	ЗАТВЕРДЖЕНО Заступник Голови Державної митної служби з питань цифрового розвитку, цифрових трансформацій і цифровізації
	_____ О.О. НІКОЛАЙЧУК
	“____” _____ 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

НА СТВОРЕННЯ ПРОГРАМНО-ІНФОРМАЦІЙНОГО КОМПЛЕКСУ “МЕНЕДЖЕР ПРОФІЛІВ РИЗИКУ”

Шифр роботи: PIC RISK PROFILES MANAGER 2.1

Версія: 2.1

На 54 аркушах

Київ
2025

CONTENT

DOCUMENT CHANGE HISTORY

Version	Date	Description of changes	Pages
1.0	09/25/2023	First draft, submitted for approval	All
2.0	01/10/2023	The list of conditional abbreviations has been updated.	9.10
		The product name has been updated.	1, according to the text
		Subsection 1.1. “Preliminary Statement” has been updated and supplemented.	11, 12
		Subsection 1.6. “Regulatory and legal documents used during the creation of the Software Product” has been updated and supplemented.	14
		Subsection 2.1. “Purpose of creating the Software Product” has been updated.	15
		Updated subsection 3.1. “Description of Software Product Users”: users excluded.	19
		Table No. 1 “List of roles and their description” has been updated: roles and access functions have been added and changed.	21
		Figure No. 1 “Functional diagram of the Software Product” has been updated.	22
		Updated subsection 4.1. “Functional diagram of the system”.	26
		Subsection 4.2.2. “BP RPM 02. PR Introduction” has been updated: a section on filling out risk profiles has been added.	30-32
		Subsection 4.2.5. “BP RPM 05. PR Register” has been updated: updated requirements for reviewing risk profiles.	38
		The numbering of subsections 4.3. “Description of the Software Product Interface” and 4.4. “List of Software Product Data Elements” has been changed to 4.4. and 4.5, respectively.	40, 41
		Added new section 4.3. “Risk Profile States”	40
		Section 8 “Procedure for Control and Acceptance of the Software Product” has been updated: the date of completion of the development of the Software Product has been updated.	51

		The “Appendices” section has been updated: the composition of Appendix No. 1 has been described; Appendix No. 2 has been added and its composition has been described	53
	18/10/2024	Spelling corrections were made to the text of the document. Changed "...risks" to "...risks"	1, according to the text
		The list of abbreviations and terminology has been updated	9, 10 text
		Updated section 1.1. “Preliminary Statement”: clarified wording, spelling corrections.	11, 12
		Updated clause 1.3. “Full name of the Software Product and its conventional designation”: the abbreviated name has been clarified name.	13
		Updated header	according to the text
		The title of clause 1.4 “Name of the developer and customer institution, their details” has been updated.	13
		Clause 2.1 “Purpose of creating a Software Product” has been updated: the wording has been removed (part 9, paragraph 1) and clarified (paragraph 1).	15
		Updated clause 2.2. “Requirements for the Software Product”: wording clarified, wording removed.	16, 17
		Updated clause 2.3. “Expected results”: wording clarified, wording removed.	17, 18
		Updated clause 2.4. “Development of the Software Product”: wording clarified.	18
		Clause 3.1. “Description of Software Product Users” has been updated: wording has been clarified, stylistic changes have been made.	19
		Updated clause 3.2. “Characteristics of users of the Software Product”: wording removed.	19
		Updated Table No. 1 “List of roles and their description”: the authority of the risk profiling unit has been removed.	21
		Section 3.4 “Description of the main functionality of the Software Product” has been updated: data has been clarified.	21
		Updated Figure No. 1 “Functional diagram of the Software Product”: the block “Electronic Digital Signature/Electronic Digital Signature Authorization System” has been removed	21

		Updated clause 3.6. “The main process performed by the Software Product”: spelling corrections; wording deletion.	23-25
	10/24/2024	Updated clause 2.1. “Purpose of creating the Software Product”: wording clarified.	15
		Updated Table No. 1 “List of roles and their description”: in the column “Risk profiling unit” of Table 1, paragraph 3.3 of section 3, spelling corrections were made; “attach electronic documents” was corrected to “add electronic documents necessary for risk profile management”;.	21
		Clause 3.6 has been updated: in paragraph 7, “and exchange of information with the relevant software and information complexes of the EAIS” has been removed.	25
		Clause 5.2. “Requirements for protecting information from unauthorized access” has been updated: the wording of legislative measures has been clarified.	42
		Updated clause 5.5. “Information security requirements”: added requirement for state expertise	44
		Updated clause 5.8. “Requirements for software power and speed”: deleted sentence, clarified requirements for simultaneous user work, removed block on preliminary data for calculating the load on the Software product (the number of sessions will be deducted from calculations during software testing). Spelling corrections made.	45
		Updated section 5.11 “User Interface Requirements”: Firefox added	46
		Updated Section 7 “Technology Stack”: removed “DB must be built in Always On mode”, made spelling corrections, updated editions and versions	50
		Section 8 “Procedure for Control and Acceptance of the Software Product” has been updated: the term “State Customs Service” has been brought into line with the table “List of Conventional Abbreviations”.	51
		Updated “Table. DE.RPM V3 Appendix No. 1” (DE002, DE017, DE019, DE020, DE050, DE051, DE052).	
		Updated “Table. DE. PR Blocks of Appendix No. 1” (DE020, DE050, DE051, DE052).	
		Updated “Table.DE.Types of EL PR Appendix No. 1” (DE017, DE020, DE050, DE051, DE052).	

		Updated “Table. Matrix. Role (Data Elements) Appendix 2: Role Model Matrix of the PIC “MPR”” (DE010, DE023, DE029-031, DE033, DE035, DE039, DE040, DE049-DE052).	
	10/29/2024	Updated section 2.3. “Expected results”: sentence removed.	17
		Updated clause 3.1. “Description of Software Product Users”: “administrator - administrator of the Software Product”, “officials of the customs competence unit” were excluded.	19
		Updated clause 3.2. “Characteristics of Software Product Users”: paragraph 5 was deleted, amendments were made to paragraph 8.	19.20
		Updated Table No. 1 “List of roles and their description”: the “Administrator” role has been removed.	21
		Updated clause 3.6. “The main process performed by the Software Product”: added paragraph 8	25
		Updated clause 4.4. “Description of the Software Product Interface”: wording of paragraph 4 changed, paragraph 4 supplemented	41
		Clause 5.2 “Requirements for protecting information from unauthorized access” has been updated: the wording of clause 1, paragraph 1 has been changed	42
		Updated clause 5.11. “User interface requirements”: changed paragraph 1, supplemented paragraph 2 with the word “Mozilla”.	46
		Updated clause 5.12.3. “Requirements for organizational support”: wording of paragraph 3 has been changed	47
		Updated section 7 “Technology stack”: changed clause 5, paragraph 5	50
		Section 8 “Procedure for Control and Acceptance of the Software Product” has been updated: clause 4, paragraph 6 has been deleted. Paragraph 6 is presented in the form of table No. 4 “Documentation of the Software Product”	51, 52
	08/11/2024	The list of conditional abbreviations has been updated: the term “Software Product” has been added	9
		Updated section 2.3. “Expected results”: added “upload and save additional documents to the risk profile in *.pdf. *.doc, *.rtf, *.xls formats;"	18

		Updated clause 3.6. “Main process performed by the Software Product”: added paragraph 8.	25
		Updated clause 4.2.1. “BP RPM 01. PR Project”: added “Exclusively the risk profiling unit of the Central Office has the right to review information and enter data elements provided for by the business process “RPM01. PR Project”.”	28
		Stylistic corrections have been made to the text of the Terms of Reference: the words and abbreviations “system”, “software” have been replaced with “Software product” in the corresponding cases.	according to the text
		Updated clause 5.8. “Requirements for the power and speed of the Software Product”: the word “systems” has been removed from paragraph 2	45
		Updated clause 5.10. “System Scaling Requirements”: added “which will use the Software Product,”.	46
		Clause 5.12.1 “Requirements for linguistic support” has been updated: clause 1, paragraph 1, has been deleted.	47
		Updated Table No. 4. Software Product Documentation: in clause 2, the word “Software Product” was replaced with “network architecture for deploying the Software Product”.	52
		The “Appendices” section has been updated: information on the Table “Format DE044 “Document Number” of Appendix No. 1 and information on Appendix No. 3 “Risk Profile Printing Template” has been added	53
		Updated Appendix No. 1: table “DE044 “Document Number” Formats” added.	
2.1	02/13/2025	Updated clause 1.6. “Regulatory and legal documents used during the creation of the Software Product”: clauses 9 and 10 of paragraph 1 were added.	15
		Updated clause 2.4. “Development of the Software Product”: clause 1 of paragraph 3 is reworded; paragraph 4 is added.	19
		Paragraph 1 of clause 5.5. “Information security requirements” has been updated: set out in a new wording.	43, 44
		Updated clause 5.8 “Software Product Power and Speed Requirements”: paragraph 3 added.	45

		Paragraph 3 of clause 5.12.3. “Requirements for organizational support” has been updated: set out in a new wording.	47
		Updated Section 7 “Technology Stack”: presented in a new edition.	50, 51
		Section 8 “Procedure for Control and Acceptance of the Software Product” has been updated: paragraph 1 has been reworded - the date of completion of the development of the Software Product has been updated.	52
		The table “Matrix of Rights and Roles” has been updated: add to the “Matrix. Rights” sheet of the “AD_2_RPM_Role matrix_v2.0.0” application, item PD08 “Review of PR management processes” with the “Risk Department” access rights for all business processes.	

