Plug	
Raid Controller	RAID 0, 1, 10 - Storage interface (SAS/SATA), 16 SAS lanes , 12Gb/s SAS, 6Gb/s SATA	

No.	Specifications	
		technology ; 2x 16Gb FC port HBA adapter , pre-installed at the factory
	Management	Remote Configuration/Monitoring, via network. Support Redfish , IPMI, Telnet , SSH, DCMI, NTP, Web-based GUI, GUI rendered in HTML5, DHCP, VLAN tagging , Dynamic DNS, OS pass-through , Role-based authority , Local users , SSL encryption , Directory services (AD, LDAP), Two-factor authentication , Single sign-on , Secure UEFI boot , Virtual Media, Remote File Share , Remote agent-free update , Auto-update , Embedded update tool , Auto-Discovery, Remote Syslog
	LAN, min	4x 1Gb ports note occupy PCI port, 4x 10Gb BASE-T, 1 x Management port
	Software license	Windows Server 2022 Standard, Microsoft SQL Server 2019 Standard
	PSU, min	2 x 800W Hot Plug, Redundant
	Accessory	1U Sliding Rails with Cable Management Arm
	guarantee	Minimum equipment warranty 36 months.
14.	**Other requirements towards the bidder**	

The offer must contain the detailed hardware and software configuration that must include at least the equipment to be integrated as well as the IT programs (solutions) to be installed.

The tenderer will guarantee that, through the solutions and the volume of work foreseen, he will create a complete functional assembly, designed and executed on the basis of the latest technologies and ensure all the elements necessary for the good, safe and normal operating behavior of the ANSP, under the operating conditions defined in this Specification for an operating cycle according to the contract.

The bidder must present an integrated, turnkey solution, which includes: supply of the necessary equipment (hardware, software, including licenses), installation, verification, commissioning, application development, user training, maintenance manuals, operation, operation and maintenance.

The bidder will demonstrate its technical ability to provide and install the requested solution through certificates from manufacturers/suppliers, through certifications from integrator partners who have provided and installed at least a solution similar in functionality, presenting in this regard a recommendation from the end customer of solutions at national or European level.