# Annex 1 to RFP-23-022

# Information and communication system «POLITICAL FINANCE PORTAL» (POLITDATA 2.0)

# TECHNICAL REQUIREMENTS

# Table of contents

## List of conventional abbreviations

| | |
|---|---|
| API | Application programming interface, a software interface that provides interaction with external systems |
| Business process, BP | A set of interrelated or interacting types of activities aimed at creating a certain product or service |
| CEC | Central Election Commission |
| CIPS | Comprehensive information protection system |
| DBMS | Database management system |
| ECoU | Election Code of Ukraine |
| EFA/RFA | Election fund accounts / Referendum fund accounts |
| ICS | Information and communication system |
| IFES | International Foundation for Electoral Systems |
| IS | Information system |
| IT | Information Technology |
| Law | Law of Ukraine “On Prevention of Corruption” dated 14.10.2014 No. 1700-VII |
| NACP | National Agency on Corruption Prevention |
| NBU | National Bank of Ukraine |
| POLITDATA | Unified State Register of Political Parties’ Reports on Property, Income, Expenses and Financial Liabilities |
| QES | Qualified electronic signature |
| QPETS | Qualified provider of electronic trust services |
| RBP | Reengineering of business processes |
| RNTAC | Registration number of the taxpayer's account card |
| SM | Software module |
| SS | Software subsystem |
| SSU | State standard of Ukraine |
| SW | Software |
| System | Information and communication system “Political finance portal” |
| TEC/DEC | Territorial election commission / district election commission |

# 1. Introduction

## 1.1. Basis for carrying out work

Taking into account the positive results of the operation of POLITDATA and in compliance with CEC Resolution No. 90 of August 12, 2022, the submission and implementation of state control of financial reports on the receipt and use of funds of election funds of political parties, their local organizations, candidates in national and local elections, provided for by the Election Code of Ukraine, should be implemented with the help of improved (modernized) POLITDATA electronic services.

This document has been prepared for the adoption of technical requirements for conducting open tenders for the creation of specialized software of the "Political finance portal" information and communication system (hereinafter - System) through the modernization of POLITDATA.

The regulatory and legal basis for the development of the System is the Election Code of Ukraine and the Laws of Ukraine "On Prevention of Corruption", "On Access to Public Information", "On Protection of Information in Information and Communication Systems", "On Information", "On Protection of Personal Data", "On electronic trust services", "On political parties in Ukraine", "On the all-Ukrainian referendum".

## 1.2. Name of the customer and payer organizations

Customer: National Agency on Corruption Prevention (abbreviated as NACP)

Payer: International Foundation for Electoral Systems (IFES)

## 1.3. List of regulatory and technical documents, methodical materials used in the preparation of technical requirements.

List of normative legal acts, methodical materials, technical documents used in the preparation of technical requirements (hereinafter - TR):

- Election Code of Ukraine;
- Law of Ukraine "On Prevention of Corruption";
- Law of Ukraine "On Political Parties in Ukraine";
- Law of Ukraine "On All-Ukrainian Referendum";
- Law of Ukraine "On access to public information";
- Law of Ukraine "On electronic trust services";
- Law of Ukraine "On Electronic Documents and Electronic Document Management";
- Law of Ukraine "On information protection in information and communication systems";
- Law of Ukraine "On Public Electronic Registers";
- Draft law "On local referendum" (reg. No. 5512 dated 05/19/2021);
- Decree of the President of Ukraine dated July 29, 2019 No. 558 "On some measures to improve the access of individuals and legal entities to electronic services";

- Resolution of the NBU dated 15.07.2020 No. 102 "On approval of the Procedure for opening and closing accounts of election funds and all-Ukrainian referendum funds";
- Resolution of the NBU Board dated July 29, 2022 No. 162 "On the approval of the Instructions on the procedure for opening and closing user accounts by providers of payment services for account maintenance";
- Resolution of the Board of the NBU of April 14, 2023 No. 49 "On approval of the Regulation on the use of means of cryptographic protection of information of the National Bank of Ukraine";
- Resolution of the CEC of February 4, 2022 No. 20 "On the procedure for control over the receipt, accounting and use of money from the fund of the initiative group of the All-Ukrainian referendum on the people's initiative, the campaign fund regarding the initiative of holding";
- Resolution of the CEC of September 10, 2020 No. 245 "On Recommendations regarding control over the receipt, accounting and use of money from election funds of local organizations of political parties, candidates for deputies, candidates for the post of village, settlement, and city mayor";
- Resolution of the CEC of October 1, 2020 No. 324 "On the forms of financial reports on the receipt and use of money from election funds of local organizations of political parties, candidates for deputies, candidates for the post of village, settlement, city mayor, the procedure for their preparation and analysis";
- Resolution of the CEC dated 12.08.2022 No. 90 "On some issues of submission of financial reports provided for by the Election Code of Ukraine on the receipt and use of money from election funds of political parties, their local organizations, candidates in national and local elections";
- NACP order dated February 19, 2021 No. 102/21 "On some issues of submitting reports of political parties on property, income, expenses and obligations of a financial nature";
- NACP order dated 07.05.21 No. 252/21 "On acceptance into permanent (industrial) operation of the information and telecommunications system "Unified State Register of Political Parties' Reports on Property, Income, Expenses and Financial Liabilities";
- NACP order dated 14.01.2021 No. 6/21 "On some issues of checking the reporting of political parties on property, income, expenses and obligations of a financial nature";
- Letter of the Ministry of Digital Transformation of Ukraine dated August 21, 2022 No. 1/04-2-7098;
- SSU 3918-1999 (ISO/IEC 12207:1995) "Software life cycle processes";
- Decision of the Board of the NBU dated January 3, 2017 No. 2-rsh (with changes) "On approval of the Public Offer of the National Bank of Ukraine for the

conclusion of a Unified Agreement for banking services and the provision of other services by the National Bank of Ukraine."

## 2. Characteristics of the object and the existing system of activity

### 2.1. General characteristics of the object

The National Agency on Corruption Prevention is a central body of executive power with a special status. NACP is responsible for the formulation of anti-corruption policy and prevention of corruption.

In accordance with paragraph 8-1 of part one of Article 11 of the Law of Ukraine "On Prevention of Corruption", the powers of the NACP include the exercise of state control over:

- compliance with legal restrictions on financing political parties, legal and targeted use by political parties of funds allocated from the state budget to finance their statutory activities, timely submission and completeness of party reports on property, income, expenses and financial obligations;
- timeliness of submission and completeness of reports on the receipt and use of money from election funds at national and local elections;
- the timeliness and completeness of submission of reports on the receipt and use of money of the campaign fund regarding the initiative to hold an all-Ukrainian referendum, reports on the receipt and use of money of the All-Ukrainian referendum fund, reports on the receipt and use of money of the initiative group fund.

According to Art. 18 of the Law of Ukraine "On Political Parties in Ukraine" the powers of the NACP, in terms of state control over the activities of political parties, include the control of:

- in compliance with the limitations established by law regarding the financing of political parties, pre-election campaigning, campaigning for the All-Ukrainian and local referendum;
- according to the legal and targeted use by political parties of the funds allocated from the state budget to finance their statutory activities;
- according to the timeliness of submission of party reports on property, income, expenses and obligations of a financial nature, reports on the receipt and use of money of election funds in national and local elections, the completeness of such reports, compliance with their design according to the established requirements, and the reliability of the information included in them.

In accordance with the requirements of Articles 97 and 153 of the Election Code of Ukraine, managers of election funds are required to submit financial reports on the receipt and use of money from election funds. The specified reporting requirements relate to the use of money from the election fund of the candidate for the post of President of Ukraine, as well as the election fund of the party or the candidate's own election fund in the elections of People's Deputies of Ukraine.

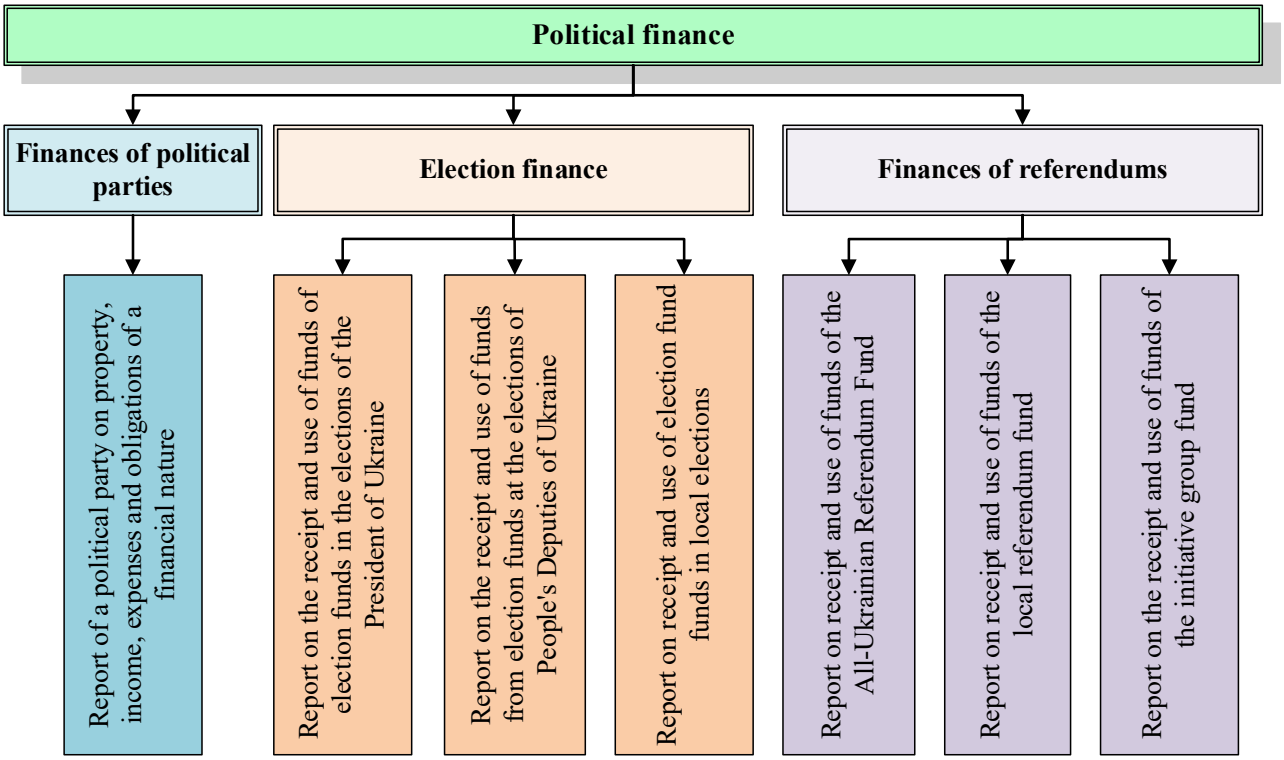
With the aim of practical implementation of the above-mentioned norms of the Election Code of Ukraine, CEC Resolution No. 90 dated 12.08.2022 initiated preparatory measures for the introduction of the submission of financial reports on the receipt and use of money from election funds provided for by the Election Code of Ukraine using electronic services.

The general goal of the creation and implementation of the "Political finance portal" information and communication system (hereinafter - the System) is to increase the effectiveness of NACP's exercise of the powers specified by the Law, including monitoring and control over the implementation of legislative acts regarding financing and legal and targeted use by participants in the political process (political parties, election candidates, participants in all-Ukrainian and local referenda) of funds, verification of possible facts of violations of the requirements of the Law by subjects to which the requirements of the Law apply, systematization and generalization of the practice of applying the provisions of the Law, analysis of conducted inspections of the subjects of the Law, inspections of financial reporting of political parties and on the receipt and use of money from election funds, other response measures provided for by the Law.

