IT Solutions Designed for the Management of Activities in the Romanian Public Institutions*

Adriana-Meda UDROIU[1]*, Ştefan-Antonio DAN-ŞUTEU[2]

[1] ROTLD Department, National Institute for Research and Development in Informatics, Bucharest, Romania
meda.udroiu@rotld.ro (**Corresponding author*)

[2] Strategic Command Department, "CAROL I" National Defence University, Bucharest, Romania
dan-suteu.antonio@unap.ro

Abstract: This paper presents an extended research in the field of optimization intended for organizational processes undertaken by the Romanian public entities. Among other objectives, this paper aims at developing the main components (modules) of an integrated information system designed for the management of activities (*IISMA*), that would enable Romanian public institutions to better manage the ever increasing flow of information by making use of their own resources and specific activities, as well as the functional software modules and the open-source applications. The system is flexible, versatile and transparent in terms of access and location of information, data replication and updating in distributed databases, control procedures, transfer of data, ensuring the feedback for a continuous comparison and evaluation of the actions undertaken in relation to what has previously been planned. *IISMA* is based on open - source solutions and functional software modules, which aim to reduce the complexity of the conceptual separation between strategic decision and operational activities.

Keywords: Integrated information system for management of activities, Public institutions interoperability, Open-source solutions, Modelling platforms.

1.Introduction

Public institutions are currently using hybrid systems and heterogeneous IT solutions for the management of information flows and specific activities. The lack of a comprehensive approach and a technical as well as procedural interoperable architecture has negative consequences for the economic and functional performance of state-owned institutions. That is why we consider it necessary to design, test and implement an integrated management system for the activities of these institutions. The system must ensure the automation of the management of the processes, activities, resources, programs and projects of that institution. The integrated IT system must also ensure the automated management of the internal information flow, data and documents security, as well as a uniform framework for the management of information and reports, providing the possibility for establishing a common agenda between specific entities. Also, the integrated information system must ensure the automation of business management in parallel with the informational flows of the organization.

The modern society (4.0 society) requires the interconnection and interoperability of information systems in public institutions, as enablers for the good governance of the state (Van Dooren, 2016). The problem is important because it ensures the implementation of the digital governance of the Romanian State, rapid access to information and, implicitly, to an accelerated economic development.

At this moment, the information systems of public institutions have a complex structure, with various degrees of development, dependent on the level of allocated resources and in line with the concepts of command and control, operational needs and technological level. Their current structure is based on a set of subsystems and components (in operation or in development) which are at different levels of implementation.

This paper sets out to describe an integrated information system - from here forward referred to as IISMA and its main architecture module designed for the management of activities performed by the Romanian sector entities.

The next section of this paper describes the main elements of the IISMA, the functional architecture, the organizational structures and, most important, the roles associated with business processes within the system.

The third section of this paper describes the most important modules of integrated information system with activities, methodologies which describes the

* This paper enlarges on earlier research presented by Udroiu M, Dumitrache M, Sandu I., Brezulianu A, in their joint paper titled Implementing an Integrated Information System Designed for Romanian Public Entities, published in Studies in Informatics and Control, ISSN 1220-1766, vol. 27(3), pp. 369-376, 2018, https://doi.org/10.24846/v27i3y201812. The current paper presents several new elements such as the modelling concept and methodologies for two out of ten functional modules, i.e. Identity Management and Access Rights Module and Institution Resource Module, which belong to an integrated information system designed for the management of activities (IISMA) in the Romanian public sector.

specific actions in the system. The figures (print screens) presented in the paper show the modelling of business processes for each module.

At the end of this paper, there is a section named Discussion, which describes the results of modeling and another one named Conclusion, which summarizes the IISMA implementation.

2. Integrated Information Systems (IIS) in public institutions

The integrated information systems of public institutions will provide the information infrastructure and services, as well as the information security for the purpose of supporting command and controlling functions under effective operational conditions and economic efficiency (Cordella, A., Iannacci, F. 2010).

In order to allow the fulfilment of the specific tasks of each institution, the system must provide services that are safe, stable, protected and continuous, irrespective of the geographical location of each user structure.

The way in which these integrated information systems for public institutions can be implemented depends on their level of commitment to mitigate the limitations identified in the information systems they currently operate.

The integrated information system (IIS) must be able to acquire/receive data from multiple sources and in various formats, to ensure the processing, storage, sharing and circulation of information and information products, while ensuring their physical and logical security (Lyytinen, K., Damsgaard, J. 2011). It is required for the IIS to be interoperable and integrated with the command and control system of the structure served so that the two systems can exchange data, information and services in order to streamline the management process at an organizational level and maintain accountability of resources used at a given time to meet the assigned objectives (Fig.1).

The integrated information system for the management of activities must be designed in such a way that it would be able to ensure the information security flow, in accordance with the good practices in the field, providing: system access for authorized users; confidentiality, integrity and availability of resident and mobile data and information; non-repudiation of access and protection of the system and users against hostile information technology attacks.

As presented in Figure 1 and in the two mentioned paper (Udroiu M, 2019 and Dan-Suteu, 2015), IISMA will receive and process information from all systems involved in the command and control act (C2), in various formats. IISMA must be interoperable and integrated with the command and control system in order to be able to offer the best decisions.

In public institutions it is very important that the decision-making act can be based on the processing of all information both in the external environment and from the internal environment of the institution.