LIST OF CONVENTIONAL ABBREVIATIONS

No. of the company	Term	Value
1. ASMO		Automated customs clearance system
2.	DB	Database
3.	State Customs Service	State Customs Service of Ukraine
4. MD		Declaration
5.	ASUR	Automated risk management system
6.	SUR	Risk management system
7.	CEP	Qualified electronic signature
8.	Application Programming Interface (API)	Application programming interface
9. MCU		Customs Code of Ukraine
10.	PIC “MPR”	Software and information complex “Profile Manager” risk”
11. MF		Customs formality
12. PR		Risk profile
13. ED		Data elements
14. EAIS		Unified automated information system
15	IT department Central apparatus	Structural unit of the State Customs Service whose functions include among others, includes ensuring the development, implementation implementation and technical support of information, telecommunications and information and telecommunications systems and technologies, automation of procedures
16	Unit profiling risks of the Central apparatus	Structural unit of the State Customs Service, which assigned functions to coordinate the application of the MAS; central unit for coordination of application SUR

17.	Software product	Software and information complex “Risk Profile Manager”

1. GENERAL INFORMATION

1.1. Prerequisite

In accordance with paragraphs 1 and 2 of part 1 of Article 363 of the Customs Code of Ukraine The activities of customs authorities in risk assessment and management consist in the formation of information database of the customs authorities' risk management system, as well as systematic analysis, identification and assessment of risks, including using information technology.

By Order of the Ministry of Finance of Ukraine No. 684 dated July 31, 2015 (hereinafter referred to as the NMFU No. 684) approved the “Procedure for conducting risk analysis and assessment, development and implementation of risk management measures to determine the forms and volumes of customs control”. According to paragraph 2 of Section I, the Procedure establishes a uniform approach to formation of an information database of customs authorities' RUS, implementation by customs authorities bodies (their structural divisions) for risk analysis and assessment, development and implementing practical risk management measures to determine the forms and volumes customs control, analysis of results and adjustment of management measures taken risks.

In accordance with paragraph 9 of Section I of the NMFU No. 684, for the development of measures to risk management at the tactical level risk management by customs authorities (their structural units) within the scope of competence based on the results of analysis, identification and risk assessment and in accordance with the Priority Areas, the following is used tool, like a risk profile.

Paragraph 13, Clause 3, Section I of NMFU No. 684 defines a risk profile as a description any set of risk indicators, including specific combinations risk indicators resulting from the collection, analysis and systematization of information.

According to clause 1 of Section II of the NMFU No. 684, risk profiles depending on the possibilities of automating their application can be documentary or electronic.

Central unit for coordination of the application of the MAS in accordance with paragraph 17 Section II of the NMFU No. 684 systematizes information on risk profiles from application of information technologies.

The purpose of creating the Software Product is to automate the accounting process and administration of electronic risk profiles.

The MPR PIC must be compatible and integrated into the IT architecture of information systems. systems of the State Customs Service, and ensure the possibility of information exchange (receiving and transmitting data) in particular with the following related systems:

“Electronic Document Management System of the State Customs Service” - integration with for the purpose of transmitting/receiving information regarding documents necessary to ensure implementation of risk profile management.

PIC “MPR” is a software functionality based on the ASMO “Center” of the EAIS of Customs bodies with integration with the “Electronic Document Management System of the State Customs Service”.

1.2. General provisions

This document provides technical and quality characteristics of the item development, list and term of provision of services for development and implementation PIC "MPR".

The requirements specified in this document are not exhaustive and may include clarifications or non-material changes in the process of developing the Software Product.

The implemented software and information complex must comply with the following basic requirements:

- universal;
- functionally sufficient (complete);
- reliable (automatic saving of all data and correct completion programs work without data loss);
- suitable for modernization and scaling;
- protected from external influences;
- document system changes made by users.

1.3. Full name of the Software Product and its symbol

Full name of the software product – Software and information “Risk Profile Manager” complex.

The abbreviated name is **PIC_RISK_PROFILES_MANAGER.**

1.4. Name of the customer's institution, details

State Customs Service of Ukraine.

Legal address: Ukraine, 04119, Kyiv, Degtyarivska St., building 11-G.

1.5. List of documents on the basis of which the Program is created product, by whom and when these documents were approved

- Customs Code of Ukraine.
- Regulations on the State Customs Service of Ukraine, approved by Resolution of the Cabinet of Ministers of Ukraine dated March 6, 2019 No. 227.
- State Anti-Corruption Program for 2023-2025, approved Resolution of the Cabinet of Ministers of Ukraine dated March 4, 2023 No. 220.
- Integrated Border Management Strategy for the period up to 2025 approved by the order of the Cabinet of Ministers of Ukraine dated July 24, 2019. No. 687-r.
- Procedure for conducting risk analysis and assessment, development and implementation risk management measures to determine the forms and volumes of customs control, approved by the order of the Ministry of Finance of Ukraine dated 07/31/2015 No. 684 and registered with the Ministry of Justice of Ukraine 08/21/2015 under No. 1021/27466.
- Long-term national strategic plan for digital development, digital transformation and digitalization of the State Customs Service of Ukraine and its territorial divisions based on the Multi-Year Strategic Plan EU electronic customs (Multi-annual strategic plan for electronic customs, MASP-C), put into effect by order of the Ministry of Finance of Ukraine dated 09.02.2024 No. 63.
- Work plan of the State Customs Service of Ukraine for 2024, approved By the Ministry of Finance of Ukraine on May 16, 2024.

1.6. Regulatory and legal documents used during the creation Software product

The system must comply with the requirements of applicable regulations. documents, namely:

- Constitution of Ukraine;

- Customs Code of Ukraine;
- Law of Ukraine “On Information”;
- Law of Ukraine “On Electronic Documents and Electronic Document Management”;
- Order of the Ministry of Finance dated 20.09.2012 No. 1011 “On approval of departmental classifiers of information on state customs affairs, which used in the process of processing customs declarations";
- Order of the Ministry of Finance of Ukraine dated July 31, 2015 No. 684 “On approval of the Procedure for conducting risk analysis and assessment, development and implementing risk management measures to determine the forms and volumes customs control”;
- Order of the Ministry of Finance dated 19.05.2023 No. 263 “On approval of the Regulation on A unified automated information system of customs authorities, procedure and conditions of application of its systems”;
- Order of the State Customs Service of 28.12.2023 No. 1017 “Procedure for access to information in systems that ensure the functioning of electronic information resources of customs authorities”.
- A comprehensive information protection system for information and communication system of the State Customs Service in accordance with the requirements of regulatory documents on technical information protection, namely: Automated customs system "Center" registration, certificate of conformity, registered in State Commission for Special Communications No. 2188B dated 12/24/2024.
- SO/IEC 25010:2016 Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models" - development quality standard software.

This list is not exhaustive. Requirements of the Legislation of Ukraine, regulatory and guidance documents relating to the purpose, purpose and objectives of service provision can be clarified.