## 2.2. Characteristics of the existing activity of the object and its structural elements with an indication of the distribution of functions between the elements of the organizational structure

A list of the main groups of objects for which NACP control activities can be automated by implementing System is provided in the following figure:

**The main groups of objects in respect of which the control activity of the NACP can be automated by implementing the ICS PFP**




The list of business processes, the implementation of which is entrusted to the NACP structural divisions and which are subject to automation within the System, is provided in the following table:

| # | Business process | Object | Normative document |
|---|---|---|---|
| 1 | Ensuring the submission to the NACP | Report of a political party | Art. 17 of the |

| | | | |
|---|---|---|---|
| | of a report on property, income, expenses and obligations of a financial nature (including its local organizations that have acquired the status of a legal entity in the prescribed manner) by filling it out on the official website of the National Agency Corruption Prevention. | on property, income, expenses and obligations of a financial nature | Law of Ukraine "On Political Parties in Ukraine" |
| 2 | Implementation of state control over the activities of political parties:<br>- in compliance with the limitations established by law regarding the financing of political parties;<br>- according to the legal and targeted use by political parties of the funds allocated from the state budget to finance their statutory activities;<br>- according to the timeliness of submission of party reports on property, income, expenses and obligations of a financial nature, the completeness of such reports, the compliance of their design with the established requirements, the reliability of the information included in them. | Report of a political party on property, income, expenses and obligations of a financial nature | Art. 18 of the Law of Ukraine "On Political Parties in Ukraine" |
| 3 | Ensuring the submission to the NACP of a report on the receipt and use of money from election funds for the presidential elections of Ukraine | Report on the receipt and use of money from election funds in the elections of the President of Ukraine | Art. 97 of the Election Code of Ukraine |
| 4 | Control of election funds in the elections of the President of Ukraine | Report on the receipt and use of money from election funds in the elections of the President of Ukraine | Art. 94 of the Election Code of Ukraine |
| 5 | Ensuring the submission to the NACP of a report on the receipt and use of money from election funds at the elections of People's Deputies of Ukraine | Report on the receipt and use of money from election funds in the elections of People's Deputies of Ukraine | Art. 153 of the Election Code of Ukraine |
| 6 | Analysis of the report on the receipt and use of money from election funds in the elections of people's deputies of Ukraine | Report on the receipt and use of money from election funds in the elections of People's Deputies of Ukraine | Art. 153 of the Election Code of Ukraine |
| 7 | Ensuring submission of a report on the receipt and use of money from | Report on receipt and use of money from election | Art. 214 of the Election Code |

| | | | |
|---|---|---|---|
| | election funds in local elections | funds in local elections | of Ukraine |
| 8 | Analysis of the report on the receipt and use of money from election funds in local elections | Report on receipt and use of money from election funds in local elections | Art. 213[1] of the Election Code of Ukraine |
| 9 | Ensuring submission of a report on the receipt and use of money from the All-Ukrainian Referendum Fund | Report on receipt and use of money from the All-Ukrainian Referendum Fund | Art. 33, 71 of the Law of Ukraine "On the All-Ukrainian Referendum" |
| 10 | Analysis of the report on the receipt and use of money from the All-Ukrainian Referendum Fund | Report on receipt and use of money from the All-Ukrainian Referendum Fund | Art. 33, 71 of the Law of Ukraine "On the All-Ukrainian Referendum" |
| 11 | Ensuring the submission of a report on the receipt and use of money from the local referendum fund | Report on receipt and use of money from the local referendum fund | Art. 64 of the draft law "On local referendum" |
| 12 | Analysis of the report on the receipt and use of money from the local referendum fund | Report on receipt and use of money from the local referendum fund | Art. 64 of the draft law "On local referendum" |
| 13 | Ensuring the submission of a report on the receipt and use of money from the initiative group fund | Report on the receipt and use of money from the initiative group fund | Art. 70, 71 of the Law of Ukraine "On the All-Ukrainian Referendum" |
| 14 | Analysis of the report on the receipt and use of money from the initiative group fund | Report on the receipt and use of money from the initiative group fund | Art. 33, 71 of the Law of Ukraine "On the All-Ukrainian Referendum" |

The main purpose of the ICS PFP is to automate the reporting of all categories of political finance, as well as to automate the state control carried out by the NACP.

The main goal of ICS PFP is the automation of processes and performance of tasks assigned to NACP in accordance with the laws of Ukraine, for:

1) enabling political party leaders to submit party reports on property, income, expenses and financial obligations in electronic form;
2) enabling EFA/RFA managers to submit reports on the receipt and use of money from election funds in the elections of the President of Ukraine and the elections of People's Deputies of Ukraine, as well as in local elections in electronic form;
3) providing an opportunity for account managers to submit in electronic form reports

on the receipt and use of money from the All-Ukrainian or local referendum fund, as well as reports on the receipt and use of money from of the initiative group fund;
4) provision of obtaining information from national electronic information resources, other information and communication systems in accordance with agreed regulations;
5) implementation of NACP state control over compliance with statutory restrictions on financing political parties, legal and targeted use by political parties of funds allocated from the state budget to finance their statutory activities;
6) implementation of NACP state control over the timeliness of submission and completeness of parties' reports on property, income, expenses and obligations of a financial nature;
7) implementation of NACP state control over the timeliness of submission and completeness of reports on the receipt and use of money from election funds at national and local elections;
8) implementation of NACP state control over the timeliness of submission and completeness of reports on the receipt and use of money from the campaign fund regarding the initiative to hold an all-Ukrainian referendum, reports on the receipt and use of money from the All-Ukrainian (local) referendum fund, reports on the receipt and use of money from the initiative group fund;
9) ensuring the interaction of NACP analysts with party leaders, EFF managers and referendum account managers through personal offices by creating official electronic documents (letters, requests, messages, etc.);
10) provision of open round-the-clock access of citizens to the public part of ICS PFP with the possibility of viewing, copying and printing information, including in the form of a data set organized in a format that enables its automated processing by electronic means (machine reading) for the purpose of reuse (in open data form), in accordance with the Law of Ukraine "On Access to Public Information";
11) monitoring of the information space and analysis of information published in online mass media, social networks, etc.;
12) performance of other tasks defined by legislation.

## 3. Goals, criteria and restrictions of IS creation

### 3.1. Designation of economic, scientific, technical and economic goals of IS creation

As part of the implementation of the System, it is envisaged to create a single mechanism for processing (collection, analysis, control, access) information in the field of political finance (financial reporting of political parties, election funds and referendum funds) to ensure a centralized and unified process based on the principles of modular architecture.

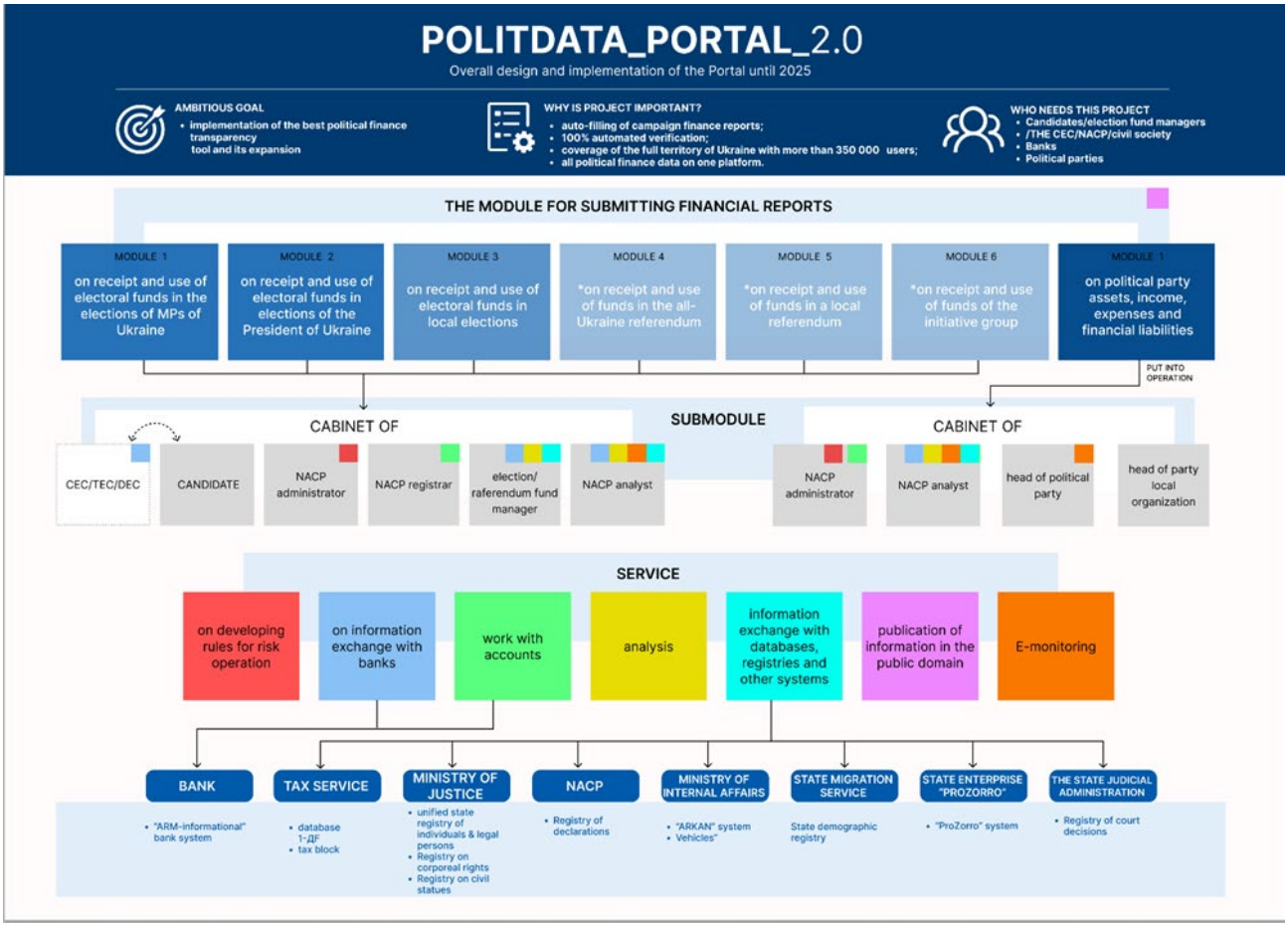
According to CEC Resolution No. 90 of August 12, 2022, a decision was made regarding the possibility of introducing the submission of financial reports provided for by the Election Code of Ukraine on the receipt and use of money from election funds of political parties, their local organizations, candidates in national and local elections using POLITDATA electronic services. It is thanks to this approach to implementation that standardization and unification of the entire process of providing financial reporting of political parties, election funds and referendum funds will be achieved:

- in the process of designing new elements of the system, technologies and approaches to the development of application software already implemented in POLITDATA will be used;

- a single user interface and information processing procedures will be used, identification of software elements and databases, typification of individual software modules according to their purpose in various functional subsystems;
- project solutions for information support will provide for the maximum use of unified forms of input and output documents;
- project solutions for information support will provide for the maximum use of local, system-wide and national classifiers.

The main principle of the proposed mechanism is to focus on reducing the overall complexity of System program parts and the possibility of using common solutions. The resulting modular architecture emphasizes the division of application functionality into independently variable modules such that each module contains everything necessary to perform only one aspect of the required functionality.

Thus, when adding a new type of reporting of political parties, election funds, and referendum funds to the System, the existing mechanism of already implemented reports is used without the need to reconfigure them (see the following figure), which obviously leads to the effective use of resources (organizational, financial, time, security) by avoiding duplication of functions (a detailed description of typical business processes is provided in Appendix 1).




The System should form a single information space, in which the interaction of the processes of carrying out audits of financial reporting is ensured through the use of common information objects. The implementation of the specified mechanism will allow to obtain additional effectiveness of the work of NACP employees in the analysis of reports, since this single mechanism will be connected to all sources of information exchange with other

registers, both external and internal, which automatically expands the development of the analysis of each type of report separately.

Implementation of the System will improve the efficiency and effectiveness of the work of NACP employees, their executive discipline, in particular:

- improve the efficiency of NACP employees due to the efficiency, reliability, completeness, availability, multivariate and reliability of accounting, processing, accumulation, transmission and presentation of primary, operational, directive, reporting and reference information regarding financial reporting;
- unify the processes of financial reporting analysis due to the observance of uniform standards for inspection processes and documents formed in the inspection process;
- ensure operational exchange of information between NACP and CEC structural units;
- improve the quality, efficiency and effectiveness of the management of the inspection process based on the decisions made by the NACP based on the results of using the System;
- to ensure electronic information interaction with information systems of NACP, executive authorities and other organizations, including when implementing interdepartmental information interaction.

Main functional tasks:

- automation of processes related to the performance of NACP functions and defined in section 2.2, in full;
- consolidation of information received by NACP for the exercise of its powers, in terms of unique identifiers of reporting entities;
- provision of data exchange with external ICS;
- ensuring process execution control;
- development of the analytical reporting system, including data collection from various sources, systematization and structuring of information for the purpose of analysis, creation of various forms and types.

After implementation, the System should:

- increase the efficiency of performing the tasks assigned to NACP thanks to the automation of business processes, which reduces the labor costs and time required to perform the functions of financial reporting audits;
- get rid of duplicated data and implementing interdepartmental communication mechanisms, which will ultimately increase operational efficiency, including NACP, CEC and banking institutions;
- create flexible architecture for performing inspections (control) with stricter compliance with legal requirements due to the built model integrated into the software;

- simplify communication procedure with reporting subjects, including the identification and authorization procedure in the System;
- provide more accurate information thanks to a centralized data source and a unified presentation of data on each reporting entity;
- simplify the decision-making procedure due to optimized interaction between NACP, CEC and banks (and external sources of information) and higher transparency of policies and algorithms;
- expand access to information thanks to a centralized data repository, where information is available around the clock;
- obtain additional information thanks to built-in analytics, which allows users to combine accurate data from various sources and systems to align strategy with the implementation process within the entire competence of NACP;
- ensure stricter cost control, reduction of operational risks due to increased responsibility, which will ultimately contribute to more accurate results of audits of reporting entities.

### 3.2. Restrictions related to the creation of IS

Information and communication system "Political finance portal", which is being designed, will partially or fully interact with automated systems already used by NACP.

The information that will be processed in ICS, depending on the purpose, is divided into:

- open information;
- confidential information;
- technological information.

According to the content of protection requirements, the information processed in ICS is divided into the following categories:

- open information;
- confidential information.

According to the normative document of technical information protection 2.5-005-99, ICS is classified as an automated system of class "3".

ICS is a multi-machine, multi-user complex, which includes a computer system, the physical environment in which it is located and functions, the user environment, processed information, including its processing technology.

**Information security requirements**

According to the requirements, the System should consist of the following main sections:

- section with confidential information;
- section with open information.

In accordance with regulatory requirements for information protection in automated systems, the SW of each System section must have a set of protection tools of the appropriate level.