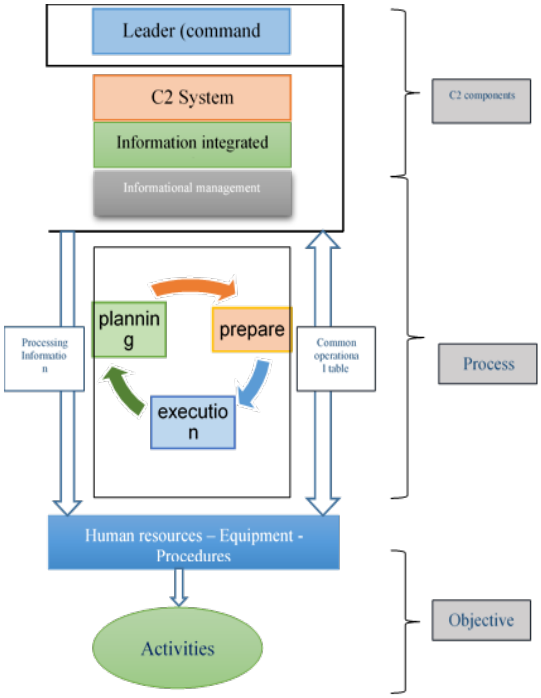

Figure 1. The role of IISMA in the C2 Process (Udroiu M, Dan-Șuteu, Ș.-A, 2019)

2.1 The Functional Architecture of IISMA

In order to achieve the objectives of the research work and to ensure the results, versatility and future development capability, the functional blocks of the platform are structured in 10 modules. These modules are described in detail in the paper "Implementing an Integrated Information System Designed for Romanian Public Entities" (Udroiu et al, 2019):

M1. Module for integrated management of identity and access rights. Unique authentication system

M2. Module for management of processes, procedures and activities

M3. Module of management of programs and projects of the institution

M4. Institution Resource Management Module

M5. Module of document and communication management

M6. Maps (GIS)

M7. Analytics and dashboard (BI)

M8. Notification

M9. Monitoring platform technical parameters

M10. Monitoring platform availability

The above-mentioned modules are presented because the current paper describes the software modeling and simulation of these and their implementation in the IISMA.

3. The Description of Modules

The following paragraphs describe the most important modules which compose the complex architecture of IISMA. The description of these modules contains the main elements and the activities associated, the methodologies and modeling tools used to implement the activities described. Also, this section lists out all use cases for the main activities and a short description of them.

3.1 Identity Management and Access Rights Module (IMARM)

This module provides a unified management of the user accounts, authorization rules, and secure multi-factor authentication mechanisms at platform level.

IISMA ID will be implemented through the WSO2 Identity Server (A guide to WSO2 Identity Server, 4/2019, https://wso2.com /identity-and-access-management) product and will have the role of identity provider across the integrated system and will represent the unique authentication point in the IISMA system.

It is the only module that will operate with user authentication data, and with each of their access roles, respectively. User data will be managed in the IISMA ID's own database but will also provide the possibility of federalizing other Identity Provider services via the SAML protocol (Hughes al all, 2005).

An Open LDAP (OpenLDAP, 2019, https://www. openldap.org/) directory will run in active cluster mode and will be used for internal identity management. The identity server will be able to federate any existing LDAP-type (e.g. Active Directory) directory in the system user's infrastructure as well as other pre-existing "Identity Provider" services capable of interacting through the SAML protocol.

The use's cases list is presented below:

Table 1. Uses' cases list for Identity module

Case	Name	Description
UC1	Register user database	Allows the definition of a user source to be used by the identity provider in the authentication process. Sources can be relational databases, Active Directory-type systems, or other directory systems accessible by the LDAP protocol (s).
UC2	Defines validation processes	Allows the definition of business processes, multi-stage, usable for approving the creation or modification of a data structure while data operates the identity provider (user, role, permission).
UC3	Assigns validation process to operation type	Allows you to enable the application of a specific approval logic for a specific operation specific to the identity provider (Create/modify/delete user, create/change/delete access role). Once activated, those operations shall only take effect after the process has been activated.
UC4	Creates role	Enables the creation of user-associable security roles
UC5	Changes role	Allows you to assign access permissions to the security role.
UC6	Deletes role	Eliminates a security role.
UC7	„Identity Provider" Configuration	Allows you to configure the identity provider type service.
UC8	„Service Provider" Configuration	Enables the registration of a service provider-type service at the identity provider level.
UC9	Creates user	Creates the user and stores the data in the primary database associated with the identity provider system or in another registered user base and Read-Write access. The process is subject to approval to produce results.
UC10	Changes user	Changes an existing user, default access roles. Process subject to approval to produce results.
UC11	Deletes User	Removes an existing user. Process subject to approval to produce results.
UC12	Validates operation	Operation by which an action to create, modify, or remove a user-type data structure or access role is approved.
UC13	Consults operations log with user accounts	Allows you to consult operations history on user-type entities, access roles.

IISMA modules will be registered at the identity server level, IISMA-ID, as "Service Provider" entities.

The communication between "Identity Provider" and "Service Provider" will be achieved through SAML (Hughes et al., 2005) messages, digitally signed and encrypted, providing the privacy and non-repudiation of messages in a two-way transmission between "Identity Provider" and "Service Provider".