2. PURPOSE AND GOAL OF CREATING A SOFTWARE PRODUCT

2.1. Purpose of creating the Software Product

The purpose of creating the Software Product is to streamline and automate the process of collecting, accumulating and processing information on risk profiles, namely creation of technical tools for systematizing information about profiles risk, as well as the formation of an electronic database of individual data elements from the stage creating a draft risk profile, reducing time spent administering profiles risk, as well as the need to ensure:

- technical tools for effective work organization State Customs Service when administering risk profiles;
- automation of processes in the administration of risk profiles;
- accumulation and processing of relevant data according to a unified structure and a format that ensures their consistency and accessibility to all authorized persons;
- avoiding the possibility of duplication of information at different levels, which relate to the same risk profiles;
- managing the process of administering risk profiles (creating a draft risk profile, entering information about the profile risk, making changes and changing the status of the risk profile);
- ensuring the possibility of exchanging information with the IT Department State Customs Service on the implementation of risk profiles;
- automation of the process of monitoring the timeliness of profile implementation risk profiles, changes to them and changes in the status of risk profiles in the process administration of risk profiles;
- storing risk profile materials in electronic form, creation of standard documents in electronic form for integrated templates;
- generation of reports and registers according to user-defined criteria;
- creating a database of information that can be used in the assessment risk profile work;
- creation of electronic documents;
- synchronization with other DMSU applications.

2.2. Requirements for the Software Product

The software product is intended for:

- save the following information: risk profile number; ASUR code risk profile; name of the risk profile; brief description (purpose of introduction risk profile); type of risk profile; ASUR module to which the risk profile is applied; the risk profile starts; termination/suspension of the risk profile; list of customs formalities that are shaped by the risk profile; information regarding changes made to the risk profile and their content (number and date of the protocol Expert Commission on the Application of the Risk Management System, letters about changes and additions); information on software implementation the relevant risk profile and/or changes to it (the specified information entered by the relevant IT department);
- recording specific actions and/or processes at each stage risk profile administration in automated and/or non-automated procedure;
- interaction of structural units participating in the process risk profile administration;
- entering information necessary for administering the risk profile;
- recording and saving the results of risk profile administration;
- formation of registers according to specified criteria;
- formalizing the process of administering risk profiles;
- providing up-to-date and reliable data regarding profile administration risk;
- assessing the quality of risk profile administration;
- methodological assistance in the administration of risk profiles;
- entering and saving information regarding the administration of risk profiles.

2.3. Expected results

The result should be a developed Software and Information Complex, which provides:

- access data from internal and external sources using API integrations;

- assigning, changing and fixing statuses, as well as those authorized to
  administration of risk profiles of customs officials
  organ;
- interaction during the administration of the risk profile by various structural
  by customs authorities;
- providing up-to-date information on the state and status of the risk profile;
- tracking deadlines set for implementation actions
  regarding the risk profile;
- the ability for users to enter information about risk profiles that are
  the moment of implementation of the PIC “MPR” were already implemented;
- formation of a data array for administration and control,
  export of this data in *.xls (and/or *.xlsx, *.csv) format for the purpose of
  further analytics and provision of summarized information (reporting) to management
  according to the appropriate forms or at the user's request (flexible formats
  reporting);
- access to methodological materials on risk management;
- storage of materials used in profile administration
  risk;
- creation of standard documents in electronic form according to integrated
  templates;
- entering and storing information regarding the administration of risk profiles;
- upload and save additional documents to the risk profile in
  *.pdf formats. *.doc, *.rtf, *.xls;
- the possibility of automated exchange of necessary information with others
  information systems of the State Customs Service.

2.4. Software Product Development

Due to the impossibility of ensuring the confidentiality of part of the data,
have the status for official use and are contained in the risk profile passport,
It seems advisable to develop the Software and Information Complex in stages.

Stage 1.

- system user management;
- automatic tracking of risk profile data implementation deadlines;

- ensuring information interaction with structural units

  State Customs Service;
- electronic database of risk profile data elements that do not have the characteristic confidentiality;
- integration with the electronic document management system of the State Customs Service;
- formation of a data array for administration and control, for appropriate forms or at the user's request.

Stage 2.

- electronic database of risk profile data elements that have characteristics confidentiality. All data elements that have confidentiality characteristics must be encrypted both in the database and when transmitted using HTTPS, TLS/SSL;
- implementation of a regulatory and methodological module.

Stage 3.

- development and implementation of the business process “Registration and evaluation of information about risk”.

3. SOFTWARE PRODUCT REQUIREMENTS

3.1. Description of users of the Software Product

The main users of the Software and Information Complex are officials customs authorities, namely:

- officials of the risk profiling unit of the Central Office;
- officials of the IT department of the Central Office;
- officials of the Central Office units;

3.2. Characteristics of users of the Software Product

The software and information complex provides the ability to create unlimited number of users with the ability to restrict access to functional components of the Software and Information Complex, taking into account data regarding their identification, authentication, and existing roles.

User identification is carried out by authentication tools and authorizations that are implemented in the ASMO “Center” / EAIS, or other proposed authentication tools.

User management is carried out within the framework and tools of the general user administration policies of ASMO “Center” / EAIS, or others proposed user administration tools.

Distribution of rights to enter, edit, and view individual data elements by structural units are given in the Role Model Matrix of the PIC “MPR” (see application “AD_2_RPM_Role matrix_v.2.1.”).

Officials of the Risk Profiling Unit of the Central Office use the Software and Information Complex to enter information about risk profile, risk profile monitoring, filling in the educational and methodological module, as well as the formation of documents and requests according to specified criteria.

Officials of the IT department of the Central Office use Software and information complex for entering and viewing information about risk profile, including the implementation of data required for proper operation risk profile.

Officials of the Central Office units use the Software -information complex for viewing information on the risk profile in volumes, appropriate to the powers granted.

3.3. Description of Software Product user roles and access

The software product should come with basic user roles given in table 1:

Table No. 1. List of roles and their description.

Role	Functions available in the system
Inspector	• review of risk profiles; • review of risk profile management results; • formation of documents and registers according to the defined parameters. • review of the educational and methodological module.
IT departments of the Central Office (CA)	• review of all risk profile management processes; • input of information on risk profile implementation; • input of information on profile changes implementation risk; • entering information on the implementation of changes to the risk profile status; • reviewing risk profiles; • reviewing the results of risk profile management; • generating documents and registers according to the specified parameters.
Risk Profiling Unit of the Central Office (CA)	• entering risk profile data elements; • entering information about risk profile projects; • entering information about changes to the risk profile; • implementing changes to the risk profile; • adding electronic documents required for risk profile management; • review of risk profiles; • review of all risk profile management processes; • formation of documents and registers according to the defined parameters; • editing, filling in, reviewing the normative and methodological module.

3.4. Description of the main functionality of the Software Product

Functionality of the Software and Information Complex “Risk Profile Manager” includes:

- user authentication according to the role in the Software information complex;
- interaction with directories in the ASMO “Center”;
- downloading files of various formats and sizes;
- ability to generate registers (in .xls, .csv format) based on specified parameters;
- saving any changes made by the user regardless of his role in system.

3.5. Functional diagram of the Software Product

Figure No. 1 shows the functional diagram of the Software Product:

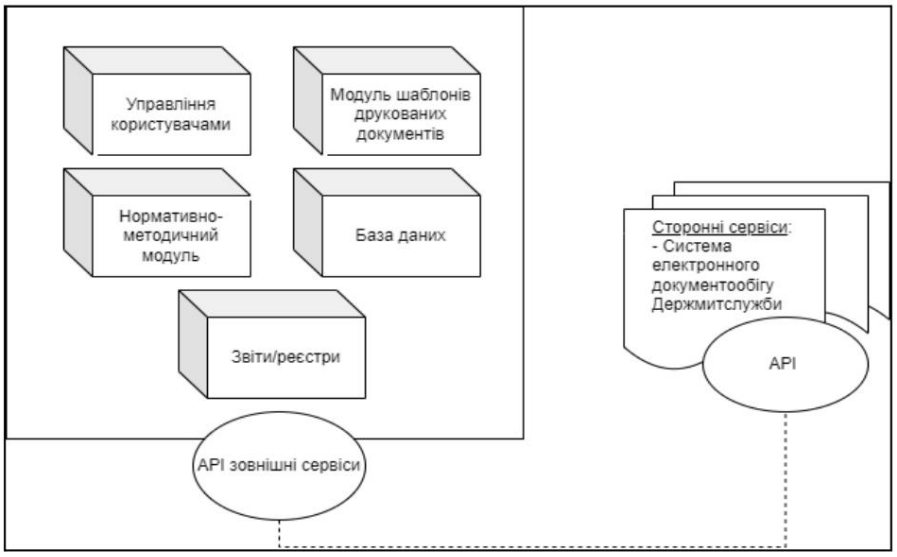

Fig. No. 1. Functional diagram of the Software Product.

The software product consists of the following elements:

Table No. 2. List of modules and their description.