Since the functional requirements for the SW of the specified System partitions do not differ significantly, namely, users are given the opportunity to add and search for information and form extracts or references in electronic format, the software of the partitions will differ in the configuration of information protection tools.

At the same time, for each of the sections, a separately developed set of information protection tools should be provided in accordance with regulatory requirements and in accordance with the characteristics of the stored data.

The hardware and software complex must include a set of measures to ensure the necessary level of integrity, availability and confidentiality of information.

User access rights (roles, groups) should be defined and implemented based on defined access levels.

A set of user access rights must be ready for further use and administration.

Security requirements can be specified at the stage of technical design of the System and outlined in the Technical Task.

The System must ensure reliable protection of information against violation of its integrity, leakage and blocking in accordance with the procedure established by regulatory and legal state acts and regulatory documents in the field of information protection.

**The construction of CIPS is not included in the scope of this procurement.**

**CIPS will be created during the implementation of a separately concluded contract based on the results of a separate competitive procurement procedure.**

**The bidder who will be awarded the contract is obliged to correct all errors in the software that will be discovered during the creation of the CIPS, including during the warranty service period.**

## 4. Functions and tasks of the IS being created

### 4.1. Justification of the selection of the list of automated functions and sets of tasks with an indication of the sequence of implementation

The list of information and communication (automated) systems, application software complexes currently used by NACP to perform the functions of conducting financial reporting audits is given in Table 1. The list describes which of these systems will be decommissioned after the implementation of the System, and with which it is necessary to implement electronic information interaction.

Table 1

| # | ICS name | Year of implementation | Integration method |
|---|---|---|---|
| 1 | Unified State Register of Political Parties' Reports on Property, Income, Expenses and Financial Liabilities (POLITDATA). | 2021 | Will be decommissioned by absorption |

| | | | |
|---|---|---|---|
| 2 | Automated non-payment information exchange workplace (ARM-INF) | 2022 | API* |
| 3 | Information and telecommunication system "Case Management System" | 2021 | API* |
| 4 | NACP official website | 2018 | API* |

* - a detailed description of the API requirements of each ICS must be developed at the stage of the System technical project and implemented at the corresponding stages of the System development by the System developer and/or the ICS developer, depending on the agreed API option.

The general structure of the ICS PFP software subsystems is graphically presented in section 3.1.

The main parameters of the ICS PFP software subsystems are determined by the logic and features of the business processes to be automated (the list is provided in section 2.2). In accordance with the tasks assigned to the NACP according to the current legislation and draft laws, it is worth grouping the specified business processes according to the type of reporting:

1) Business process «Submission and verification of financial reporting of political parties on property, income, expenses and obligations of a financial nature» (BP VFR-PP);
2) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the presidential elections of Ukraine» (BP VFR-EFFP);
3) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the elections of People's Deputies of Ukraine» (BP VFR-EFFPD);
4) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in local elections» (BP VFR-EFFLE);
5) Business process «Submission and verification of financial reporting on the receipt and use of money from the All-Ukrainian Referendum Fund» (BP VFR-RFFUA);
6) Business process «Submission and verification of financial reporting on the receipt and use of money from the local referendum fund» (BP VFR-RFFL);
7) Business process «Submission and verification of financial reporting on the receipt and use of money from the initiative group fund» (BP VFR-RFFG).

It should be noted that BP VFR-EFFP, BP VFR-EFFPD, BP VFR-EFFLE, BP VFR-RFFUA, BP VFR-RFFL and BP VFR-RFFG are practically identical in their general logic. It is this fact that determines the presence in each of the corresponding SS of the same set of SMs covering the same set of corresponding BP steps.

In particular, each of the six SS (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) contain the following SMs in their structure:

- SM "Workstation of NACP registrar";
- SM "Workstation of the manager of EFA/RFA";
- SM "Workstation of NACP analytics".

Common and specific features of the above SMs within the implementation of the above BP (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) are given in the description of each individual SS (Appendix 1 to this Technical Task).

As for VFR-PP, it contains a unique (different from other SS in ICS PFP) set of such SM:

- SM "Workstation of the head of analysts";
- SM "Workstation of NACP analytics";

- SM "Party Leader's Workstation";
- SM "Workstation of the head of the regional office";
- SM "Workstation of the authorized person for filling out the report".

Of particular importance in the ICS PFP structure is the SS CSM, which interacts with all the above-listed SS and includes a set of such SMs (a detailed description is provided in Appendix 1 to these Technical Requirements):

- SM writing the rules of risk operations;
- SM exchange of information with banks;
- SM work with accounts;
- SM of logical and arithmetic control (analytics);
- SM information exchange with other ICS (registries, databases, etc.);
- SM publication of information in the public part of ICS PFP;
- SM e-monitoring.

Taking into account the positive results of the operation of POLITDATA and in compliance with CEC Resolution No. 90 of August 12, 2022, the submission and implementation of state control of financial reports on the receipt and use of money from election funds of political parties, their local organizations, candidates in national and local elections, provided for by the Election Code of Ukraine, should be implemented with the help of improved (modernized) POLITDATA electronic services.

Given the further perspective of expanding the number of reports to be submitted and state control, it is appropriate to create ICS PFP by modernizing POLITDATA.

Thus, the general structure of the ICS PFP in the form of a portal will ensure the organization of a single information space in the process of working with information for all financial reporting systems of political parties, election funds and referendum funds, unification and centralized management of directories and classifiers with the ability to manage their structure and information content and, if necessary in the future, scaling (expanding) the functionality of the portal.

In turn, the existing "Unified State Register of Political Parties' Reports on Property, Income, Expenses and Financial Liabilities" with the available data in its entirety remains unchanged and should become the SS VFR-PP of the new ICS PFP.

**Stages of creating System**

| **Stage** | **Phase of work** |
|---|---|
| 1. Formation of IS requirements. Development of the IS concept | 1. Survey of the automation object |
| 2. Technical specification | 2. Development of the technical specification |
| 3. Technical project | 3. Development of a technical project |
| 4. Working documentation | 4. ICS PFP software development |
| 5. Implementation | 5. Testing of System software in the scope of preliminary tests.<br>6. Introducing the System into trial operation |
| 6. IS support | 7. Provision of services related to System warranty service<br>8. Provision of services related to post-warranty maintenance of the System (not included in the scope of this purchase). |

It is allowed to carry out individual phases of work before the completion of previous phases, parallel in the time of execution of phases of work, inclusion of new phases of work taking into account the specifics of the IS under construction.

**Phases of System construction and reporting**

| # | The name of the phase | |
|---|---|---|
| **1.** | **Survey of the automation object.** | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Conduct an analysis of information, information systems and complexes currently used, information structures and data structures used to automate the process of conducting financial reporting audits. The results of the analysis must include:<br>1) Description of the processes of inspections of the subject of the Law, including:<br>• according to legislation and regulatory documents;<br>• taking into account the practice of using reporting systems and control in state institutions.<br>2) Description of the existing software complexes and systems for automating the submission and verification of financial statements, which are used by the Customer, including:<br>• description of existing software complexes and systems in relation to the described processes;<br>• availability and description of information interaction with related systems (including those of other departments);<br>• software name, software version.<br>3) A detailed assessment of the quantitative indicators that characterize the operational characteristics of the System, as well as its users.<br>4) Descriptions of identified "bottlenecks" that must be eliminated to achieve project goals.<br>*5)* Description of the approach to solving the problem of System implementation, taking into account the results of the analysis and evaluation. |
| **2.** | **Development of the technical specification** | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Form requirements for the System in the form of the document "Technical specification for the supply and implementation of ICS PFP". |
| **3.** | **Development of a technical project** | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Make improvements (reengineering, optimization) and agree with the Customer on the processes of submission and verification of financial statements within the System, taking into account the requirement for maximum coverage of the |

| | | |
|---|---|---|
| | | existing set of information available in the software packages used by the Customer. The results of the implemented improvement should be presented in the document "Description of all processes and the constructed model". |
| | 2 | Perform all other technical design works, the list of which is defined in the document "Technical specification for the supply and implementation of ICS PFP". The results of the development of the technical project should be presented in the document "Technical project" and its annexes, in accordance with the list defined in the document "Technical specification for the supply and implementation of ICS PFP". |
| **4.** | **ICS PFP software development** | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Develop and supply software products developed through computer programming. |
| **5.** | **Testing of System software in the scope of preliminary tests.** | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | To prepare for preliminary tests of the System, including:<br>1) preparation of the automation facility for testing;<br>2) training for the Customer's specialists (at least 2 people) on administration and work with the System to ensure independent support and development of the System;<br>3) training end users of the System (at least 5 people) on working with the SW System.<br>The results of the work carried out must be recorded in the Training Protocols. |
| | 2 | Preparation by the Contractor of the System configuration according to the model of future processes, as well as running a control example on a limited amount of data. The result of the performed works should be the program and methodology of preliminary tests of the System, the program of trial operation of the System, a control example in the amount sufficient for conducting the preliminary tests of the System. |
| | 3 | Carrying out preliminary tests of the System by the Contractor together with the Customer. The result of the performed work should be the Test Protocols and the System Test Act. |
| **6.** | **Introducing the System into trial operation** | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Carrying out the trial operation of the System by the Contractor together with the Customer in accordance with the trial operation program. The result of the work should be a System filled with up-to-date information and an Act of trial operation. |
| **7.** | **Provision of services related to System warranty service** | |

| | | |
|---|---|---|
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Performance by the Contactor of warranty maintenance of the System during the warranty period from the date of commissioning of the System. As a result of the work carried out by the Contractor, fully functioning, updated System boot modules, documentation for the updated System on machine media and a report on the provided System warranty service services must be transferred to the Customer. |
| **8.** | **Provision of services related to post-warranty maintenance of the System** (Under a separate contract) | |
| | # | *A detailed description of the activities to be carried out within the framework of the accompanying service* |
| | 1 | Performance of System post-warranty services by the Contractor within the agreed post-warranty period after providing System warranty services. As a result of the work carried out by the Contractor, fully functioning, updated System boot modules, documentation for the updated System on machine media and a report on the provided services for System post-warranty service must be transferred to the Customer. |

As part of the warranty and post-warranty service, the Contractor provides ICS PFP technical support services, including system updates taking into account legislative changes.

During the phases of development and implementation of the System, the Contractor must provide the Customer with the following reports:

- Report No. 1 – after the provision of Phase 1 "Survey of the automation object" services, but no later than 4 weeks from the date of commencement of work on the development and implementation of the System (signing of the Agreement);

  The document "Report on the results of the survey" is attached to Report No. 1.

- Report No. 2 – after the provision of Phase 2 "Development of the technical specification" services, but no later than 8 weeks from the date of the start of work on the development and implementation of the System (signing of the Agreement);

  The document "Technical specification for the supply and implementation of ICS PFP" with a detailed list of System functions is attached to Report No. 2.

- Report No. 3 – after the provision of Phase 3 "Development of a technical project" services, but no later than 12 weeks from the date of signing the Agreement;

  The "Technical project" and its annexes are attached to Report No. 3, in accordance with the list defined in the document "Technical specification for the supply and implementation of ICS PFP".

- Report No. 4 – after the provision of Phase 4 "ICS PFP software development" services, but no later than 24 weeks from the date of signing the Agreement;

  The following are attached to Report No. 4: i) software prototype; ii) test program and methodology.

- Report No. 5 – after the provision of Phase 5 "Testing of System software in the scope of preliminary tests" services, but no later than 32 weeks from the date of signing the Agreement;

  The following are attached to Report No. 5: i) program and operational documentation in accordance with the list specified in the document "Technical specification for the supply and implementation of ICS PFP"; ii) loading modules on machine carriers; iii) deployed System with filled information in the amount sufficient for conducting preliminary tests; iv) the program and method of preliminary tests of the System; v) trial operation program.

- Report No. 6 – after the provision of Phase 6 "Introducing the System into trial operation" services, but no later than 36 weeks from the date of signing the Agreement;

  The following are attached to Report No. 6: i) a functioning, modified System based on the results of trial operation with updated information; ii) System documentation revised based on the results of trial operation; iii) update bootable modules on machine carriers; iv) Protocol for introducing the system into trial operation; v) Protocol of trial operation of the system; vi) User manual; vii) Instruction of the administrator; viii) Protocol of acceptance tests of the system.

- Report No. 7 – after the provision of Phase 7 services "Provision of services related to System warranty service";

  Fully functioning, updated boot modules and documentation on machine carriers under the terms of System support in accordance with the terms of the Agreement are attached to Report No. 7.

- Report No. 8 – after the provision of Phase 8 services "Provision of services related to post-warranty maintenance of the System" (Under a separate contract);

  Fully functioning, updated boot modules and documentation on machine carriers under the terms of System support in accordance with the terms of the Agreement are attached to Report No. 8.

The System will be built in queue in accordance with the terms of adoption of the relevant legislation. First of all, the following will be implemented:

1) Business process «Submission and verification of financial reporting of political parties on property, income, expenses and obligations of a financial nature» (BP VFR-PP) (already implemented in POLITDATA);

2) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the elections of People’s Deputies of Ukraine» (BP VFR-EFFPD);

3) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the presidential elections of Ukraine» (BP VFR-EFFP).