The following settings for obtaining privacy and non-repudiation SAML messages transmitted between "Identity Provider" and "Service Provider" will also be made in the registration process:

- Generate an X509 certificate consisting of public key and private key for each IISMA module registered as "Service Provider"

- Registration of the private key for the above-mentioned X509 certificate for which IISMA module is registered as "Service Provider". It will be used for the digital signing of SAML authentication request messages submitted to IISMA-ID; it ensures non-repudiation of messages submitted by "Service Provider" modules to "Identity Provider";

- Record the public key of the X509 certificate for each "service provider" within the IISMA -ID module to encrypt SAML messages of response for the authentication request by means of IISMA-ID. These messages will only be decrypted by "Service Provider" IISMA module, via its private key;

- Configure the public key related to the IISMA-ID for each IISMA module registered as "Service Provider". The IISMA module will encrypt messages sent to IISMA ID with the public key of IISMA-ID, and only IISMA-ID will be able to decrypt the message using the private key maintained on the IISMA-ID server. It ensures the confidentiality of communication from "Service Provider" to "Identity Provider".

The authentication methods are specific to each "Service Provider" registered, i.e. different authentication schemas can be configured for each "service provider".

The authentication scheme represents the chain of authenticators which must be applied in order to validate the user's identity.

The following types of authenticators can be used:

1. Login with username and password;
2. Authentication with digital certificate;
3. KERBEROS authentication (Windows Authentication).

Regarding digital certificate authentication, the digital certificate validity check is envisaged by integrating with an existing Online Certificate Status Protocol (OCSP) server within the institution, i.e. CRL (Certificates) Revocation List).

The authentication (login) scheme includes the following steps:

1. The user accesses the "Service Provider" system;
2. The "Service Provider" system checks the user's authentication status, and if it is not authenticated, redirects it to the identity service, IISMA-ID;
3. The identity server applies the authentication methods configured for the service provider (password, certificate, etc.). After the successful authentication is achieved at the Identity provider level, a digitally signed and encrypted SAML message is generated. Then, the message is forwarded to the service provider;
4. The "Service Provider" system decrypts the SAML message, checks the digital signature, extracts authenticated identity data, and provides user access to system resources in accordance with access rules.

The logout scheme includes the following steps:

1. The "Service Provider" system receives the "Logout" command and redirects the command to the "Identity Provider" for generalized logout.
2. The "Identity Provider" system runs logout in its system after calling the logout link for the service from which the logout process was initiated. This is how you obtain SLO (Single Logout.)

At the identity management level, the IISMA HR and IISMA LOGISTICS modules have been included for the use of the integrated authentication service via SAML protocol.

Figure 2 presents the authentication service through management console of WSO2 Identity Server. For each module authentication is performed by a specific code (name pattern).

The HR module and LOGISTICS module are part of Institution Resource Management Module, described below.

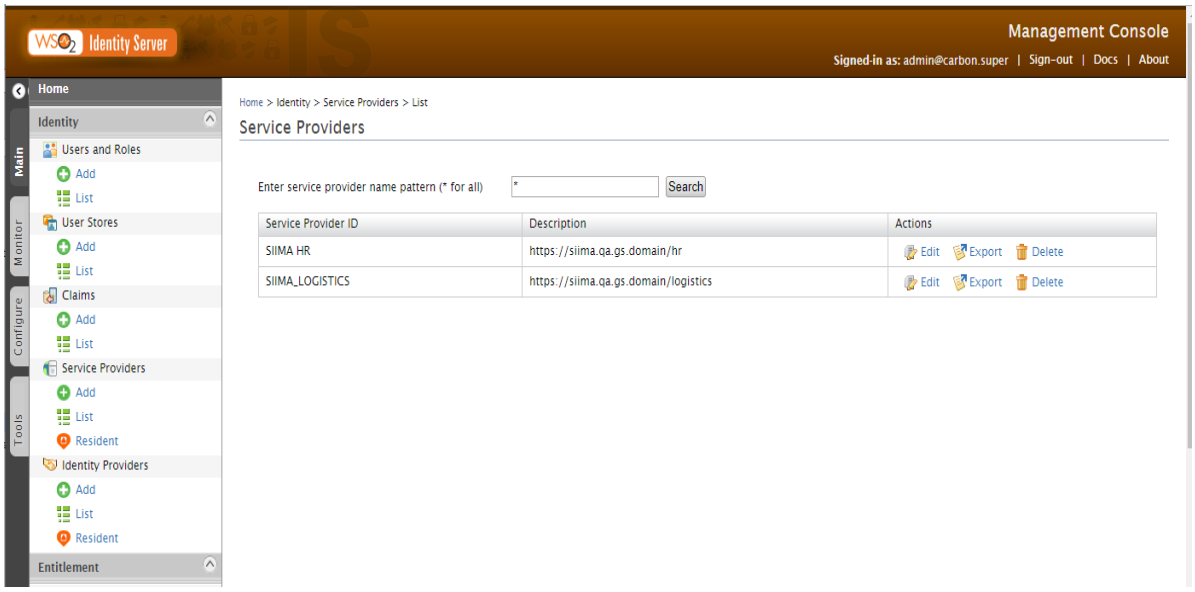

Figure 2. Integrated authentication service for HR and Logistics Modules

3.2 Institution Resource Management Module (IRM)

This module includes several submodules which manage all the institutional resources such as: human resources, logistics resources, stocks, productions and so on. Thus, the following submodules are part of IRM:

1. The modelling of the resource and ranker types allows the modelling of different institutional resources (products, fixed assets, assets, management, locations, partners, etc.)
2. Material and financial planning deals with planning, setting and monitoring budgets for revenue and expenditure, and procurement programs
3. The Treasury facilitates logical structuring and tracking of all monetary transactions and other assets, financial and cash flows.
4. Marketing supplying and acquisitions allow registering purchase requisition, orders and purchasing processes
5. The inventory gathers and stores information about the inventory movement, based on input / output documents approved through M2 specific processes.
6. The production facilitates management of recipes and means of production, operational and production costs
7. Logistics enables registration of administrative and logistic support activities, planning of administrative, maintenance and support activities, and deployment of logistic resources
8. Human Resources allow the description of posts, the definition of job descriptions, staff specifications, the formation of organizational structures, and hierarchy.

At this time, for the beneficiary of the project it is very important to model the modules of human and logistic resources, as presented below.

3.2.1 The Human Resource Management Submodule

This submodule manages the following elements:

- the organizational structure of the institution;
- the list of functions related to each department;
- the structure of the job description for each function;
- the nomenclature of qualifications and responsibilities that are included in the job description, i.e. the structure and data in the employee's staff file;
- the list of functions that meet certain criteria relating to the imposed requirements;
- if there are employees from a department who cumulatively meet a set of parameters mentioned in the personnel file (courses, qualifications, licensing, authorizations, etc.);
- the list of employees in a particular department (required for the planification module). The DEP-OWNER user has access to the list of employees under his control, to whom he can assign for operation stages of business processes. Through the authorization process, users with a DEP-

OWNER top-level role can have access to all the functions of their subordinates.

Integration will be achieved through the integration platform, and WS-SECURITY secure web services.

The organizational structure will be administered by the "Human Resources" department.

Each function within the organization chart will appear as busy or not, highlighting unfilled posts.

The job description is an information structure associated with the function. It consists of a set of responsibilities that will be selected from a nomenclature which will standardize these responsibilities, by codifying them in a unique way. Such structuring of the post sheet facilitates the process of retrieving the right human resource for carrying out project activities.

The task and responsibility nomenclature are used to create job descriptions and queries regarding the availability of a human resource that cumulatively performs a set of tasks, and the responsibilities associated with the requirements of a project activity.

It includes the following information:

- Code – unique identifier of the task;
- Name;
- Description.

The initialization of this nomenclature is allowed from the CSV input files.

Each employee assigned to a position in a department will be defined as a staff file. In case the employee has worked before in that institution, the previously created staff file will be reactivated. A unique identifier will be assigned to the staff folder.

The structure of the staff file contains a set of standardized sections specific to the employee's personal data, as well as a series of registry sections that can be supplemented in the future as needed. Thus, the standard structure of the staff folder contains the following sections:

- Personal data (e.g. mark, name, surname, personal identification number, date of birth, place of birth, address);
- Identity documents – CI, Passport;
- Study papers – represents a register in which all the employee's study papers will be recorded, along with the scanned version of the document.
- Administrative changes (commitment / recommitment suspension, secondment, liquidation):
- The Register of work experience – contains information on cumulative/ or detailed working seniority from the previous workplaces:
- Increases – a record for each type of increase granted to the employee (e.g. seniority).
- Holidays
- Sanctions

The system will allow the maintenance in the archive of data relating to people who are no longer part of the institution. Their file corresponds to one of the following states:

- Active employee;
- Suspended employee;
- Posted employee;
- Employee out.

A CV section will be added to the employee's file and the updated CV will be maintained in this section. The updating of the CV is done automatically, by setting the validity of the CV, notifying the user about the need to update the CV, launching a business process for updating your CV.

From a technical point of view, the human resources software module will be able, through the API interface, to recover the posts in the system based on lists of skills, courses, certifications, authorizations, licenses, entered as filters. Therefore, such an interpellation will indicate the number of posts that meet the filter conditions, grouped by departments. For project management, this represents the start of initiating the process of allocating human resources at the activity level. Requests will be addressed by project managers to all departments that have competence in the project.

Document template management allows the DOCX document management, used as a template for generating the printable version of the resulting documents. For example: Seniority Cover, Workplace Seniority Certificate, Advancement Notice Form. There is no limit to the number of templates, and other uniquely identifiable templates can be recorded by a code. Then, to generate the export of the document, the template code will be referenced as a parameter in business processes.