Module	Purpose and main characteristics
User Management	Designed to manage users of the Software Product. In this module, the administrator

	configures access to the components of the Software Module depending on the user role.
Reports/registers	Designed for generating reports/registers using existing data in the system, based on user-defined criteria, with the ability to export reports to the xls file type;
Printed document templates module	Systems designed to manage (edit) printed document templates
Database	Designed to store information about risk profiles, execution status, and files associated with the risk profile of various sizes.
Normative and methodological module	Designed to aggregate regulatory and methodological information on risk profile management. Contains: links to codes, laws, subordinate regulations, methodological recommendations for customs officials on risk management, explanations from relevant departments on issues that arise in the management process risks.

3.6. The main process performed by the Software Product

The main process of the PIC “MPR” is the fixation in the program and information system complex of risk profile data elements, streamlining and automating the process collection, accumulation and processing of information on risk profiles and its systematization, and also the formation of electronic databases, from the stage of creating a profile project risk.

The development of the Software and Information Complex will take place in stages, in accordance with clause 2.4 of the Technical Requirements, with gradual increase in functionality.

The risk profile management process includes developing a draft risk profile, entering information about the approved risk profile, the possibility of making changes to risk profile and changes in its status in the regulatory acts cases.

The Software and Information Complex also provides the ability to track timing of events such as risk profile implementation, changes made to the profile risk, changes in risk profile status, marking of implementation, authorized structural unit. Software and information complex allows you to create registers according to specified criteria.

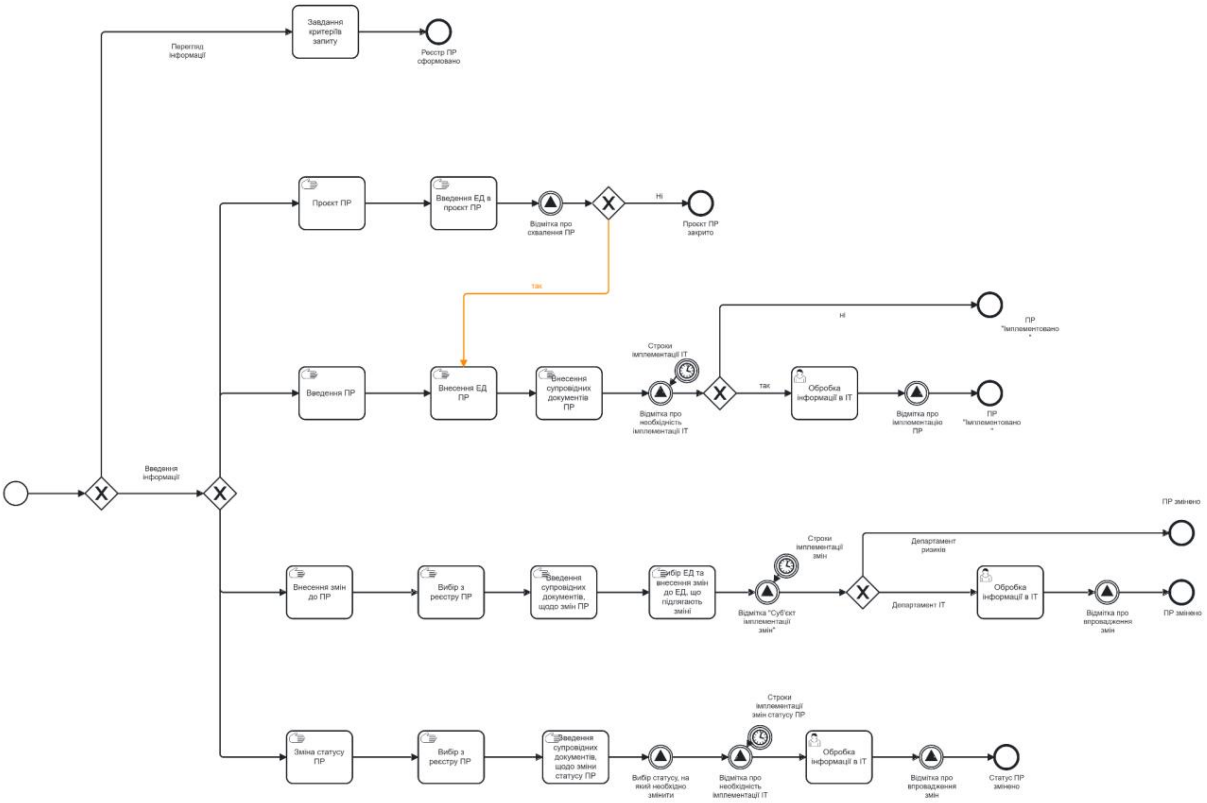

Fig. No. 2. "RPM General. General process".

A prerequisite for creating a risk profile is the existence of grounds. Next, the user goes through the following stages:

- creating a draft risk profile;
- entering a risk profile;
- changes to the risk profile (if necessary);
- change the status of the risk profile (if necessary);
- review information (if necessary).

Potentially automated processes include interaction with the system electronic document management of the State Customs Service. The integration setup will be carried out by the State Customs Service.

Integration with the electronic document management system of the State Customs Service is carried out by querying the document number (DE044 "Document number").

Integration is performed exclusively for documents for which a specific format is defined. DE044, according to the Table “Format DE044 “Document Number””. Documents regarding whose format number is not specified are added to the PIC “MPR” in the formats *.pdf. *.doc, *.rtf, *.xls.

The following steps, within the framework of the work envisaged by this TOR, are envisaged: expansion and detailing of the electronic database of risk profile data elements that have confidentiality signs.

3.7. Data structure description

The main entities of the data structure contained in the Software Information complex:

- user data - contains information about registered users and their roles in the Software and Information Complex;
- risk profile data - contains information about the current status, change logs;
- save files in formats up to 100 MB in size as a single file;
- the necessary automated control procedures must be provided data integrity and consistency of information stored in Software and information complex, namely:
    - checking the compliance of the entered data types by means of user interface;
    - data integrity and data type compliance control by means database management systems.

4. FUNCTIONAL REQUIREMENTS

4.1. Functional diagram of the Software Product

The State Customs Service uses the following main software and information complexes: information systems and their components:

1. **EAIS is** a multifunctional integrated automated system that constitutes a set of interconnected information, electronic communication and information and communication systems that provide functioning of electronic information resources of customs authorities with the purpose of carrying out customs affairs, and the means of ensuring them.
2. **The ASMO "Center"** ensures the accumulation of information at the central level, functioning of the business logic of key processes, including maintaining registers, directories, control over the movement of goods, etc.

4.2. Detailed description of business processes

Implementation of organizational services related to MDP is supported special business processes. The risk profile management process includes following blocks:

- **View information** (RPM 05. PR register).
- **Entering information,** including four sub-blocks:
  - **Draft** risk profile (RPM 01. Draft PR).
  - **Entering** the risk profile (RPM 02. Entering the PR).
  - **Making** changes to the risk profile (RPM 03. Changes to the PR).
  - **Change of risk profile status** (RPM 04. Change of PR status).

Design processes, information input, changes and status changes risk profile are carried out taking into account the provisions of the Order of the Ministry of Finance dated 31.07.2015 No. 684.

Table No. 3. Transition between business processes.

Business process	Prerequisites	Postconditions
RPM 01. PR Project Entering	PR project data elements.	The "Risk Profile Entry" process begins. PR project closed
RPM 02. Introduction PR	Input of PR data elements	Risk profile implemented.
RPM 03. Changes to PR	Selection from the PR register.	The PR has been changed.
RPM 04. Change of PR status	Selection from the PR register.	The PR status has been changed.
RPM 05. Register	Tasks for the criteria for forming the register	The PR register has been formed.

A detailed description of business processes and the necessary tools for them administration is given below.

The functionality of the Software Product can be expanded depending on needs, results of experimental operation and changes in legislation.

IMPORTANT! The business processes listed are a preliminary description of the business processes that will be take place in the Program and Information Complex. They may be subject to clarifications time to detail the technical requirements for the Software and Information Complex.