Secondly, the following business processes will be implemented in accordance with the terms of adoption of the relevant legislation:

1) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in local elections» (BP VFR-EFFLE);

2) Business process «Submission and verification of financial reporting on the receipt and use of money from the All-Ukrainian Referendum Fund» (BP VFR-RFFUA);

3) Business process «Submission and verification of financial reporting on the receipt and use of money from the local referendum fund» (BP VFR-RFFL);

4) Business process «Submission and verification of financial reporting on the receipt and use of money from the initiative group fund» (BP VFR-RFFG).

The execution of each queue should include the entire list of works specified above for the entire System as a whole:

- development of technical project;
- development, configuration, and deployment of software (including the integration with information system of the NACP and data migration) and development of documentation;
- acceptance testing;
- providing instructions;
- trial operation.

### 4.2. Requirements for the characteristics of the implementation of functions and tasks determined by the general technical requirements for IS

The main parameters of the ICS PFP software subsystems are provided in Appendix 1 to these technical requirements.

### 4.3. Additional requirements for the IS as a whole and its parts, taking into account the specifics of the management object and the IS being created

Note: All references to a specific trademark or brand, patent, design or type of procurement item, source of origin or manufacturer should be read with the expression "or equivalent".

**System must be implemented according to the principles:**

- saving data in the database management system (DBMS);
- a single interface for WEB users.

**System must provide:**

- allocation of user access rights to System functionality;
- integrity of information;
- saving information in databases and restoring it when:
    - accidents and power supply interruptions;
    - accidents (malfunctions) and failure of servers;
    - appearance of computer viruses in the computer network;
    - in case of unauthorized intrusions;
- confidentiality and protection of information;

- backup of databases followed by their archiving and restoration of information from backup copies, regardless of which of the previous versions of the program the backup copy was created in.

**Requirements for the structure and functioning of the System**

System has the following usage levels:

- the level of unauthorized users - using the WEB interface (searching and viewing information);
- the level of authorized users - using the WEB interface (searching and viewing information);
- System administrator level.

**Requirements for data exchange formats**

System should allow data exchange in the following formats:

- text - TXT, XML, HTML, JSON, etc.
- spreadsheets – XLSX, XLS, CSV, etc.

**System performance and reliability requirements**

The working capacity of the created System must be ensured 24 hours a day.

Reliability of System functioning must be ensured through:

- installation of licensed software, whose reliability characteristics correspond to the highest modern international indicators and are guaranteed by agreements with representatives of supplier companies;
- using modern technologies of software engineering to develop application software;
- quality testing;
- reservation of main components and System elements;
- regulation of the organization of backup copying and archival preservation of information;
- the chosen method and regulation of technical support for the operation of the System;
- hardware and software compatibility.

System must ensure compliance with the following requirements for saving information in case of accidents:

- provision of local and remote detection and prevention of System emergency situations;
- recovery of information from backup copies of System data;
- implementation of standard procedures for eliminating System emergency situations;

- restoration of System performance.

**Software reliability requirements**

System reliability must be ensured by:

- reliability of system-wide software;
- reliability of System hardware;
- carrying out a set of debugging, searching and correcting errors.

**Hardware reliability requirements.**

The reliability of the equipment is subject to the following requirements:

- technical means with increased reliability should be used as hardware platforms;
- use of technical means that correspond to the tasks to be solved;
- the System hardware and software complex must be capable of recovery in the event of a failure.

**Organizational measures for reliability**

Reliability of hardware and software should be ensured through the following organizational measures:

- preliminary training of service personnel;
- timely execution of administration processes;
- compliance with the rules of operation and maintenance of software and hardware;
- timely performance of database backup procedures.

**Requirements for methods of assessment and control of reliability indicators at various stages of System creation in accordance with current regulatory and technical documents**

System as a whole is characterized by the following estimates of reliability indicators:

- the average working time between System server failures is at least 320 hours;
- the average recovery time after a failure is no more than 8 hours;
- availability – the percentage of time during which the System is ready for user service – 97.5%.

**Requirements for the number and qualifications of the System staff and its mode of operation**

All System users must have the following skills and knowledge before starting work:

- operation of a personal computer and peripheral equipment;
- work with office software;
- understanding of the general principles of using information, its search and storage;
- working with a qualified electronic signature;

- understanding of the general principles of information protection.

System administrators must have the following qualifications:

- configuration, installation of server and client parts;
- configuration and operation of applications;
- installation, configuration, backup and recovery of data, operation of DBMS;
- installation, configuration and operation of System software.

**Destination indicators**

System should provide the ability to:

- simultaneous work of at least 10,000 users who are allowed to add, edit, and receive data from arbitrary parts of the System;
- the work of up to 5 (five) persons authorized by the Customer who perform software and hardware maintenance (Administrators);
- provision of round-the-clock access to the System;
- the number of requests for reading - at least 50,000 per hour;
- the number of requests for recording - at least 5,000 per hour;
- volume of databases - at least 1 TB.

For the System, reliable (stable) functioning must be ensured by the implementation of a set of organizational and technical measures:

- organization of uninterrupted power supply of technical equipment;
- use of licensed software;
- meeting the requirements of SSU 3396.0-96 Information Protection. Technical protection of information. Substantive provisions;
- use of technical equipment, system software that corresponds to the class of tasks to be solved;
- timely performance of System administration processes;
- implementation of hardware rules of operation and maintenance of hardware and software.

**Requirements for ergonomics**

System should provide a convenient, intuitive user interface that meets the following requirements:

- localization in Ukrainian;
- uniformity of display forms;
- uniformity of data processing mechanisms (for fields of the same type, for operations of the same type, etc.);

- minimal use of graphic images on web pages to speed up their loading;
- for operations that require waiting, a notification should be issued about the progress of the process;
- the ability to control the interface by moving through the forms using both the "mouse" and the keyboard.

In the dialogue with the System user:

- use of "hot" keys to perform a set of frequent operations;
- a concise message about errors with instructions on how to correct them.

In terms of data input and output:

- formation and submission for review of the protocol for monitoring the execution of operations.

**Patent purity requirements**

The patented purity of the System and its parts is ensured by:

- use of licensed software tools for System development;
- use of licensed software and other information objects that are used in the creation or included in the System and are its components.

All necessary licenses of application SW (upgradeable) and DBMS system components must be perpetual and must be transferred to the Customer as part of the System.

All third-party software components licensed separately and planned for use in the System, the cost of their licenses and technical support must be submitted as part of the offer. The contractor must transfer perpetual licenses for all third-party components of the application SW (upgradable) and DBMS and provide information about them.

The “IIT User CSK-1” libraries are already provided by NACP and embedded in POLITDATA, so the cost of their licenses and technical support should not be included in the proposal.

Backwards compatibility of versions of the licensed software that will be used as part of the System must be supported, that is: functionality created using the tools and tools built into the System must be compatible with new versions of such licensed System software.

The proposed SW and System components, with which or on which the deployed solution should not be subject to restrictive measures (sanctions), are introduced in accordance with the Decrees of the President of Ukraine and other requirements of current legislation.

**Prospects for the development and modernization of the System**

The development of the System should take place in accordance with the purpose and purpose of creation.

The System should be open from the point of view of the possibility of modernization without stopping its intended use.

**Requirements for standardization and unification**

Requirements for standardization and unification of System software are as follows:

- when developing the System, standard industrial technologies of the programming language and DBMS, which are documented, must be used;
- System source code must be uniformly formatted and documented (acceptable code documentation languages - English, Ukrainian);
- the internal software implementation of the System should be based on the use of standard programming templates;
- the System code should not use undocumented capabilities of programming languages, as well as those capabilities that are considered obsolete (legacy) at the time of development and for which the termination of support in future versions is declared.

Requirements for standardization and unification of System user interfaces are as follows:

- all interfaces must be arranged in the same way (for example, standard panels must always be in the same place);
- all interfaces must use the same design (for example, an icon or inscription must indicate the same thing on all System interfaces);
- all interfaces must use uniform behavior (for example, the formation of control protocols in case of incorrect user actions on all System forms).

Requirements for standardization and unification of System hardware:

- typical hardware components of server and switching equipment should be standard and interchangeable.

**Requirements for adaptation of content for persons with visual and hearing disabilities**

In order to ensure proper access of persons with visual and hearing disabilities to the information posted on the official websites of executive authorities, the Government adopted Resolution No. 730 of the Cabinet of Ministers of Ukraine dated September 26, 2013 "On Amendments to the Resolution of the Cabinet of Ministers of Ukraine dated January 4, 2002 No. 3 of 2002 and No. 1302 of August 29, 2002.

The public part of the System must be adapted for users with visual and hearing disabilities:

- the information posted on the portal should be accessible to users with visual and hearing disabilities, as well as provide for the possibility of using screen access computer programs that provide data output in sound or relief-dot form;
- audio and video materials uploaded by the content manager must be accompanied by text equivalent to the information contained in the audio and video recording. Information placed on a moving tape, graphic and multimedia materials must be duplicated using plain text;
- the font size of the text, with the exception of titles, must change within 200 percent without the use of assistive technologies and loss of information content or functionality of the service portal;
- the visual presentation of the text must have a contrast ratio of at least 5:1;

- navigation using a computer keyboard should be implemented;
- it is not allowed to apply time limits on the performance of navigation functions and/or interactive interaction of the user with the service portal, as well as objects that flash on the screen more than three times per second.

**Requirements for personnel training**

The supplier must provide training (instruction) for System administrators and users.

Number of personnel for training:

- administration and operation support: at least 2 (two) professional IT employees of NACP;
- System users: at least 10 (ten) NACP employees.

The cost of training must be taken into account in the Supplier's price offer.

**Documentation requirements**

The Contractor must provide the Customer with technical documentation for all modules of the software and hardware complex, which must include information on the technical characteristics of the product (architecture, applied technologies, work algorithm), a description of the functions of the modules, instructions for System users, etc., as well as information necessary for independent maintenance of the product by the customer. The source codes of the programs are provided by the Executor with comments that allow determining the functional purpose of individual blocks of the program code.

All documentation is drawn up in Ukrainian and approved in printed form with copies provided in electronic form (Microsoft Word format).

Technical documentation must be developed in accordance with current state standards and using terminology in accordance with industry and corporate standards.

The list of documents for each subsystem that must be developed during the execution of works and provided after the completion of the corresponding stage:

Technical specification:

- general requirements;
- purpose and goals of system creation;
- characteristics of automation objects;
- system requirements (functional and non-functional);
- composition and content of works on the creation of the system;
- description of the architecture of the solution and its constituent parts;
- system control and acceptance procedure (including a description of work stages);
- requirements for the composition and content of works on the preparation of the automation facility before the system is put into operation;
- documentation requirements.

Technical project:

- composition and purpose of subsystems;
- description of the architecture of the solution;
- description of process groups (functional subsystems);
- description of the functionality that is being developed;
- description of subsystems' work algorithms;
- description of interaction mechanisms between subsystems and external systems;
- requirements for third-party system software with a list of recommended software;
- description of implementation of reliability, fault tolerance and scalability;
- mechanisms for backing up and restoring subsystem configuration and data;
- data archiving and storage procedure;
- description of the security of the solution;
- composition of works;
- implementation restrictions.

API specification:

- description of mechanisms of interaction between subsystems and external systems/equipment - algorithms, data formats, API.

Specification of automated processes (for each process):

- description of the process;
- process inputs (flows coming from the outside and subject to transformation);
- process outputs (transformation results);
- roles participating in the process;
- resources possessed by the process;
- algorithm (scheme);
- performance indicators of the process.

Specified hardware and system software requirements.

Installation Guide:

- subsystem installation (installation) instructions;
- subsystem recovery instructions;
- a description of the means and methods of improving the productivity of the subsystem after its installation;
- a description of means and methods of diagnosing non-standard situations that arise during installation, methods of solving them.

Program-methodology of acceptance tests:

- volume of tests;
- test conditions;
- a list of testing and inspection stages;
- sequence of tests;
- method of carrying out loading tests;
- the method of carrying out subsystem fault tolerance tests;
- test results.

Subsystem Administration Guide:

- description of the architecture of the solution, composition and purpose of the subsystem;
- list of subsystem hardware components;
- list of subsystem software;
- schemes of operation of the subsystem;
- a description of the functions and mechanisms of setting the subsystem;
- location and structure of configuration files;
- the location and structure of files that register the operation of the subsystem (log files);
- description of possibilities for creating/changing user interfaces, displayed data formats, filters;
- means and methods of diagnosing out-of-state situations that arise, and methods of solving them;
- list of regular scheduled works;
- a scheme for including hardware in the corporate network;
- procedure, mechanisms for backup and recovery of subsystem configuration and data (with recommended backup schedule for subsystem components);
- data archiving and storage procedure (with a recommended archiving schedule);
- instructions for granting and delimiting access rights to the subsystem;
- a list of means and methods of subsystem monitoring;
- subsystem hardware requirements (for user workstations: minimum, optimal; for the server part: minimum, optimal);
- system software requirements (operating systems and their versions, separately for the server, separately for users' computers, browsers with which the subsystem works).

User manual according to subsystem roles:

- a general description of the purpose and functions of the subsystem;
- description of standard (implemented) user interfaces with given examples of information displayed on the display (in the form of screen copies);
- instructions for each functional role of users on operations;
- a list of subsystem messages in case of failures and necessary corresponding user actions (in tabular form).

Trial operation program:

- place and duration of trial operation;
- scope of trial operation;
- conditions and procedure for trial operation;
- reporting and the procedure for eliminating deficiencies.