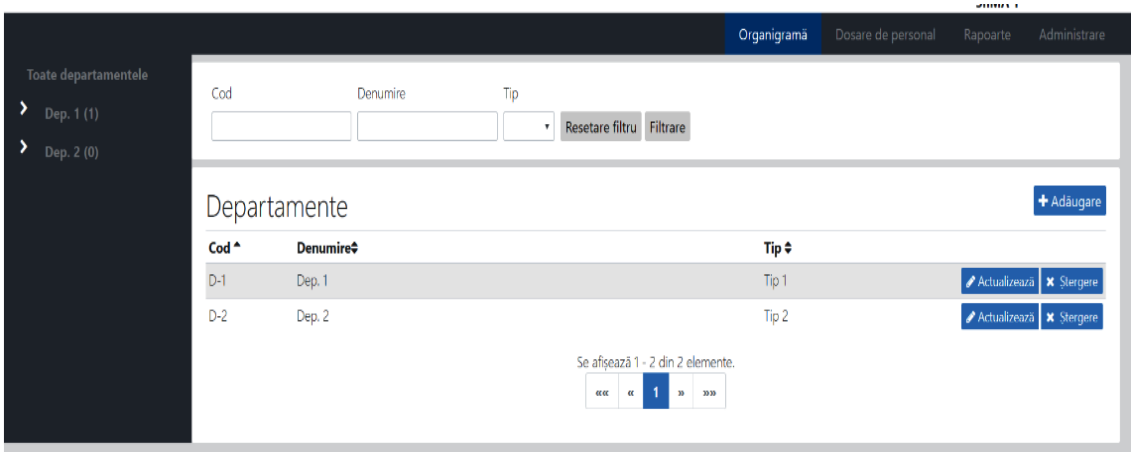

Figure 3. Organization chart – level 1

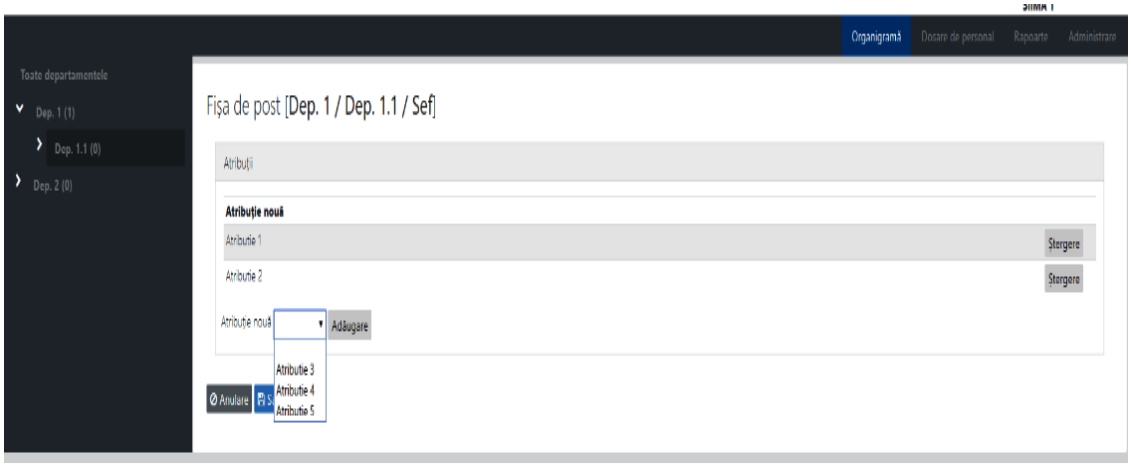

Figure 4. Task definition for job description

Modelling these parameters of the Human Resources module, using the Gitlab (https://about.gitlab.com/) platform, with PostgreSQL databases (https://www.postgresql.org/docs/10/datatype-json.html) and a Drag&Drop Utility makes it possible to achieve the following interfaces at the end user level.

Figure 3 presents an example of organization chart of all departments in a public institution. Each department are associated a code, name, type and a series of filter associated. For each department, a human resource is developed and for each employee, the staff folder is created.

Figure 4 presents the task definition for job description. The job is described through some parameters which represents a set of responsibilities for each function.

In figure 5 it is presented how to complete the personnel folder. The folder for each employee is completed by the Human Resource Department and consist the data which define the person (name, surname, personal identification number and so on).

Figure 6 presents administration of data through document templates.

All the figures illustrated above are in Romania language because this system (IISMA) is used by Romanian Public Entities and all of these modules must be in Romanian language. These figures are used to exemplify the information provided in the text.

3.2.2. Logistic Resources Management Submodule (LRM)

This submodule defines the types of logistic resources and the parametric data for each type of resource.

To facilitate the editing or selection of the values of the parameters of the logistic resources, the