4.2.1. BP RPM 01. PR Project

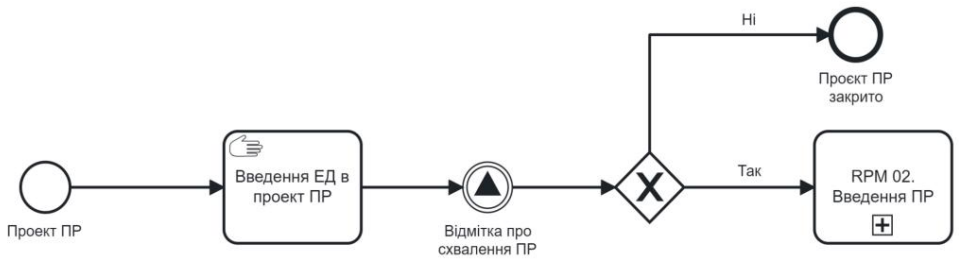

Fig. No. 3. Business process: RPM 01. Project PR

This process belongs to the “Information Entry” block and describes the creation of of the PR project. The risk profiling unit of the Central Office has exclusively the right to view information and enter data elements as required by the business process “RPM01. PR Project”.

In accordance with clause 2 of Section II of the Order of the Ministry of Finance No. 684 of 07/30/2015, profiles The risk profile is developed by the central risk profiling unit.

Customs authorities (see the “Units” Guide) provide the profiling unit Central Office of Risks proposals for the development of risk profiles.

After deciding whether to develop a risk profile or obtain a customs authorities risk profile development proposals, risk profiling unit The central office enters data elements into the PIC “MPR” according to the list, defined in the table “DE. PR Blocks” - Block 06 “BL06. PR Project”, taking into account type of electronic risk profile (see “DE. EL PR Types”).

From the moment the ED is saved, the risk profile automatically acquires the status “Project PR".

After the Expert Commission makes a decision regarding the electronic profile risk, the data element: DE039 “PR approval mark” is affixed and the transition to “BP RPM 02. PR input” is made.

The final result of the “RPM 01. PR Project” process is:

- if the value of DE039 “PR approval mark” is “Yes”: initiation process “RPM 02. Introduction of PR”.
- if the value of DE039 “PR approval mark” is “No”: PR project automatically receives the status “Project PR closed”.

4.2.2. BP RPM 02. Introduction of PR

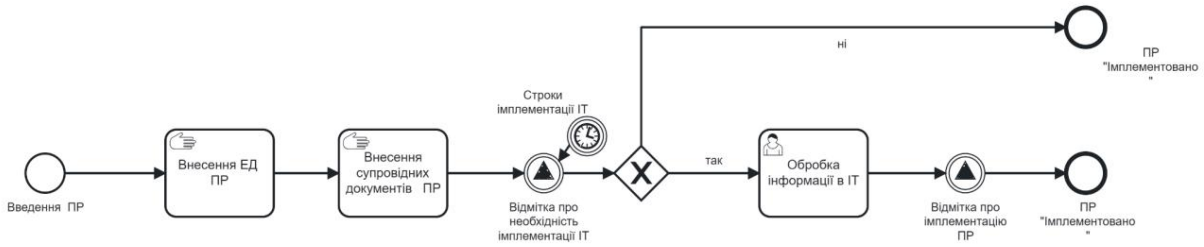

Fig. No. 4. Business process: RPM 02. Introduction to the RPM

This process belongs to the “Information Entry” block and describes the actions officials of the risk profiling unit of the Central Office and the unit IT of the Central Office, which must be carried out in cases of decision-making on approval and implementation of a new risk profile, filling in framework profiles risk, and the procedure for PR actions that must be included in Software and information complex, but have already received the status of approved, enacted and implemented by its launch date.

In accordance with Clause 7 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, the decision on The approval of electronic risk profiles is made by the Expert Commission.

Decisions of the Expert Commission are made during meetings and/or through the application of information technology with the use of commission members qualified electronic signatures.

The decisions of the Expert Commission are recorded in the minutes of the meeting.

In accordance with clause 15 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, the decision on approval of documentary risk profiles is made in accordance with the procedure provided for for electronic risk profiles.

Official of the Risk Profiling Unit of the Central Office enters the risk profile data elements according to the list specified in table “DE. PR Blocks” - Block 01 “BL01. PR General Information”, taking into account the type electronic risk profile (see “DE. EL PR Types”), and Block 02 “BL02. Documents, regarding the implementation and filling of the PR”.

If the PR refers to normal or framework risk profiles, the job title
A person from the risk profiling unit of the Central Office fills in the ED block 05
“BL05. Customs formalities” of the table “DE. PR blocks”.

In accordance with clause 7 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, copies
electronic risk profile passports are sent by letter to the profiling unit
Central Office risks to the Central Office IT unit for software
implementation.

Official of the Risk Profiling Unit of the Central Office
puts DE048 “Mark on the need to implement IT”.

Value “No” DE048 “Mark on the need for IT implementation”
is affixed ***only*** in the case when the PR has already received the status of approved,
put into effect and implemented by the launch date of the Program and Information
complex. In all other cases, the value “Yes” is set.

From the moment of saving the PR with DE048 “Marking the need for implementation
IT”, which has the value “No”, the risk profile acquires the status “PR implemented”.

In accordance with Clause 7 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, in the minutes
The Expert Commission meeting determines the deadline for the implementation of the electronic profile
risk by the IT departments of the Central Office. The period begins
(timer is set) from the moment the value “Yes” is set DE048 “Mark about
the need for IT implementation”, taking into account the value of DE049 “Implementation period
information”.

From the moment the IT department of the Central Office affixed DE034 “Mark
IT about the implementation of PR”, the risk profile acquires the status “PR implemented”.

If it is necessary to fill in the framework risk profile, the authorized
the official activates the data element DE050 “Filling of PR” defined in the table
“DE. PR Blocks” - Block 01 “BL01. PR General Information”, and complements Block 02
“BL02. Documents on the implementation and filling of the PR”.

The authorized official affixes DE048 “Mark of necessity
IT implementation”.

Storing information regarding DE050 “Filling the PR” in conjunction with
by marking DE048 “Marking the need for IT implementation” activates DE051
“Number of PR fillings”.

The software product does not allow the repeated setting of DE 048 “Mark about the need for IT implementation” in cases of supplementing elements DE041-DE049, DE051, related to element DE050 “Filling of PR”, which is stored in PIC “MRP” and which is related to DE034 “IT Mark on PR Implementation”, which has the meaning "Yes".

From the moment of saving the PR, for which the filling was carried out, with DE048 “Mark on the need to implement IT”, meaning “No”, filling in the PR acquires the status “PR implemented”.

From the moment of setting the value “Yes” DE048 “Mark on the need "IT implementation" of the risk profile for which the filling was carried out, the time period starts (the timer is set), taking into account the value DE049 “Information implementation period”.

From the moment the IT department of the Central Office affixed DE034 “Mark IT on the implementation of PR”, filling in the risk profile acquires the status of “PR implemented”.

The final result of the process “RPM 02. Introduction of PR” is:

- the risk profile receives the status “PR implemented”.

4.2.3. BP RPM 03. Changes to the PR

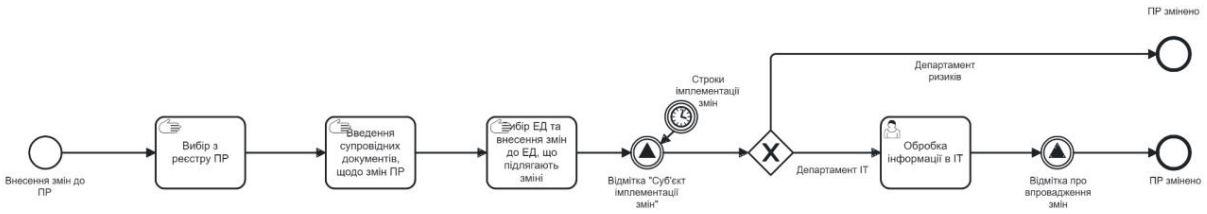

Fig. No. 5. Business process: RPM 03. Changes to the PR

This process belongs to the “Information Entry” block and describes the actions officials of the risk profiling unit of the Central Office and the unit IT of the Central Office, which must be carried out in cases of decision-making on making changes to the risk profile.

In accordance with Clause 7 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, the decision on Changes to electronic risk profiles are accepted by the Expert Commission, except in cases where defined in paragraphs 8, 12 of Section II .

In accordance with clause 8 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, the subdivision Risk profiling of the Central Office makes a decision on amendments to electronic risk profile, if such changes are related to:

1) with changes to documents, the provisions of which were taken into account during the development risk profile, and/or the need to update the relevant values individual risk indicators or risk profile parameters;
2) with changes in the numerical values of the positive/negative history of the risk profile, algorithms for determining the numerical value of risk based on the risk profile;
3) with the need to correct errors in the risk profile passport.