List of documents to be developed after the final stage of System implementation:

Program-methodology of complex acceptance tests of the system:

- volume of tests;
- test conditions;
- a list of testing and inspection stages;
- sequence of tests;
- method of carrying out loading tests;
- method of conducting system fault tolerance tests;
- test results.

Protocol of completed works:

- conditions and procedure for performance of works (provision of services);
- volume of performed works (providing services);
- the result of work performance (service provision).

The given list is not exhaustive, at the stage of technical design, the Contrator must compile a detailed list of documentation and approve it with the Customer.

After approval by the Customer, the list of documentation is mandatory for compliance. During the works, the Contractor must develop and provide the Payer with all the documents listed in the documentation list.

**Warranty requirements**

The warranty period of System operation is at least 12 months (or another agreed term) from the date of signing the act of acceptance and transfer of the provided services.

During the warranty period, the Contractor’s support service will provide software and technical support and consultations on the functioning of the System. Warranty service means:

- performance of all necessary actions (including elimination of malfunctions in the System, provision of operational consultations, changes to the System at the Customer's request, etc.) that will ensure the system's operability and allow the Customer to use the System in accordance with its functional purpose;
- correction of defects in the System or its non-compliance with the agreed technical conditions.

**Functional requirements**

To ensure the integrity of System data and reliable operation of the SW, access to any sections and modes of addition or editing should be granted only to authorized users with mandatory logging of all performed actions. Links that activate add and edit modes should only be visible to authorized users.

Searching for information in the System databases can only be performed by authorized users. Fields that provide for the possibility of entering data from a certain range should be presented in the form of appropriate control elements of web forms.

SW System's response to a search query is a set of records from the System databases, which in the corresponding fields contain the values included in the query fields. According to the requirements for the interface, the results of the query must be presented in the form of a formatted web page with the possibility of page-by-page output. Also, the results page should contain information about the user's request and a link to the main page. There are no additional requirements for the arrangement of entries on the results pages.

**Requirements for linguistic support**

The System language must be Ukrainian. This language should be used:

- in the System documentation;
- in user interfaces;
- in user error messages, except for the part of messages necessary for diagnosing the operation of the operating system and DBMS.

**Software requirements**

System software should provide full functionality for users.

System WEB components must be accessible from automated user workstations without the need to install System client software components (this requirement may not apply to cryptographic libraries for qualified electronic signatures).

System software must:

- be based on proven industrial technologies of input, storage, processing, data analysis and access to them;
- have a flexible and effective configuration change system, which allows you to adjust the parameters of functional modules without adjusting the source codes of the programs;

- use generally accepted standards for building interaction between functional components;
- use an industrial database management system (for example, PostgreSQL, already used by POLITDATA), which functions in the environment of Unix and Windows operating systems and includes tools for quickly creating and deploying web applications that allow developing fast and reliable professional applications using only a web browser and minimal programming experience;
- have in its composition developed means of administration that ensure centralized management of the System;
- fully function with the use of modern versions of Internet browsers by users: Mozilla FireFox, Google Chrome, Internet Explorer, Safari, Opera, Microsoft Edge.

The software should have the ability to create new and edit existing logic and arithmetic control (checking) rules.

The software should allow setting (adding and editing) logical and arithmetic control rules, adding and editing groups of checking rules.

Each rule must support versioning, taking into account the rule code, its parameters, the relationship to the check object.

The control unit for rules and groups of rules should provide the ability to view the list of logical and arithmetic control rules, rule status, version, group of rules and allow creating new rules, editing existing rules, changing the status and group of rules.

Access to the control unit of rules and groups of rules must be granted to specific users or users with certain roles according to their authority in System.

The software must have a document template editor, that is, be able to edit document templates (excerpts for display in the system interface), including allowing the creation of groups and blocks of templates with dynamic loading of these blocks into any template, without restrictions.

The document template editor should be able to preview generated document templates (in HTML and/or PDF format) based on loading data from various sources and formats.

SW System should ensure compatibility and integration, support of functioning in heterogeneous hardware and software environments.

Linguistic support of the System should include advanced programming languages for the software and user interface.

Programming languages must be selected by the supplier in accordance with the system software solutions at the System Technical Design stage.

The following criteria must be taken into account when formulating requirements for SW:

- The operating systems on which System is built must have up-to-date versions. All subsystems must work on the same (version, manufacturer) operating systems.
- All operating systems must have support from the manufacturer for at least 2 years from the date of completion of System implementation. Operating systems must be

designed to work on servers in a cluster architecture. Operating systems must be reliable and secure, as well as designed for high load.

- The DBMS must meet the requirements for high-performance corporate DBMSs, have the ability to scale, optimize and parallelize query processing on several processors, backup and automatic recovery after a failure, have a multi-level protection system and a system for diagnosing the integrity of the database and individual tables. If errors are detected during the verification process, the diagnostic system must attempt to correct the error found. In the case of detection of errors, the diagnostic system must record information about errors in the electronic system logs of the corresponding database server.
- Anti-virus software must:
    - ensure the protection of the System and its components against intentional criminal destruction, destruction, correction, editing and theft of information by virus software;
    - be recommended for use in state institutions of Ukraine.
- When choosing software, it is not allowed to use third-party software solutions without technical support.

**System diagnostic requirements**

All subsystems must have the functionality of journaling (logging) events to diagnose the operation of subsystems and identify problems.

Event logging should be done in the DBMS. It should be possible to output logs to a file on the application server (optional). In the case of using log files, the ability to integrate with the monitoring system by sending Syslog messages is required.

Logs should be read-only available to a limited number of users. Special interfaces should be provided that will allow analysis of logs and search for necessary events.

Logs are divided into two classes:

- system events – events that affect the operation of subsystems and their modules, which occur at the level of system and application software, hardware, etc. Such events are considered by the administrator, and they may include: when the module of the subsystem started, whether correctly used configurations, whether the necessary services are available, as well as all errors and warnings related to this;
- application events – all actions performed by users of subsystems or subsystems themselves automatically. Any user actions must be recorded in the event log. For example, if the user edits (adds, deletes) information in the report card, then the following should be logged in the "report card edit" event: user ID, date, time, workstation ID, report card edit identifier (the object on which the operation), the events, the result of the operation are described.

Event logs should be able to restore all user actions for a selected time period.

Event logs must be available for analysis during the year (or any other period if required by law). Logging of all events should not affect the performance of System and its subsystems.

Subsystems must support the following logging levels:

- Trace — display of all system events. It should be possible to turn this level on and off;
- Warning & Error — events that require an administrator's response, they show that something is going wrong in the subsystem. For example, unexpected call parameters, incorrect request format. That is, everything that may indicate abnormal use.

Note: The list is not exhaustive and defines the minimum requirements for logging levels.

The information in the logs should be enough for both system administrators and SW developers to understand and analyze the situation. Messages should be informative enough to enable problem localization.

In the event of the same accidents or errors, all subsystems must generate messages with the same code.

Application events should always be logged. Diagnostic information in the section of each subsystem, business process, operations should have end-to-end numbering.

A configurable mechanism for informing administrators about self-diagnosis events via e-mail should be created.

Notifications should be divided, for example, into:

- warning about the unavailability of the service (or exceeding the specified response time);
- warning about reaching the threshold value of the waiting queue for processing;
- a warning about reaching the estimated maximum bandwidth of the channel;
- warnings about critical and blocking errors.

It should be possible to configure a variety of filters that would form samples of events in terms of functional processes or other end-to-end (those performed in different subsystems) operations, for example, it is necessary to be able to filter all events in all subsystems that were performed within a specific functional process during operation with a report.

A configurable log archiving mechanism should be created.

During the implementation of the System, the criteria for regular and non-regular functioning of the subsystems must be determined.

The description of errors, measures for their diagnosis and elimination, mechanism for setting monitoring of subsystems, notification mechanism, criteria for normal and abnormal functioning of subsystems must be described and listed in the operational documentation.

Subsystems in the implementation process should be configured in such a way that events are generated to control the following parameters:

- availability of user services;
- availability of APIs used for electronic information interaction with other systems;
- DBMS availability;

- monitoring of critical processes.

This list is minimal and should be supplemented and detailed during the design process.

Subsystems must provide the ability to remove performance parameters. For this, it is necessary to provide for the use of both the system API and requests to the database.

It is necessary to be able to monitor the following parameters:

- system response time;
- number of requests from users per unit of time;
- the average value of the execution of processes per unit of time (for example, the average execution time of downloading data from a file - records per second).

This list is minimal and should be supplemented and detailed during the design process.

During the implementation, the supplier is obliged to provide a description of the interfaces for monitoring the functionality and performance of all subsystems, a detailed description of the steps and ranges of permissible values of the monitoring parameters.

If necessary, a detailed description of mechanisms (including SQL queries) for monitoring subsystem parameters, including subsystem health and performance, should be provided.

**System operating mode requirements**

System application mode should be 24/7.

System operation should include the following operating modes:

- basic mode – is the mode of regular operation of all subsystems of the system according to their purpose;
- maintenance mode – there is a mode of regular maintenance and restoration of technical means of subsystems.

**Requirements for the construction of System interfaces (API)**

The requirements for API apply both to the exchange interface with external systems and to the interfaces that are built between System subsystems.

Replacing one of the subsystems with another should not require the modification of the API of the subsystems, except for the subsystem that will be implemented.

Subsystems must support API versioning. There should not be a situation where the new version of the subsystem does not support the previously used API, and therefore adaptation of the API of other subsystems is necessary. If such a need arises, all costs for adapting the API are borne by the Contractor.

The API of all subsystems must be documented. Such documentation should include descriptions of methods, parameters, returned values, and call examples.

The API for each of the Subsystems must be complete, i.e. sufficient to perform all proper functions of interaction both in the system and with external systems.

For the possibility of automated API testing, the Contractor will have to develop and provide special scripts that will test the API by calling API methods with control parameters and analyzing the received values for correctness.

The supplier must develop and provide special scripts for load testing of API methods that can potentially affect the performance of subsystems.

The API must:

- support applied authorization functions. Authorization must be carried out through the subsystem of authentication and authorization by the method of obtaining a key (Token). One of the authorization protocols must be supported, for example, oAuth;
- support work in both synchronous and asynchronous modes;
- provide the possibility of multi-threaded work;
- repeat requests if they were not delivered due to the unavailability of the interface, the number of repetitions must be configured;
- the API should be implemented using SOAP or RESTful web services.

Integration at the database level is not planned.

During the exchange, the integrity and completeness of the received and sent information should be monitored. Information exchange between adjacent information systems should be ensured using modern means, protocols and data transfer formats.

**System reliability requirements**

All key elements of the System, in order to ensure high reliability and stability of the system as a whole, must use only industrial-level serial system software.

System should not have a single point of failure.

To reduce the potential threat of critical failures leading to the inoperability of the main server, it is recommended to install System on two server platforms: the main and the backup. At the same time, the backup part of the system should be able to take over 100% of the entire load if necessary. The time of transition to the backup server platform should not exceed 2 hours.

System reliability must be ensured at several levels:

- hardware level - due to the availability of a backup server platform;
- the level of application servers - due to special hardware or software tools that will provide load balancing, analysis of service availability and switching of requests to an available service in case of service unavailability;
- database level - due to the use of highly reliable architecture, which will allow to distribute the load on the loaded database between DB servers and ensure productivity increase due to the addition of additional computing power to the cluster.

**Reliability criteria**

System as a whole should work and be available around the clock.

Maintenance of the System during working hours should not last more than 12 hours during the period of submission of Reports by the participants of the election process and more than a day at other times.

Emergency and recovery works are carried out immediately.

**Crash recovery**

Restoration of availability in the event of a failure for the operation of all subsystems should not exceed 4 hours. In the event of a failure, the information in the database should remain correct and complete, there should be no loss of data stored in the database.

In the event of a failure (for example, failure of a hardware server), which will require the replacement of a System element, such replacement must take place without interrupting the System's operation, and the System's performance must remain within normal limits (not exceed the limit values).

Failure recovery mechanisms must be regulated and described by the System developer.

**Backup and restore**

System should provide the ability to backup and restore data and configurations. Performing a backup should not cause subsystems to stop working.

The duration of the procedure for backing up software and configuration of subsystems to internal storage resources should not exceed 8 hours.

The duration of the full backup recovery procedure should not exceed 10 hours.

A full data backup should be performed once a week.

Incremental backups should be performed once a day.

Backup copies should be stored in two geographically separated data centers.

All subsystems must support one of the industrial virtualization systems.

**Development quality requirements**

The creation of the System can be carried out using licensed application software available to the Contractor with the functionality required for the System in accordance with the Customer's technical requirements.

System software must be created in accordance with the requirements of SSU 3918-1999 (ISO/IEC 12207:1995) "Software Life Cycle Processes".

**Regarding the organizational and functional structure of the created System**

When creating a System, special attention should be paid to the organization of exchange gateways both between IS, which contain confidential information and are outside the NACP, and between System subsystems, which are in different circuits of the information class. Exchange gateways should be organized in accordance with the recommendation on the creation of a comprehensive information protection system.

When designing exchange gateways, it is desirable to take into account the possibility of exchanging information both incrementally (according to a template, for a period starting from a certain date), and the entire data set, which is effective, for example, when data reconciliation between IS is needed.