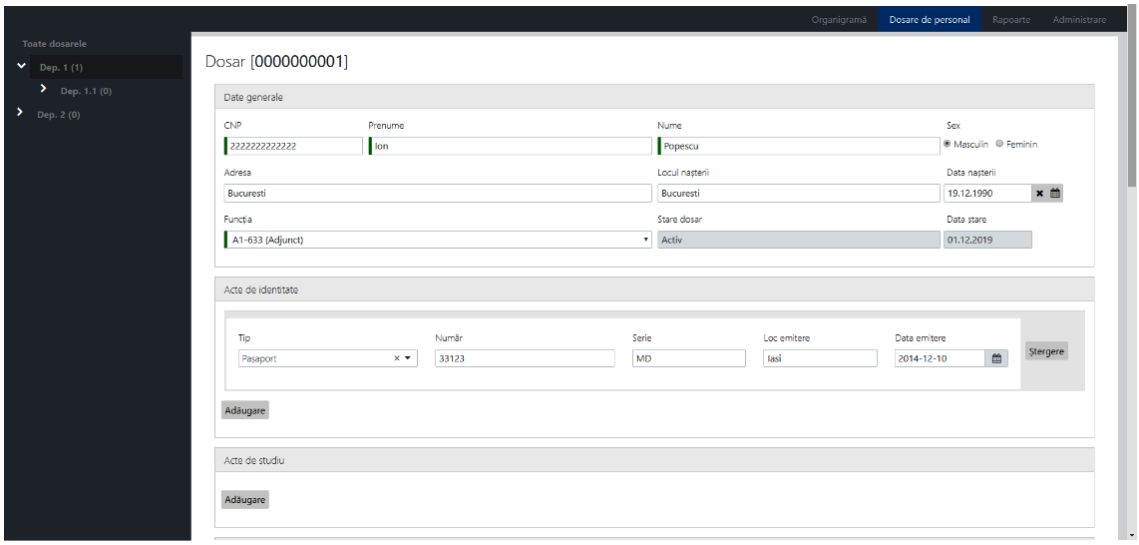

Figure 5. Edit the data in the personnel folder

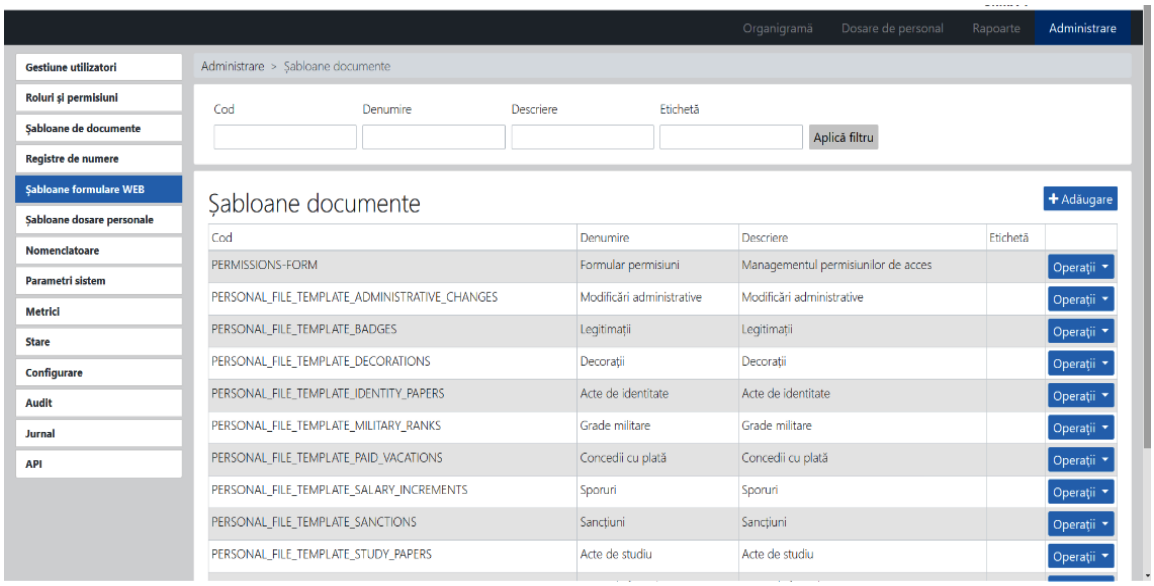

Figure 6. Administration of data

value nomenclature that defines the code, value or name will be dynamically defined. Thus, for parameters such as model, category, etc. the range of values is given by the list of values of a predefined nomenclature.

The characteristic parameters of the types of logistic resources are following:

- Integer or comma;
- String;
- Date / Date and time;
- Truth value (true / false);
- Predefined list or existing nomenclature.

Each type of logistics resource is assigned to a life cycle, which is the sum of all the states through which the resource passes. The life cycles of logistics resources are very similar to the definitions of business processes, the difference being that the life cycles are always sequential (without parallelistic possibility), a resource being in one state at a time.

The Changing of the business process which validates the operation.

The functional blocks in this submodule are:

- The types of logistic resources – this functional block allows the definition of the logistic resources.

- Nomenclature technical parameters – this functional block allows the definition of the nomenclatures used for selecting the values of technical parameters.
- The inventory of the logistic resource – presents the list of all active logistic resources, with the possibility of retrieving and accessing the resource card.
- The logistic resource card – allows the user to consult the technical parameters of the logistic resources, the calendar of availability, the business processes in which he/she was involved in the past and the business processes in which he/she is involved at this moment, respectively.
- Logistic resource requests – this functional block presents a list of business process instances requesting the allocation of a type of logistic resources with certain constructive parameters for a certain period of time with the aim of using it in a project. It also allows the user to generate a list of resources in the inventory, available during the requested period and which cumulatively meets the specified criteria. Allocating a logistic resource affects its availability calendar. An allocated resource can be withdrawn or replaced from the process.
- Internal processes – represents internal, departmental, specific business processes for the logistic departments (e.g. Revision process, Repair process, etc.).

In term of modelling, the following items should be defined:

- Types of logistical resources (for each of them the dynamic modelling form of the logistic resource properties is used)
- Types of management – represents all types of logistical resources with which the type of management operates
- Management – representing the management courts (Stocks) – with specific operations (reception, consumption, transfer)
- Nomenclatures specific to logistic processes
- Numbers register – to obtain unique document numbers

From an operational point of view, it allows:

- Registration of Input/Output documents
- Stocks consultation
- Consultation of the management object sheet

The use's cases list is presented below:

Table 2. The use's cases list (LRM Module)