In accordance with clause 10. Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, adopted in accordance with Section 8 of Section II of the decision on electronic risk profiles, software which were implemented by the risk profiling unit of the Central device using the functionality of the EAIS, including ASMO, are issued in in the form of a memorandum with a resolution from the head or deputy head central unit for coordinating the application of the MES.

Adopted in accordance with Clause 8, Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015 solutions regarding electronic risk profiles, the software implementation of which was carried out

by the IT department of the Central Office, are issued in the form of a letter from the department Central Office risk profiling to the Central Office IT department.

In accordance with clause 10 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, the decision, provided for in Clause 8 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015 are adopted with regard to electronic risk profile and/or its supplement.

In accordance with clause 12. Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015 in the case of identification of problematic issues during the software implementation of the electronic profile risk, the risk profiling unit of the Central Office initiates consideration of the issue regarding the need to make changes to the program code by sending a letter to IT department of the Central Office.

Provided there are grounds for making changes to the PR and taking into account the subject their implementation, an official of the risk profiling unit of the Central the apparatus enters the risk profile data elements according to the list defined in the table “DE. PR Blocks” - Block 03 “BL03. PR Changes”, taking into account the type electronic risk profile (see “DE. EL PR Views”).

PIC “MPR” when selecting the “Making changes to PR” functionality provides the ability to select EDs to which changes are made, record and display historical data retrospectives of their introduction.

In case of changes to the usual or framework risk profiles, PIC “MPR” should provide simultaneous display of primary data elements of block 05 “BL05. Customs formalities” of the table “DE. PR blocks”, and the amendments made to them.

Value “Risk Department” DE029 “Change Implementation Entity” is affixed exclusively if there are grounds provided for in clause 8 of Section II of the Order Ministry of Finance No. 684 dated 07/30/2015.

From the moment of saving ED DE030 “Reason for making changes”, which is activated by conditions of value DE029 “Change Implementation Entity” - “Risk Department”, profile The risk becomes “PR changed” status.

In cases where there are no grounds for changes to the risk profile by the risk profiling unit of the Central Office, it sets the value DE029 “Change Implementation Entity” - “IT Department”.

From the moment of setting the value “IT Department” DE029 “Subject implementation of changes”, the time limit begins (a timer is set)

defined in letters regarding the implementation of changes to the risk profile by the IT department Central office, taking into account the value of DE049 “Implementation period information”.

From the moment the IT department of the Central Office affixed DE031 “Mark IT about implementing changes to the PR”, the risk profile acquires the status “PR changed”.

The final result of the process “RPM 03. Changes to the PR” is:

- the risk profile receives the status “PR changed”.

4.2.4. BP RPM 04. Change of PR status

Fig. No. 6. Business process: RPM 04. Change of PR status

This process belongs to the “Information Entry” block and describes the actions officials of the risk profiling unit of the Central Office and the unit IT of the Central Office, which must be carried out in cases of decision-making on change in risk profile status.

In accordance with clause 7 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015, the decision on The Expert Commission decides on the termination/renewal of electronic risk profiles, except in cases specified in paragraph 11 of Section II.

Clause 9 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015 establishes that The central unit for coordinating the application of the SUR temporarily suspends the effect of the electronic risk profile, including upon submission by the customs authority (its structural unit), in the case of:

1) making changes to documents, the provisions of which were taken into account during developing an electronic risk profile when such changes lead to the need for significant changes to the electronic risk profile;
2) cancellation, loss of validity of documents, the provisions of which are taken into account under time to develop an electronic risk profile;
3) loss of relevance of the electronic risk profile;
4) identification of problematic issues when using the electronic profile risks that cannot be resolved by making changes to it;
5) identification of problematic issues during the programmatic implementation of electronic risk profile;
6) establishing low performance of a particular risk profile and failure to achieve the goal of implementing such a profile.

Clause 10 of Section II of the Order of the Ministry of Finance No. 684 dated 07/30/2015 establishes that decisions regarding electronic profiles taken in accordance with paragraph 9 of this section risk, the programmatic implementation of which was carried out by the central unit for

coordination of the application of the RAS using the UAIS functionality, including
ASMO, are drawn up in the form of a memorandum with a resolution of the manager or
Deputy Head of the Central Unit for Coordination of the Application of the RUS.

Adopted in accordance with Clause 9 of Section II of the Order of the Ministry of Finance No. 684 of 07/30/2015

solutions regarding electronic risk profiles, the software implementation of which was carried out
structural unit for IT issues, are issued in the form of a letter from the central
of the unit for coordination of the application of the RUS to the structural unit for
IT.

The decisions provided for in paragraph 9 shall be taken in relation to the electronic profile.
risk and/or its addition.

Clause 11 of the Section establishes that in the event of elimination of the deficiencies that became the basis for

for the temporary suspension of the electronic risk profile in accordance with paragraph
9 of Section II of the Order of the Ministry of Finance No. 684 dated 30.07.2015, the central unit for
coordination of the application of the RUS makes a decision on the renewal of such a profile
risk, which is drawn up in the manner prescribed for decisions taken in accordance with

to paragraphs 9 of Section II of the Order of the Ministry of Finance No. 684 of 07/30/2015.

Official of the Risk Profiling Unit of the Central Office
enters the risk profile data elements according to the list specified in
table “DE. PR Blocks” - Block 04 “BL04. PR Status”, taking into account the type
electronic risk profile (see “DE. EL PR Views”).

Official of the Risk Profiling Unit of the Central Office
puts DE048 “Mark on the need to implement IT”.

From the moment of setting the value “Yes” DE048 “Mark on the need
IT implementation”, the time limit is set (the timer is set)
in letters regarding the implementation of a change in the risk profile status by the IT department
Central office, taking into account the value of DE049 “Implementation period
information”.

From the moment of posting and storage by the IT department of the Central Office
value “Yes” DE035 “IT mark on change of PR status”, the risk profile acquires
status “PR status changed”.

The final result of the process “RPM 04. Change of PR status” is:

- the risk profile receives the status “PR status changed”.

4.2.5. BP RPM 05. PR Register

Fig. No. 7. Business process: RPM 05. PR register

This process belongs to the “View Information” block and describes the creation of the PR register for the purpose of further statistical data processing.

Customs authorities (see the “Units” Guide) according to the distribution powers (see “AD_2_RPM_Role matrix_v2.1.”) taking into account the list of EDs that available for filtering and searching, defined in the “DE.RPM” table , inflict request criteria according to which the PR register is formed.

By default in the user interface, when viewing risk profiles, they are displayed in accordance with the access criteria, taking into account the requirements given lower:

- the risk profile must not have the status “Deleted” (ST09 Deleted = "No");
- the risk profile should be sorted in descending order by default the values of attributes SN05 “PR implemented” and SN03 “PR approved” with timestamp, according to the “State of PR” Handbook, and allow sorting by all displayed attributes;
- the user should be able to sort the list by any a set of data elements (columns) presented in such a list, with taking into account sorting by other columns, ascending or descending value, with the ability to reset the sort order for the data item in natural order of succession, taking into account numerical values, dates, alphabetical order of text values, etc.;
- the user should be able to filter the list by available for filtering by data elements;
- all restrictions regarding viewing availability are also relate to the possibility of exporting data to external formats;

• detailed requirements for the availability of risk profile data elements for views are given in the DE.RPM table.

List of criteria by which records can be filtered and searched separately defined in the list of data elements (see - DE.RPM).

The above list is basic but not exclusive. It may be changed in depending on the construction of databases and technical capabilities.

For list and reference values, the option should be available indications of all or some values.

For dates, the ability to specify a value range should be available, unless otherwise specified.

The system should provide the ability to pre-display data on the screen for with selected filtering and grouping parameters, with the possibility of unloading selected data in *.xls (and/or *.xlsx, *.csv) format.

The system should allow the user to create a selection request data for all available data elements in the database, their preliminary display in the user interface of such data and outputting it in *.xls (and/or *.xlsx, *.csv) format.

When selecting a separate risk profile, the user, depending on the role models, either all data elements or a limited number of them will be available for viewing list.

From the moment the register is formed, it automatically acquires the status of “Register of PR formed”.

The final result of the process “RPM 05. PR Register” is the formation of the PR register according to given criteria.

4.3. Risk profile states

Risk profile according to the stage of passing the algorithm individually the business process stipulated by the technical requirements for the PIC “MPR” acquires a certain the state recorded by the technical means of the software product.

The list of states provided for the PIC “MPR” is given in the table “Directory. "State of PR".

The transition of states is carried out when the specified technical requirements are met. conditions.