To ensure e-interaction of e-resources, the use of the Internet, a secure channel with the NBU, and the channels of the National System of Confidential Communication with mandatory compliance with the requirements of the Resolution of the CMU dated May 14,

2015 No. 303 "Some issues of the organization of interdepartmental information exchange in the National confidential communication system".

**Intellectual property rights to System**

Property, including exclusive, intellectual property rights to the System (including all components listed in the Technical Requirements), including those stipulated by the Civil Code of Ukraine, the Law of Ukraine "On Copyright and Related Rights", as well as other legislation of Ukraine and international legal acts, from the moment of development (creation, modernization) must belong to NACP.

## 5. Estimated schedule

| No Stages | Name of Stage | Reporting (see section 4.1.) | Deadline, months |
|---|---|---|---|
| | Stage 1 | | |
| 1. | Automation of business processes:<br>1) Business process «Submission and verification of financial reporting of political parties on property, income, expenses and obligations of a financial nature» (BP VFR-PP) (already implemented in POLITDATA);<br>2) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the elections of People's Deputies of Ukraine» (BP VFR-EFFPD);<br>3) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the presidential elections of Ukraine» (BP VFR-EFFP); | | 6.5 months from the date of signing the Agreement |
| 1.1. | Designing (Survey of the automation object, Development of the technical specification, Development of a technical project) | Report No. 1, Report No. 2, Report No. 3 | 2 months from the date of signing the Agreement |
| 1.2. | SW development, SW customization, SW implementation (including electronic information interaction with the Customer's information systems and data migration), documentation development | Report No. 4 | 5.5 months from the date of signing the Agreement |
| 1.3. | Acceptance tests | Report No. 5 | 6 months from the date of signing the Agreement |
| 1.4. | Training | Report No. 5 | 6 months from the date of signing the Agreement |
| 1.5. | Trial operation | Report No. 6 | 6.5 months from the date of signing the Agreement |
| 1.6. | Warranty support (including updating the system taking into account changes in legislation) | Report No. 7 | 12 months from the moment of signing the Acceptance Act |
| | Stage 2 | | |
| 2. | Note: the sequence of implementation of clauses 2.1-2.4 is agreed no later than the start of implementation of clause 1.6 by the Customer and the Supplier in accordance with the terms of adoption of the relevant legislation | | 2.5 months for each business process in accordance with the agreed schedule, but no later than the |

| | | | |
|---|---|---|---|
| | | | deadline for the completion of clause 1.6. |
| 2.1. | Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in local elections» (BP VFR-EFFLE); | Report No. 1-6 (within this business process) | 2.5 months for each business process in accordance with the agreed schedule |
| 2.2. | Business process «Submission and verification of financial reporting on the receipt and use of money from the All-Ukrainian Referendum Fund» (BP VFR-RFFUA); | Report No. 1-6 (within this business process) | 2.5 months for each business process in accordance with the agreed schedule |
| 2.3. | Business process «Submission and verification of financial reporting on the receipt and use of money from the local referendum fund» (BP VFR-RFFL); | Report No. 1-6 (within this business process) | 2.5 months for each business process in accordance with the agreed schedule |
| 2.4. | Business process «Submission and verification of financial reporting on the receipt and use of money from the initiative group fund» (BP VFR-RFFG). | Report No. 1-6 (within this business process) | 2.5 months for each business process in accordance with the agreed schedule |

# Appendix 1. Descriptions of typical business processes of the Customer

## 1. MAIN PARAMETERS OF ICS PFP SOFTWARE SUBSYSTEMS

### 1.1. General structure of ICS PFP

The main parameters of the ICS PFP software subsystems are determined by the logic and features of the business processes to be automated. In accordance with the tasks assigned to NACP according to the legislation, the following main business processes should be highlighted:

1) Business process «Submission and verification of financial reporting of political parties on property, income, expenses and obligations of a financial nature» (BP VFR-PP);
2) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the presidential elections of Ukraine» (BP VFR-EFFP);
3) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in the elections of People's Deputies of Ukraine» (BP VFR-EFFPD);
4) Business process «Submission and verification of financial reporting on the receipt and use of money from election funds in local elections» (BP VFR-EFFLE);
5) Business process «Submission and verification of financial reporting on the receipt and use of money from the All-Ukrainian Referendum Fund» (BP VFR-RFFUA);
6) Business process «Submission and verification of financial reporting on the receipt and use of money from the local referendum fund» (BP VFR-RFFL);
7) Business process «Submission and verification of financial reporting on the receipt and use of money from the initiative group fund» (BP VFR-RFFG).

It is worth noting that BP VFR-EFFP, BP VFR-EFFPD, BP VFR-EFFLE, BP VFR-RFFUA, BP VFR-RFFL and BP VFR-RFFG are practically identical in their general logic. It is this fact that determines the presence in each of the corresponding SS of the same set of SMs covering the same set of corresponding BP steps.

In particular, each of the six SS (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) contain the following SMs in their structure:

- SM "Workstation of NACP registrar";
- SM "Workstation of the manager of EFA/RFA";
- SM "Workstation of NACP analytics".

Common features of the above SMs are specified in Section 1.4.

The specific features of the above SMs, within the implementation of the above BPs (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) are given below in the description of each individual SS (Chapter 1.5 – 1.10).

As for VFR-PP, it contains a unique (different from other SS in ICS PFP) set of such SMs:

- SM "Workstation of the head of analysts";
- SM "Workstation of NACP analytics";
- SM "Party Leader's Workstation";
- SM "Workstation of the head of the regional office";
- SM "Workstation of the authorized person for filling out the report".

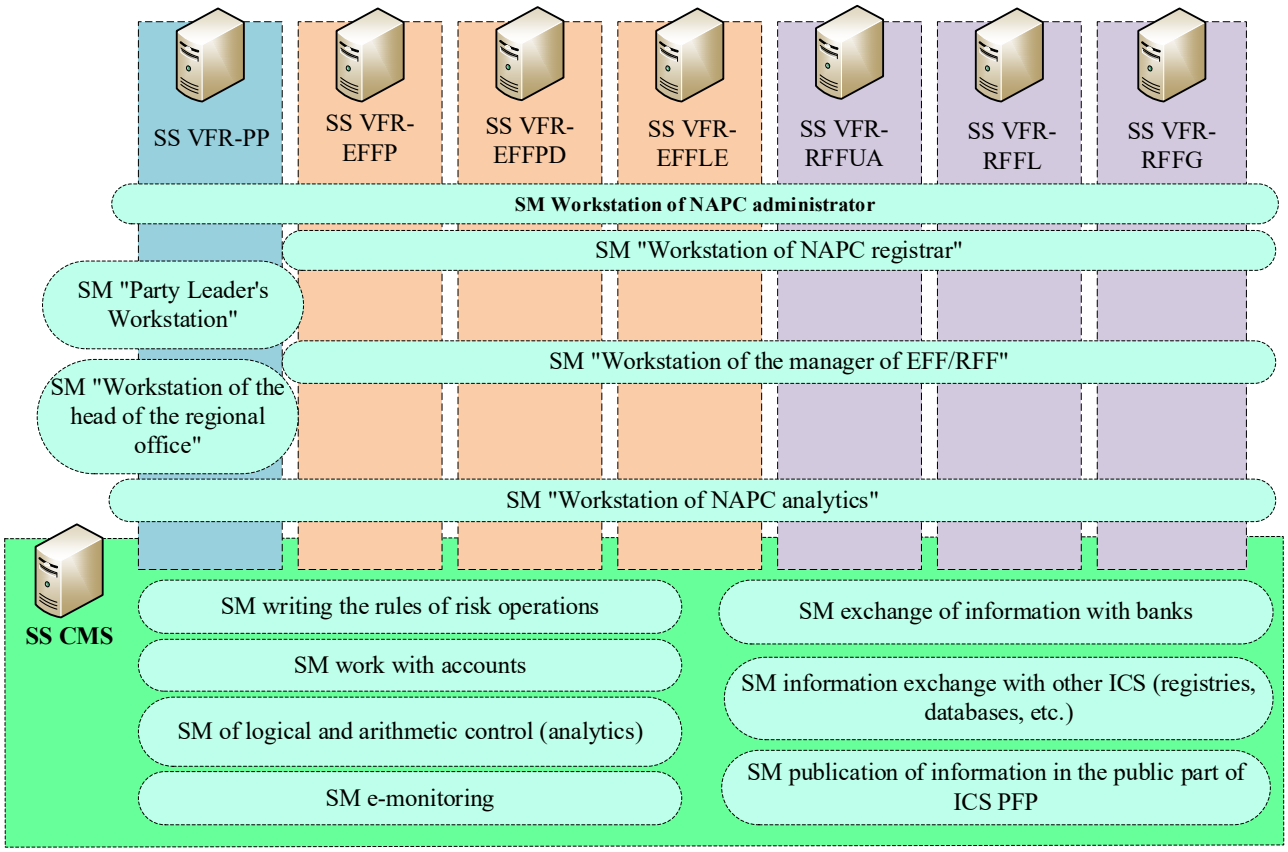
Of particular importance in the ICS PFP structure is the SS CSM, which interacts with all the above SS and includes a set of such SMs (a detailed description is provided in Chapter

2):

- SM writing the rules of risk operations;
- SM exchange of information with banks;
- SM work with accounts;
- SM of logical and arithmetic control (analytics);
- SM information exchange with other ICS (registries, databases, etc.);
- SM publication of information in the public part of ICS PFP;
- SM e-monitoring.

The figure below shows a graphical representation of the overall SS structure, with corresponding SMs displayed.

**The general structure of the software subsystems of the ICS PFP**




Peculiarities of SS CSM interaction with other SS (VFR-PP, VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) at the SM level are given below in the description of the main parameters of each individual SS.

A separate entity is the SM Security Administrator ICS PFP (not shown in the figure, a detailed description is provided in Section 3.1.), the functionality of which extends to the entire ICS PFP as a whole and does not depend on the logic and features of the business processes to be automated.

## 1.2. Peculiarities of data structuring in the chronology of the main BPs

As already mentioned above, each of the six SS (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) contain the same set of SMs in their structure:

- SM "Workstation of NACP registrar";
- SM "Workstation of the manager of EFA/RFA";

- SM "Workstation of NACP analytics".

The main (key) feature of the respective BPs (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) is their clear organization (exhaustiveness of stages) and determination of the same groups of time frames for the implementation of its key stages for all without excluding participants. In general, all specified BPs (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) start and end simultaneously for all participants and are implemented in one cycle.

Let's consider the above statement and the corresponding cycle model on the example of BP VFR-EFFPD. Thus, in accordance with Article 136 of the ECoU, regular elections to the Verkhovna Rada of Ukraine take place on the last Sunday of October of the fifth year of the Verkhovna Rada of Ukraine's mandate. At the same time, the electoral process of regular elections of deputies begins sixty days before the voting day. The Central Election Commission announces the beginning of the election process no later than sixty-one days before the voting day.

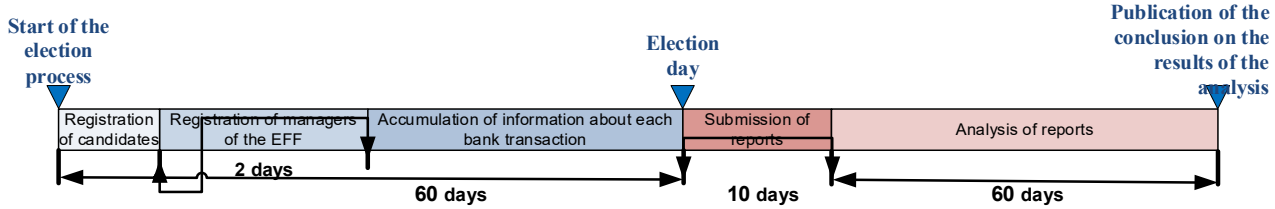
In turn, according to Article 151 of the ECoU draft, the manager of the party's EFF or the candidate's EFF is obliged to undergo authentication in the ICS PFP within two days from the date of appointment.

In accordance with Article 151 of the ECoU draft, the EFF manager, not later than on the tenth day after the election day, forms and submits in the VFR-EFF module a report on the receipt and use of the EFF.

In turn, the analysis of reports on receipts and use of EFF is carried out by the NACP within sixty days from the date of completion of the deadline for submission of such reports by the relevant managers of the EFF. Accordingly, NACP not later than on the sixtieth day after submission of the report on receipts and use of the EFF shall publish in the open part of the ICS PFP the conclusion based on the results of the analysis of such report.

The figure below shows a general diagram of the time frame for the implementation of the key stages of BP VFR-EFFPD.

**General scheme of time frames for implementation of key stages of BP VFR-EFFPD**




It is also worth noting that during the extraordinary (interim) elections of People's Deputies, the general time frames for the implementation of the key stages of BP VFR-EFFPD for all participants without exception are preserved.

The exact same logic of organization (exhaustiveness of stages) is preserved for other BPs (VFR-EFFP, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG). However, the corresponding norms of legislative acts provide for slightly different groups of time frames for the implementation of their key stages. In general, as with BP VFR-EFFPD, all phases of BP (VFR-EFFP, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) start and end simultaneously for all participants and are implemented in one cycle.

Taking into account the peculiarity of the organization (exhaustiveness of stages) for BP (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG), as well as the same timeframe for the implementation of key stages for all participants without exception, data structuring should be considered based on the conditional division of each BP (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) into two key stages:

- Stage I - from the moment of opening a bank account until the EFA/RFA manager makes a decision to submit a report on receipts and use of EFA/RFA;
- Stage II - from the moment the manager of the EFA/RFA makes a decision to submit a report on the receipt and use of the EFA/RFA until the NACP analyst performs its analysis.