Case	Name	Description
UC1	Defines types of logistics resources alongside with their technical characteristics	Represents the data model of the logistic resource. It also contains validation criteria for the mandatory parameters to be filled in, i.e. the range of values from which it can take values
UC2	Defines technical parameter nomenclatures (structure and data)	Creates new nomenclatures, updates existing nomenclature data. The values will be selected from the list in order to set the technical parameters of the logistics resource.
UC3	Records logistics resources by completing characteristic parameters of the resource type	Represent skilled instances of logistic resource in inventory. It shall be accompanied by the inventory number of the logistic resource.
UC4	Uploads technical documents associated with the logistic resource	Allows the association of technical data sheets of the logistics resource.
UC5	Consults and downloads existing logistic resource data/documents	Allows the user to view the technical data and consult the technical data sheets associated with the logistics resource.
UC6	Searches for logistic resources by type, technical characteristic parameters of the type of logistic resource, as well as by its availability range.	Allows the user to retrieve logistic resources. It is possible to determine the resources that have exceeded the due date.
UC7	Allocates a logistic resource following a request generated by module M2 for the purpose of using it in a project	The requests come from the M3 module. The request is resolved by identifying the resources available.
UC8	Records its current technical status, i.e. the time required to refreeze the resource if it is defective	Allows signaling the periods of unavailability of resources.
UC9	Records future unavailability periods as a result of the planning of maintenance/ overhaul/repair operations.	Allows the planning of re-revision and maintenance operations.

The following figures show the entities described above and illustrate how the logistic resources are operating: resources allocation (i.e. auto resources - in Figure 7) and allocation of codes specific to each resource (Figure 8).

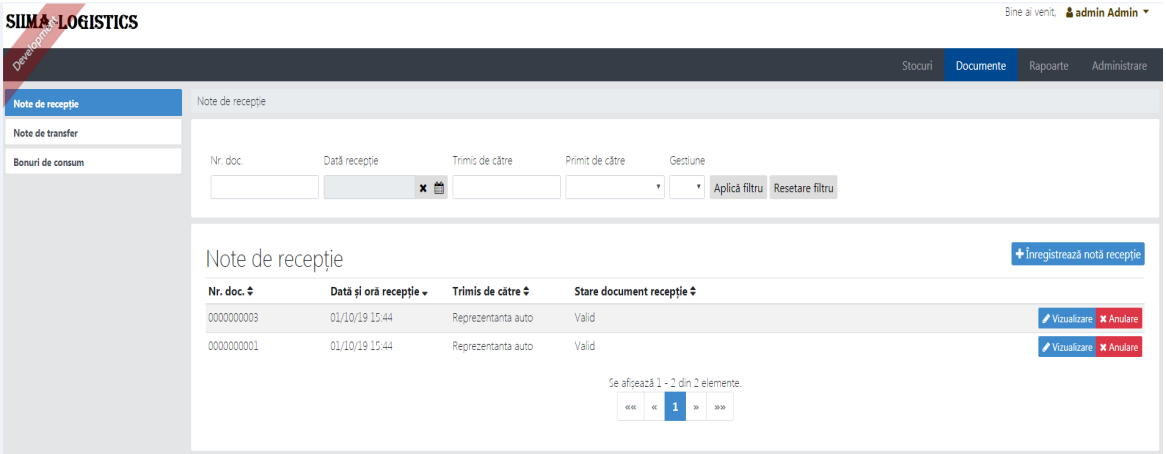

Figure 7. Resources reception list

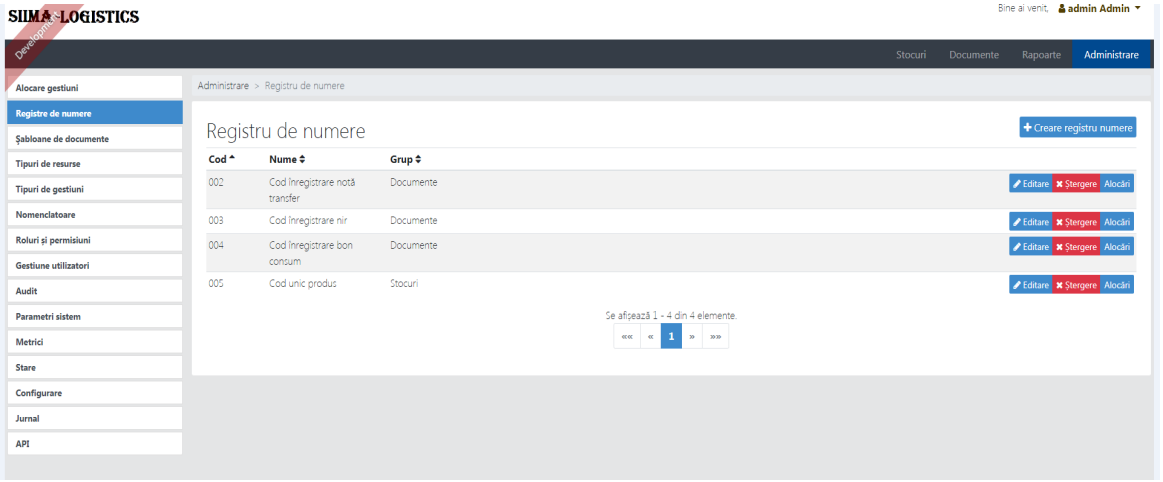

Figure 8. Numbers register

4. Discussion

Currently, the system described above (IISMA) is designed to connect and interconnect ten public entities, each of them with their own characteristics, into an integrated system that serve all the entities' requests. The customer feedback has been positive, which generated increased motivation among the research team members.

In this context, the specific elements of public entities are adequately designed and accommodated by IISMA so that the interconnectivity and interoperability requirements of all the systems owned by Romanian public entities can be achieved.