Figure 8 shows the functional diagram of the profile state transition. risk and the conditions under which it occurs.

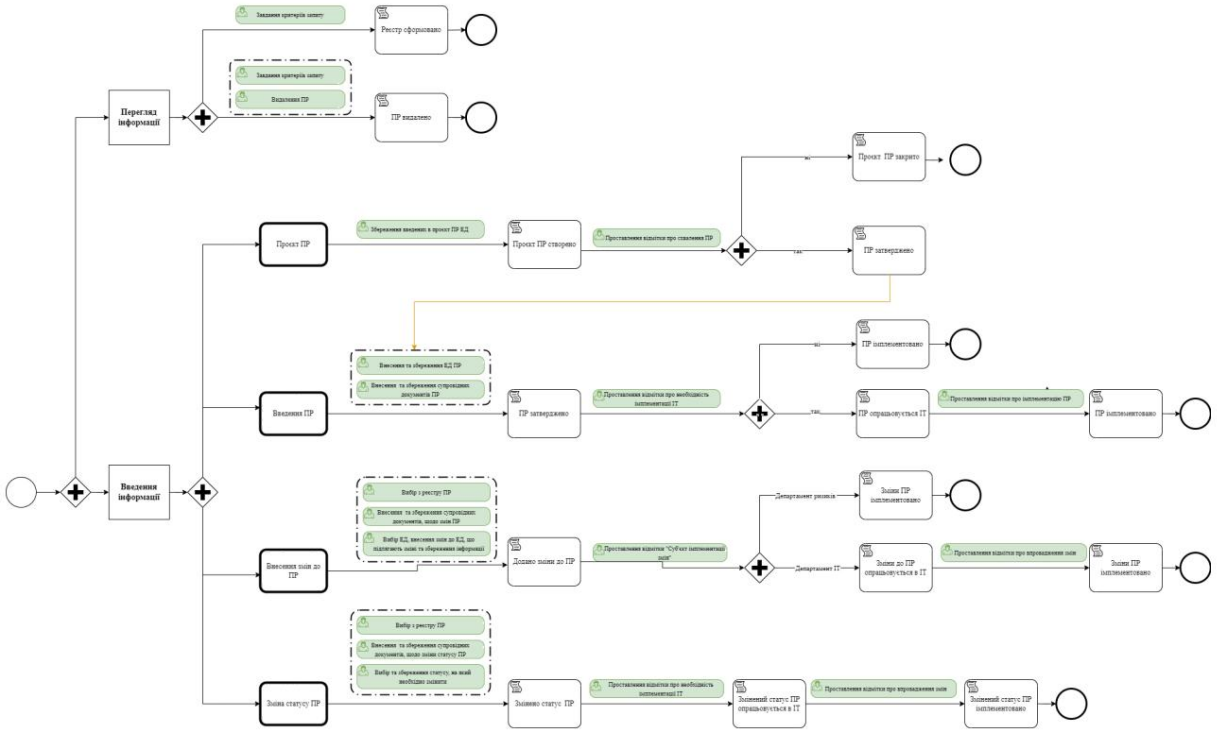

Fig. No. 8. Risk profile states and transition conditions between them

4.4. Description of the Software Product interface

A separate interface is developed for each user group, which adapted to the appropriate maximum set of functions. The interface should be adaptive and scale correctly on screens of different sizes.

Each risk profile should have separate tabs corresponding to the blocks risk profile with a defined list of EDs according to the table “DE.PR Blocks” .

Graphic design must be created using a design system
government websites of Ukraine https://design.gov.ua and comply with the framework of the general ECG design. All interface elements should be easily recognizable on monitors with any contrast and brightness.

The client part of the System must be supported by Google Chrome browsers, Microsoft Edge, Mozilla Firefox latest productive versions at the time of development Software product based on Windows operating systems versions 7, 8, 10, 11, 32/64 bit.

4.5. List of Software Product data elements

The Appendices provide a list and description of data elements and a list and values relevant reference books used in the development and maintenance of the Software -information complex “Risk Profile Manager”.

It should be noted that during the development process, lists of system data elements their meanings etc. can be changed depending on the need and creation electronic document forms.

5. NON-FUNCTIONAL REQUIREMENTS

5.1. Reliability and fault tolerance requirements

The reliability of the elements of the Software Product must be ensured by in the following areas:

- ensuring the operability of the Software Product;
- data storage.

This should require minimal attention from the system administrator. administrator regarding the response to eliminate the consequences of component failures, as well as Data preservation must be ensured by software and hardware.

The software product must provide fault-tolerant operation in the mode 24x7x365 and guarantee availability for end users at a minimum level 99%.

Data retention should be ensured in cases:

- power off;
- failure of technical means of information processing;
- errors, failures or corruption of the software.

System reliability requirements can be specified and should be specified in the revised Technical Requirements.

5.2. Requirements for protecting information from unauthorized access

To ensure the protection of information in the Software Product, it is necessary a combination of the following measures:

1. legislative (taking into account regulations, standards, etc.);
2. administrative and organizational (protection of network systems, especially management systems, selection and control of the activities of personnel involved in creation of a software product);
3. software and technical (use of special hardware and software means that prevent or hinder unauthorized access to network elements and information, checking compliance with requirements technical protection of equipment used in software product).

Information protection in the Software Product is based on the implementation of the following basic principles:

- centralized management of the Software Product;
- sequence of information protection boundaries;
- adequacy and effectiveness of protection;
- maintaining protection during failure of parts of the Software Product;
- protection of safety equipment;
- continuity of protection;
- stealth protection.

5.3. Requirements for protection against external influences

The software product must function exclusively in the INTRANET (departmental communication network) without access by users from the global INTERNET network.

5.4. Requirements for information retention in the event of accidents

The software product must have reliability that ensures 24/7 operation users and rapid recovery in case of failures. In operation The software product must provide for technological breaks during non-working hours. time, which are intended for:

- carrying out preventive work;
- performing version updates;
- other measures necessary for the functioning of the Software Product.

The software product must provide recovery of performance in the event of failures, accidents and failures that occur in network equipment.

The software product must ensure the integrity and preservation of the entered data. data without any loss.

For reliable operation of the Software Product, it is necessary to provide for automatic performing the following actions:

- storing backup copies (creating archives) of data;
- storing backup copies of the software modules of the Software Product, hosted on the servers of the Software Product applications.

The software product as a whole must remain operational when incorrect actions of end users:

- entering incorrect data;
- incorrect exit from the Software product (termination of work with the Software product) on the workstation.

5.5. Information security requirements

The software product must be protected against the most common types of attacks.

The Risk Profile Manager PIC must comply with ISO 31000 requirements (Risk Management), ISO 27001 (Information Security) and ISO 22301 (Business Continuity) regarding threat detection, assessment and response.

1. Threat detection:
- the system must automatically monitor events in real time time using anomaly analysis mechanisms and behavioral patterns;
- all potential threats should be classified according to their level criticality (low, medium, high, critical).

2. Notification and communication:
- Threat reports should be automatically transmitted to responsible persons through secure communication channels;
- the message format must comply with the ISO 22301 crisis management standard communications and contain:
  - incident identifier;
  - threat category;
  - recommended actions for remediation;
  - contact information of responsible persons.

3. Threat elimination:
- system requirements define threat elimination algorithms in accordance with ISO 27035 (information security incident management), including:
  - automated threat neutralization mechanisms;
  - clearly defined procedures for manual incident resolution;
  - verification of threat elimination using logging mechanisms and audit.

- all actions to detect, notify and eliminate threats must be recorded in centralized logging system, in accordance with ISO 27001 requirements;
- Incident reports should be generated periodically, including analysis causes, assessment of the effectiveness of measures and recommendations for prevention similar situations in the future.

The software product must use methods already available in the EAIS user identification and authentication.

At the physical level, the following rules must be followed:

- physical access to equipment must be limited and all actions must be be fixed;
- physical access to system backups should be limited in accordance with the system administration regulations and all actions must be fixed;
- the system must have functionality to limit the number of requests to the database from to protect it from overload.

If, during the deployment of the Software Product, it becomes necessary obtaining an Expert Opinion based on the results of state expertise in the field technical information protection, the developer of the Software Product provides (or contributes to obtaining a positive Expert opinion in accordance with the legislation of Ukraine) conclusion.

5.6. Requirements for patent purity

To all software and hardware used in The terms of the license agreements must be complied with for the software and information complex and patent purity is ensured.

If it is determined that the Software Product needs to be integrated with another system using an exchange protocol or algorithm for which there are restrictions in Ukraine, permission to use such a protocol or algorithm must be obtained from the competent authorities before implementing the integration and introducing it into operation.