At the 1st stage of BP - from the moment the bank account is opened until the EFA/RFA manager makes a decision to submit a report on the receipt and use of EFA/RFA, the system will include only data on each completed bank transaction on the receipt or use of EFA/RFA.

The specified information on each completed banking operation for receipt or use of EFA/RFA will be provided by banks and entered into SS (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) through the Information Exchange Module with SS CSM banks.

Information about each completed bank transaction for the receipt or use of EFA/RFA will be provided in chronological order as the relevant bank transactions are carried out (according to the principle of forming a bank statement).

Upon receipt of information from the banks about each completed bank transaction, within 3 working days from the date of receipt, the manager of the EFA/RFA:

- is obliged to analyze the information received from the bank;
- has the right to make changes or supplement information on those details, the information on which does not correspond to reality or is completely absent;
- confirm the authenticity of each bank transaction (after its analysis and, if necessary, adjustment).

If the EFA/RFA manager makes a decision to confirm bank information, this information about transactions on the movement of funds is automatically published in the public part of ICS PFP (via the Information Disclosure Module in the public part of ICS PFP).

The manager of the EFA/RFA (only within the limits of the requisites defined by the law) may decide to make changes (additions) to the bank information in the event of:

- erroneous transfer of funds, which later (by another bank operation) were returned to the EFA/RFA;
- detection of errors or inaccuracies in the details of the payment document "payment details";
- detection of other facts, according to which the information about the conducted banking operation does not correspond to reality or is completely absent.

If the bank information is not confirmed by the EFA/RFA manager, this information about the transactions on the flow of funds is automatically published in the public part of ICS PFP three working days after its receipt from the bank (via SM publication of information in the public part of ICS PFP).

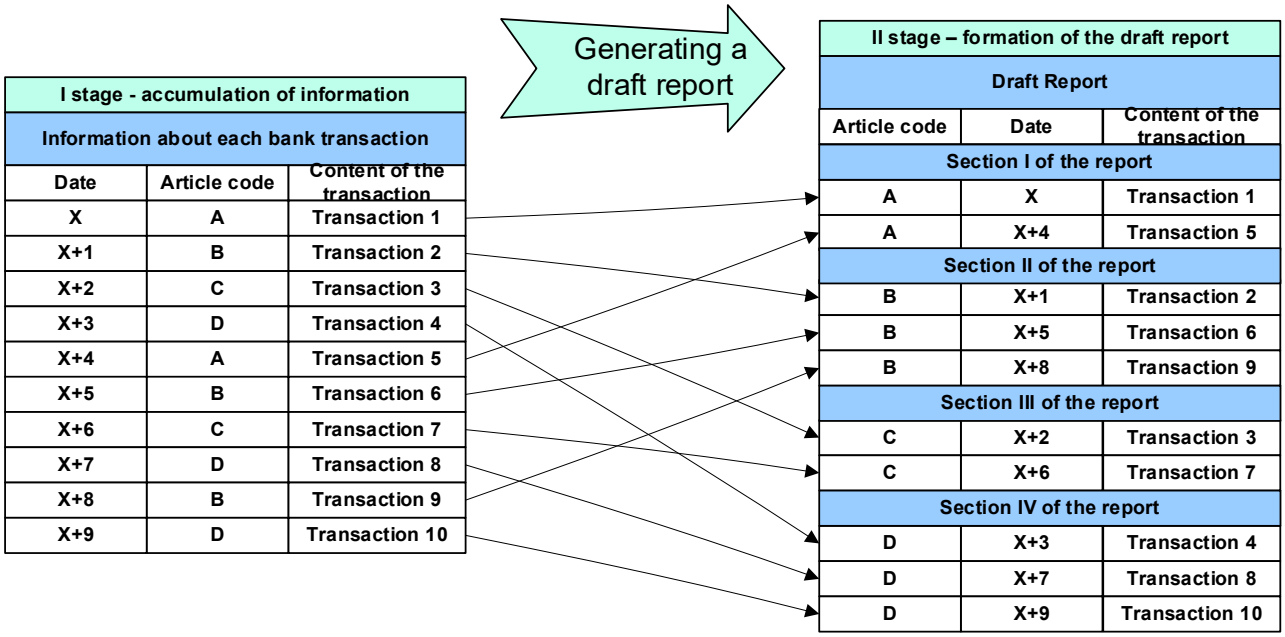
At the II stage of BP - from the moment the manager of EFA/RFA makes a decision to submit a report on the receipt and use of EFA/RFA until the analysis is carried out by the NACP analyst, all information (data) about each completed bank transaction on the receipt or use of EFA/RFA is grouped under a common identifier "article code".

At the same time, according to the given set of "article codes" for the corresponding section of the report on receipts and use of EFA/RFA, the draft of the corresponding report is formed automatically at the moment when the manager of EFA/RFA makes the corresponding decision.

The general model of transformation of the data accumulated at the 1st stage into a

new array according to the structure of the report at the 2nd stage of BP (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) is shown in the figure below.

The general model of transformation of the data accumulated at the 1st stage into a new array according to the structure of the report at the 2nd stage of BP (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG)




## 1.3. Main parameters of SS VFR-PP

The general requirements for the technical and operational characteristics of the SS VFR-PP are largely determined by the specifics of the tasks that must be provided by the ICS PFP through its functional capabilities, namely:

1) support of interaction in a single information space of heads of political parties (local organizations) with NACP analysts and voters;
2) integrated support of heads of political parties (local organizations), including by providing access to convenient information search tools in other ICS (registries, databases, etc.);
3) data exchange with other ICS and reference systems, registers, data banks, including those containing information with limited access, the holder (administrator) of which is state bodies or local self-government bodies;
4) creation, preservation, submission and review of financial reports of leaders of political parties (local organizations) and other electronic documents, the possibility of generating statistical reports;
5) increasing the transparency of the process of receipt and use of funds and property of political parties, voters' access to relevant information;
6) protection of data (including personal data) against unauthorized access, destruction, modification and blocking of access to them;
7) control of storage periods of electronic documents and information;
8) cost savings of political parties due to information exchange and complete elimination of "paper" document circulation (information exchange).

Entered into industrial operation in May 2021, the "Unified State Register of Political

Parties' Reports on Property, Income, Expenses and Financial Liabilities" with the available data fully meets the specified requirements, therefore remains unchanged and should become the SS VFR-PP of the new ICS PFP. Instead, it is necessary to take into account the requirement for compliance of the System's functionality with the requirements of the law, including taking into account possible changes in the law during the modernization of the System.

### 1.4. SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG common parameters

In Section 1.1. "General structure of ICS PFP" it was stated that BP VFR-EFFP, BP VFR-EFFPD, BP VFR-EFFLE, BP VFR-RFFUA, BP VFR-RFFL and BP VFR-RFFG are practically identical in their general logic. It is this fact that determines the presence in each of the corresponding SS (VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) (hereinafter SS(6)) of the same set of SMs covering the same set of corresponding BP steps.

The general requirements for the technical and operational characteristics of the SS(6) are largely determined by the specifics of the tasks that must be provided by the ICS PFP through its functional capabilities, namely:

1) support of interaction in a single information space of EFA/RFA managers with NACP registrars, NACP analysts and voters;
2) integrated support of EFA managers, including by providing access to convenient information search tools in other ICS (registries, databases, etc.);
3) ensuring systematic and comprehensive support for the efficiency of the EFA/RFA managers by automated accumulation of information on the flow of funds to the EFA/RFA with further transformation of the accumulated information into a report of the EFA/RFA manager according to the established form;
4) creating, saving, submitting and reviewing EFA/RFA reports and other electronic documents, the possibility of generating statistical reports;
5) increasing the transparency of the process of receipt and use of funds, voters' access to relevant information (note: the category of funds is indicated for each of SS(6));
6) protection of data (including personal data) against unauthorized access, destruction, modification and blocking of access to them;
7) control of storage periods of electronic documents and information;
8) savings of budget funds and EFA/RFA due to information exchange and complete elimination of "paper" document circulation (information exchange).

SS(6) consists of three interconnected software modules and interacts with 6 separate SS CSM software modules.

#### 1.4.1. Software module 1 (SM 1): "Workstation of NACP registrar"

***Purpose***

Only authorized NACP officials who can create, edit, activate/deactivate EFA manager accounts will have access to this SM.

***Characteristics of the data***

SM 1, like the ICS PFP as a whole, will contain data for the authorization of EFA/RFA managers in the system. In addition, it will contain other reference/relevant information necessary for the implementation of the process of submitting financial statements on receipts and use of the fund.

***SM 1 should provide for the following technical features:***

- functioning of the cabinet for defined groups of users - NACP registrars;
- creation, editing, activation/deactivation of personal accounts for defined groups of users - EFA/RFA managers;
- a section for placing general background information on issues of system operation and data entry.

The specified features of SM 1 are implemented taking into account the interaction (information exchange) of SS(6) with the following program modules of SS CSM:

- SM exchange of information with banks;
- SM work with accounts;
- SM writing the rules of risk operations.

### 1.4.2. Software module 2 (SM 2) "Workstation of the manager of EFA/RFA"

***Purpose***

Only authorized managers of EFA/RFA will have access to work with this SM (note: the category of authorized managers is specified for each SS(6)).

The EFA/RFA manager undergoes two-factor authentication in the ICS PFP based on the authorization data obtained through the SM exchange of information with banks (automated data acquisition method) or in another way outside the system.

***Characteristics of the data***

SM 2, like the ICS PFP as a whole, will contain information on (1) bank details of the EFA/RFA, (2) bank information on the flow of funds to the EFA/RFA and (3) reports of the managers of the EFA/RFA on the receipt and use of fund funds. Information on the specified three groups should also be displayed in the open part of the ICS PFP (public access is provided).

***SM 2 should provide for the following technical features:***

- functioning of personal offices of EFA/RFA managers;
- filling in information about bank details of open current EFA/RFA, as well as displaying it in the open part of ICS PFP (ensure public access);
- daily filling of information about each performed bank transaction on the receipt or use of fund funds and displaying it in the open part of ICS PFP (public access is ensured);
- making changes (additions) by managers of EFA/RFA to information (exclusively within the limits of the requisites specified by law) received from banks, about each completed banking operation on the receipt or use of funds of the fund, grouping it according to uniform characteristics;
- automatic generation of relevant reports of EFA/RFA managers on the receipt and use of money from election/referendum funds, as well as their display in the open part of ICS PFP (public access is ensured);
- interaction of EFA/RFA managers with NACP analysts through personal offices by creating official electronic documents (letters, requests, messages, etc.).

The specified features of SM 2 are implemented taking into account the interaction (information exchange) of SS(6) with the following program modules of SS CSM:

- SM exchange of information with banks;
- SM information exchange with other ICS (registries, databases, etc.);

- SM of logical and arithmetic control (analytics);
- SM publication of information in the public part of ICS PFP.

### 1.4.3. Software module 3 (SW 3) "Workstation of NACP analytics"

***Purpose***

SM 3 uses the processed data entered in SM 2. Only authorized NACP analysts - employees of the NACP Political Corruption Prevention Department will have access to work with this module.

***Characteristics of the data***

SM 3, like the ICS PFP as a whole, will reflect the information and details that are included in the EFA/RFA managers' reports on the receipt and use of funds. The findings of the NACP analysts' analysis of the EFF managers' reports are published in the open ICS PFP (public access is provided).

***SM 3 should provide for the following technical features:***

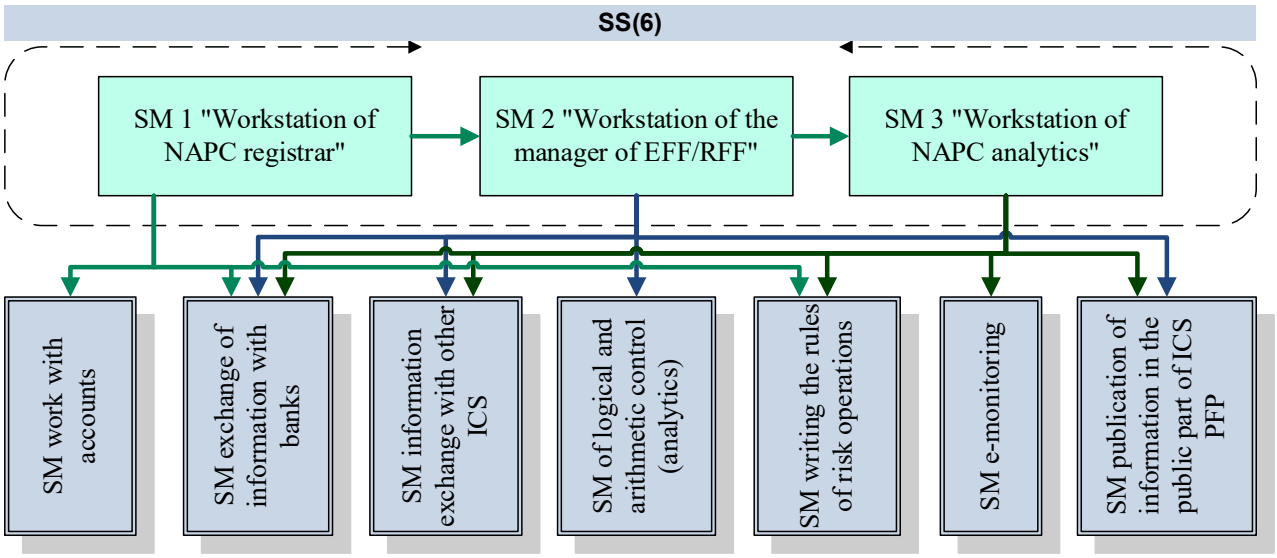
- functioning of personal offices of NACP analysts;
- publication in the open part of the ICS PFP of conclusions (pdf) based on the results of the mandatory and/or selective analysis of reports of EFF managers conducted by NACP analysts;
- the possibility of open round-the-clock viewing, copying and printing of information, saving electronic copies of documents outside ICS PFP, as well as in the form of a set of data (electronic document) organized in a format that allows their automated processing by electronic means (machine reading) for the purpose of reuse;
- interaction of NACP analysts with EFA/RFA managers through personal offices by creating official electronic documents (letters, requests, messages, etc.).