Currently, after an in-depth research and analysis of the theoretical and practical framework associated with the design, development and implementation of an IIS at the level of public institutions, completed with the identification of the software solutions for the management of activities, resources and communication within public institutions, the project team started the development of this system. Taking into account that the requirements of the beneficiaries are extremely complex, the present article is presenting the modeling of only three modules of the system functional and technical architecture. The other seven modules of functional and technical architecture will represent the subject of a future article.

In the future papers the other modules of the information integrated system for management of activities (IISMA) will be presented. The purpose of these papers is to demonstrate the possibility of implementing an IISMA through open-source solutions. The advantages of these solutions are: high accessibility, the modularization of the applications and portability.

5. Conclusion

The operating environment of the public institutions is characterized by the accelerated dynamics of specific processes and activities, predominantly carried out in an intensified informational context. Therefore, we are recommending to public institution to design and implement an integrated information system for the management of institutions activities, safe and interoperable, based on an integrated open-source software solution that satisfies the identified operational requirements.

In particular, the main operational requirement resides in the implementation of an automation component associated with diversified organizational processes. Thus, the system must ensure the automation of the processes and activities of public institutions, automation of the development, management and monitoring of the institution's projects and programs, automation of resource management as well as the automated management of the internal information flow.

The design of the system should be done in strict accordance with international standards, and the system must be compliant with EU and GDPR specific standards. The system must be flexible, versatile and transparent in terms of access and location of information, replication and updating in distributed databases, control procedures applicable to all magnetic media and electronic data transfer and storage, ensuring the inverse connection (feedback) for continuous comparison and evaluation of what has been done in relation to what has been proposed.

The information system facilities and services must allow for the rapid development and management of standardized documents (plans, orders, reports, summaries, documentaries, etc.), text processing, multi-media information, interactive graphics and collaborative work in Internet and Intranet networks. Due to the importance of geolocation information, it is recommended to include within IISMA the solution of a GIS-Geographic Information Systems and a GPS-Global Positioning System component, for precise spatial identification of organizational and technical elements as well as for decision-making and execution structures for which specific operational information is provided.

Finally, the reliability of the information system must be ensured in any operating conditions (stationary or on the move, in case of physical damage or in the event of a cyber-attack) by adopting structures and working techniques that provide redundancy and resilience.

Acknowledgements

This research work was financially supported by a grant awarded by the Romanian Ministry of Innovation and Research, UEFISCDI, project number 8SOL/2018 within PNCDIII, project code: PNIII-P2-2.1-SOL-2017-09-0102, project name: Integrated Information System for Management of Activities (IISMA) (http://sima.ici.ro/en/)

REFERENCES

Cordella, A. & Iannacci, F. (2010). Information systems in the public sector: The e-Government enactment framework, *The Journal of Strategic Information Systems, 19*(1), 52-66.

Dan-Şuteu, Ş.-A. (2015). Apărarea cibernetică în concepţia unor armate moderne, *Buletinul Universităţii Naţionale de Apărare „Carol I"*, *2*(3). Editura UNAp. "Carol I", Bucureşti.

Gagliardi, D., Schina, L., Sarcinella, M. L., Mangialardi, G., Niglia, F. & Corallo, A. (2017). Information and communication technologies and public participation: interactive maps and value added for citizens*, Government Information Quarterly*, *34*(1), 153-166.

Gitlab Platform. Available at: <https://about.gitlab.com/>.

Han, Y. & Sun, R. (2016). Research on public management efficiency improvement method based on parallel database oriented optimization management information system, *RISTI (Revista*

Iberica de Sistemas e Tecnologias de Informacao), *E5*, 425-437.

Hughes et al. (2005). *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard*, March 2005. Document identifier: saml-profiles-2.0-os. Available at http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

Jones, S., Irani, Z., Sivarajah, U. & Love, P. E. (2017). Risks and Rewards of Cloud Computing in the UK Public Sector: a Reflection on Three Organisational Case Studies, *Information Systems Frontiers*, *21*(2), 359-382.

Lyytinen, K. & Damsgaard, J. (2011). Inter-organizational information systems adoption – a configuration analysis approach, *European journal of information systems*, *20*(5), 496-509.

OPEN LDAP. Available at: https://www.openldap.org/.

PostgreSQL databases. Available at: <https://www.postgresql.org/docs/10/datatype-json.html>.

Sermersheim, J. (ed.) (2006). *Lightweight Directory Access Protocol (LDAP): The Protocol*. Available at: <https://tools.ietf.org/rfc/rfc4511.txt>.

Udroiu, A. M. & Dan-Șuteu, Ș.-A. (2019). *Sisteme informatice integrate pentru managementul activitatilor din institutiile militare*. Ed. Unap „Carol I", Bucuresti.

Udroiu, M., Dumitrache, M., Sandu, I. & Brezulianu, A. (2018). Implementing an Integrated Information System Designed for Romanian Public Entities, *Studies in Informatics and Control*, *27*(3), pp. 369-376. DOI: 10.24846/v27i3y201812

Van Dooren, W. & Van de Walle, S. (eds.) (2016). *Performance information in the public sector: How it is used*. Springer.

WSO2 Identity Server. Available at: <https://wso2.com/identity-and-access-management/>.

Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M. & Alamri, A. (2017). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data, *IEEE Systems Journal*, *11*(1), 88-95.