5.7. Requirements for standardization and unification

Standardization and unification of the functions of the Software Product should be ensured through the use of modern software tools,
which support a single technology for designing and developing functional,
information and software.

The Software Product as a whole, and other software components of the Software product must comply with major international and national agreements and
standards in the field of information technology.

5.8. Software Product Power and Speed Requirements

The power of the elements of the Software Product must be designed for processing the appropriate number of requests with double the reserve.

The power is calculated taking into account the additional load due to
using the system at different stages of the customs procedures lifecycle. In general
The software product must support simultaneous operation of ~ 100 users in
system, the average activity of which is planned at the level of: up to 80 users on average per day (direct and indirect).

The interface response time should not exceed 0.5 seconds.

5.9. Information requirements

Information support must meet the following requirements and possibilities:

- ensuring physical and logical data integrity;
- minimizing the redundancy of stored data;
- standardization of data representation;
- reliability and relevance of data;
- flexible change of algorithms in accordance with changes in legislation.

The software product must have the properties of an integrated information system. environments:

- ensure the storage of data on the history of data changes by users for ensuring responsibility for making changes to data;

- ensure the distribution and provision of access rights based on role or another similar principle;
- provide for the possibility of integration with a documented API other information systems.

5.10. System Scaling Requirements

Each element of the Software Product must be designed with taking into account the possibility of scaling. All modules of the Software Information System The complex must have the ability to scale horizontally and vertically. The database servers that will use the Software Product must have the possibility of vertical or, if possible, horizontal scaling.

5.11. User interface requirements

Inspectors access the Software Product through a centralized web interface. A unified interface is being developed for each user role with different levels of functionality. The interface should be adapted for both for both the minimum and the maximum set of functions (elements). It is necessary to provide for the universality of interfaces for different functionalities and to lay down the following expanding the list of functions available to users.

The website must be responsive and scale correctly on screens of different sizes. size and resolution. The system website must be adapted to display in the latest versions of browsers such as: Microsoft Edge, Google Chrome, Mozilla Firefox.

5.12. Requirements for types of collateral

5.12.1 Requirements for linguistic support

The language of interaction between users and the software product is Ukrainian. It is necessary to provide that:

- all documents and reports of the Software Product are prepared and output in Ukrainian;
- the graphical user interface of the Software Product must be created in Ukrainian.

5.12.2. Requirements for methodological support

There are no special requirements.

5.12.3. Requirements for organizational support

Organizational support for the functioning of the Software Product must be based on the existing organizational structure and anticipate possible changes in processes of business process execution that do not require significant changes in the organizational structure.

The developer trains personnel with software components and accompanies the process of implementation and trial operation of the software product.

Software performance testing should take place on the server equipment of the State Customs Service.

Testing includes the following types of testing:

- functional testing – checking the compliance of the system's operation with its requirements;
- performance testing - assessment of speed and load resistance;
- security testing - determining the level of protection against potential threats and vulnerabilities.

Testing is performed as the development stages are completed. results are carried out in accordance with the testing program and methodology.

5.13. Requirements for the development and modernization of a software product

The system must be flexible to upgrade in accordance with changes in legislation throughout the entire period of operation.

6. ADMINISTRATIVE INFRASTRUCTURE

6.1. Placement of the Software Product

For the development and implementation period - The software product must be hosted on the servers of the State Customs Service.

6.2. Backup and disaster recovery system

Within the framework of the development of the Software Product, mechanisms must be provided backup, backup schedule and instructions for
recovery of the Software Product after accidents.

Software Product Recovery includes:

- restoring system and application software configurations;
- restoring user information;
- data recovery.

6.3. Logging system

The software product must provide for integration with central logging modules of the State Customs Service, which provides for logging of the following events:

- starting/stopping individual services of the Software Product;
- login/logout security events;
- all actions are provided in the business process RPM 01. - RPM 05. (creation, modification, deletion);
- errors in the operation of the Software Product, such as communication, integrity data in the subsystem, unpredictable delays in information processing;
- critical events from the monitoring system (critical memory volume, disk space, etc.);
- other security events.

6.4. Monitoring system

The software product must provide for integration with central monitoring modules of the State Customs Service, which provides for operational monitoring operation of all subsystem components (quantity, current state, etc.), including the CPU,

RAM, Disk I/O and free space on the disk system, load, channel availability

communication.

7. TECHNOLOGY STACK

The software must be developed using technologies that
that provide high performance, scalability, availability and compatibility with
existing infrastructure solutions of the organization. Considering the requirements for
technological environment, the following technical specifications are offered for
system development:

Back-end programming stack:

- the development platform must support .NET execution
  Framework 4.8 or other compatible platform that allows development
  C# applications.

Programming stack for front-end:

- a framework must be used to implement the user interface
  Blazor (version 9.0), or other frameworks with similar functionality
  capabilities that meet the requirements for interactivity,
  interface adaptability and in the future with the possibility of switching to Blazor
  (version 9.0).

Server architecture:

- database: The system must support a relational database compatible with
  MS SQL Server 2019 or later versions, with the ability to implement
  high availability (AlwaysOn);
- infrastructure: Windows Server 2019 x64 operating system or later, with
  support for Hyper-V hypervisors (version 7 or later) or ESXi 7 and higher;
- web server: Requires IIS WebServer support or other compatible
  a web server that meets security and scalability requirements.

System requirements:

1. High Availability: The system must provide
   constant availability even in the event of individual component failures.
2. Fault Tolerance: Ensuring continuous operation in the event of
   hardware or software failures.
3. Redundancy: The system should include redundant components
   to prevent downtime.

4. Horizontal Scaling ability: Ability
   increasing capacity by adding new nodes to the system.
5. Monitoring (Observer): The system should include monitoring mechanisms
   for prompt identification and resolution of problems.

8. PROCEDURE FOR CONTROL AND ACCEPTANCE OF THE SOFTWARE PRODUCT

Expected completion date for development and deployment of the Software Product The Contractor - 9 months, starting from the day after signing the contract for development of PIC.

Control and acceptance of the developed Software Product are carried out through tests, which consist in checking the performance The software product as a whole or its components according to the documentation Software product and in order to establish its compliance with the technical the task for creating the Software Product and other software documentation product.

Testing and acceptance of the Software Product is carried out by the acceptance by a commission, which is formed and the composition of which is approved by order of the State Customs Service.

A report (protocol) is drawn up based on the results of testing the Software Product. about his ordeal.

Acceptance of the Software Product into experimental or industrial operation is carried out on the basis of an order of the State Customs Service.

The software product must have the following documentation:

Table No. 4. Software Product Documentation.

No.	Type of Software Product Documentation	Performer
1.	Technical specifications for the creation of a Software Product	State Customs Service
2.	Specification: • description of the Software Product architecture • detailed L2/L3 topology of the network architecture of the Software Product deployment in the form of a diagram; • database structure. • instructions for deploying the development environment • developer documentation • API documentation for the developer, which is generated automatically: • has a list of supported methods and their description;	Developer

	• has a list of query parameters and their description; • has a list of response attributes and their description; • allows emulating a request/response with a description of the response status (success, error).	
3. Program code		Developer
4. Testing program and methodology		Developer
5. User instructions		Developer
6. Training program and training materials users of different roles		State Customs Service

The above list is not exhaustive, the specific composition and content of the documentation The software product is determined during the implementation of an IT project.

ДОДАТКИ

Додаток 1: Елементи даних та довідники, що використовуються при веденні Програмного інформаційного комплексу “Менеджер профілів ризику”.

Додаток 1 складається з наступних частин:

- Таблиця. DE.RPM
- Таблиця. Формат DE044 “Номер документа”
- Таблиця. DE.Блоки ПР
- Таблиця. DE.Види ЕЛ ПР
- Блоки ПР
- Довідник. Стан ПР
- Довідник. Статус ПР
- Довідник. Тематика документів
- Довідник. Модулі АСУР
- Довідник. Підрозділи
- Довідник. Назва документу
- Довідник. Підстави змін Деп.ризиків
- Довідник. Підстави тим. призупинення Деп. ризиків

Додаток 2: Матриця рольової моделі ПІК “МПР”.

- Таблиця. Matrix. Role (Data Elements)
- Таблиця. Matrix. Rights

Додаток 3: Шаблон друку профілю ризику.

Директор Департаменту з питань
цифрового розвитку, цифрових
трансформацій і цифровізації — Аліна БРЕНДАК