The specified features of SM 3 are implemented taking into account the interaction (information exchange) of SS(6) with the following program modules of SS CSM:

- SM exchange of information with banks;
- SM information exchange with other ICS (registries, databases, etc.);
- SM of logical and arithmetic control (analytics);
- SM writing the rules of risk operations;
- SM e-monitoring;
- SM publication of information in the public part of ICS PFP.

The general model of information exchange between SM SS(6), as well as their interaction with individual software modules of SS CSM, is shown in the figure below.

The general model of information exchange between SM SS(6),
as well as their interaction with individual software modules of SS CSM



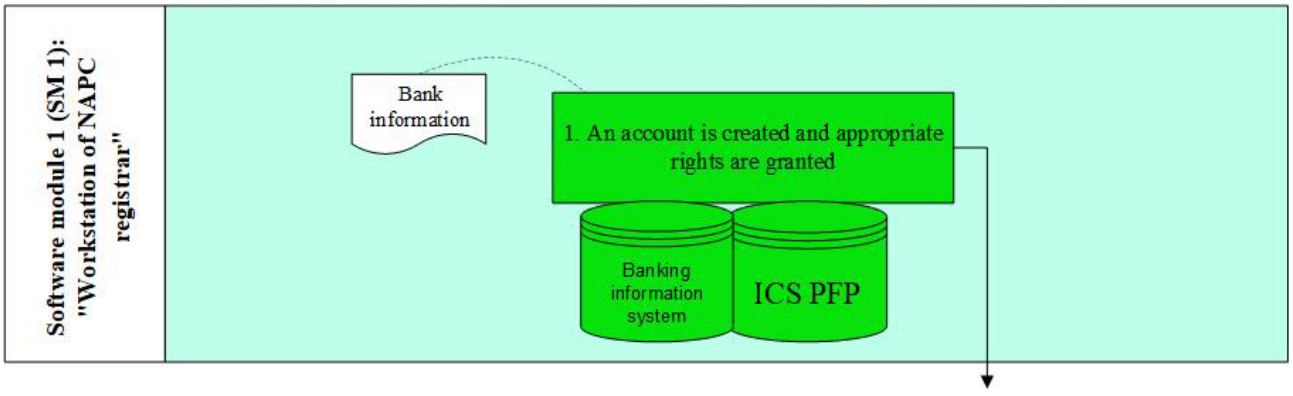

### 1.4.4. Description of the component model BP(6), which is implemented within the framework of SM 1

Only one step BP(6) is implemented within SM 1 "Workstation of NACP registrar". In particular, it is:

***Step 1.*** NACP creates manager accounts, activates/deactivates/edits them in SS(6).

The model of the BP(6) component, which is implemented as part of SM 1 "Workstation of the NACP registrar" is shown in the figure below.

The model of the BP(6) component,
which is implemented as part of SM 1 "Workstation of the NAPC registrar"




### 1.4.5. Description of the component model BP(6), which is implemented within the framework of SM 2

Within SM 2 "Workstation of the manager of EFA/RFA", eight steps (all but the tenth) of the following nine steps of BP(6) are implemented. In particular, it is:

***Step 2.*** The manager of the EFA/RFA within two days, from the day of appointment, undergoes two-factor authentication in the ICS PFP (SS(6)) according to the data contained in the system, received through the SM exchange of information with banks.

At this step, SM 2 "Workstation of the manager of EFA/RFA" also performs control of the following restrictions (quantitative restrictions are parameterized in accordance with the legislation, including taking into account the introduction of legislative changes):

- the maximum number of managers per account is 2 (two);
- the maximum number of accounts that can be serviced by one manager is 2

(two).

***Step 3.*** Information on the opening of EFA/RFA and its details is entered by the manager within two working days after opening the account in ICS PFP (SS(6)) and is displayed in its open part (SM publication of information in the public part of ICS PFP).

***Step 4.*** The bank provides daily information on the amounts and sources of contributions received by the EFA/RFA, the movement of funds, as well as their balances on the current account, which are automatically included in the ICS PFP (SS(6)). This step envisages the integration of ICS PFP with the banking system through the SM exchange of information with banks.

***Step 5.*** The manager of the EFA/RFA gets the opportunity to analyze bank information about the operation and decide on its further confirmation within three working days from the day of its completion. In the event that the manager of the current account of the fund does not confirm the operation of the movement of funds on the current account of the fund within the set time (3 working days), the information received from the bank is automatically displayed in the open part of ICS PFP (SM publication of information in the public part of ICS PFP).

***Step 6.*** In the event of a decision to confirm bank information, the manager of the EFA/RFA confirms each individual transaction or enters new reliable data about the transaction (if the information received from the bank is missing or incorrect for any reason). Information about transactions on the flow of funds confirmed by the manager are automatically published in the open part of ICS PFP (SM publication of information in the public part of ICS PFP).

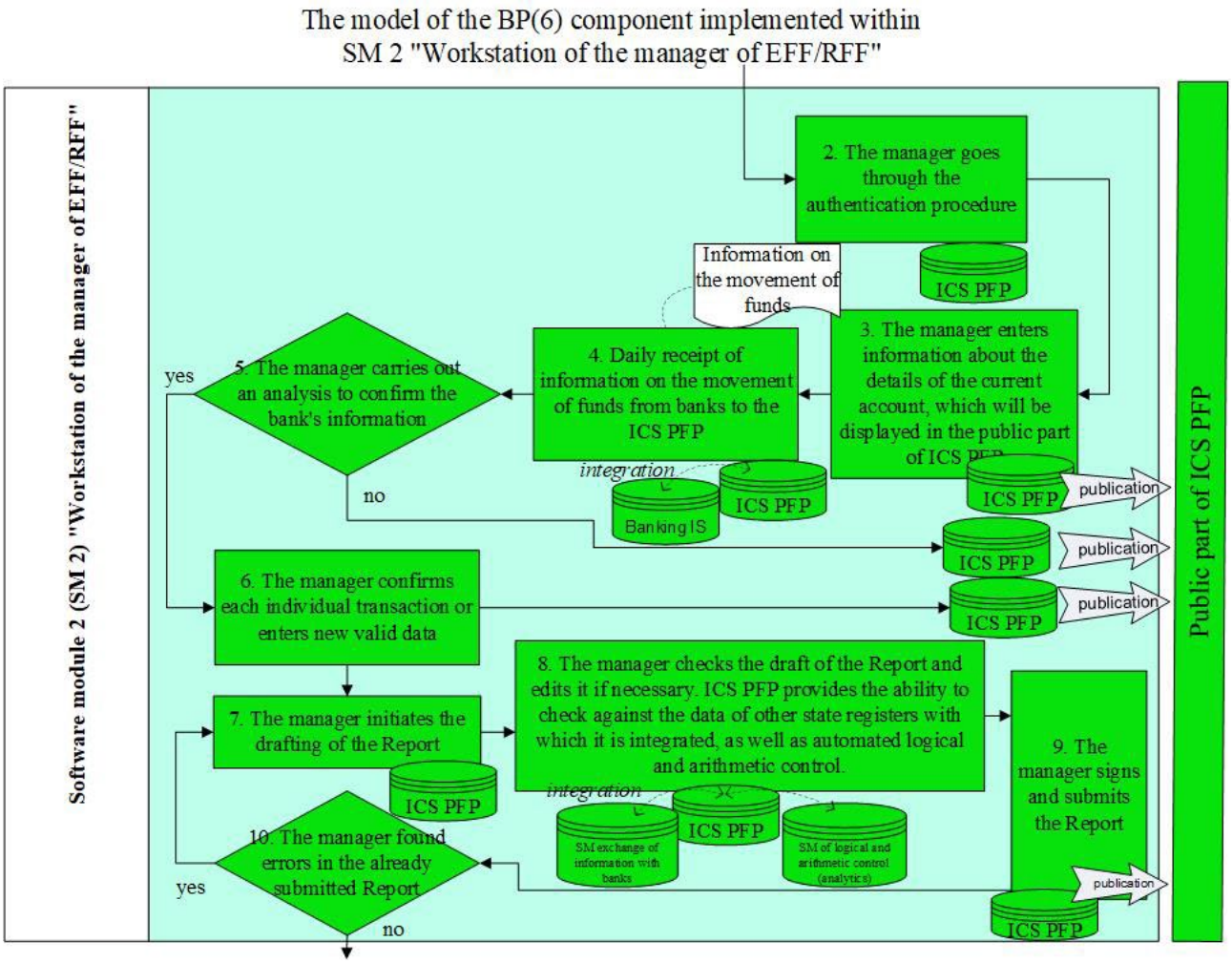
***Step 7.*** The manager of the EFA/RFA initiates the creation of a draft Report in ICS PFP based on information on the flow of funds to the EFA/RFA.

***Step 8.*** The created draft of the Report is checked by the manager of EFA/RFA for the completeness and reliability of the information displayed in it, it is edited and, if necessary, supplemented with appropriate reporting information. ICS PFP (SM information exchange with other ICS (registries, databases, etc.)) functionally provides the manager with the opportunity to perform additional checks of the reliability of reported information based on the data of other state registers with which electronic information interaction has been built. At the same time, ICS PFP (SM of logical and arithmetic control (analytics)) carries out general automated logical and arithmetic control of the correctness of the report.

***Step 9.*** The fund manager signs and submits the report. The submitted report is automatically published in the open part of ICS PFP (SM publication of information in the public part of ICS PFP).

***Step 10.*** If errors (inaccurate information) are found after submitting the Report, the manager will re-form and submit the Report (one-time right) in its entirety within the general term set for its submission.

The model of the BP(6) component implemented within SM 2 "Workstation of the manager of EFA/RFA" is shown in the figure below.




### 1.4.6. Description of the component model BP(6), which is implemented within the framework of SM 3

Three steps of SS(6) are implemented as part of SM 3 "Workstation of NACP analytics". In particular, it is:

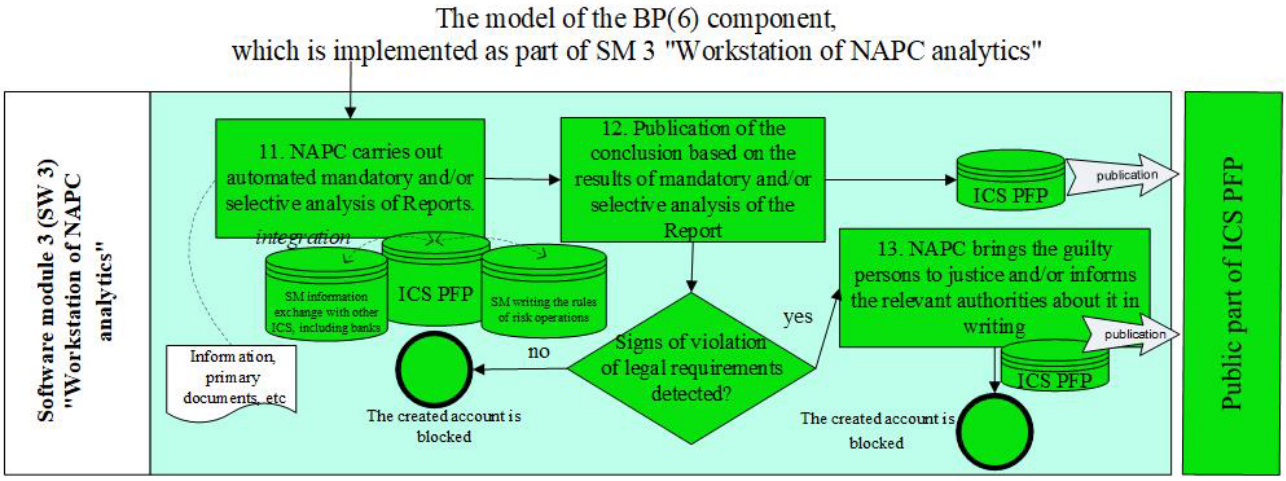
***Step 11.*** The NACP analyzes the EFA/RFA managers' reports (note: the time frame and scope of the report analysis is specified for each SS(6)).

NACP can also carry out a selective analysis of the reports of EFA/RFA managers - in accordance with the risks of financial and economic and other activities of election funds, the criteria of which are approved by NACP.

***Step 12.*** NACP publishes in the open part of the ICS PFP (SM publication of information in the public part of ICS PFP) the conclusion based on the results of the mandatory and/or selective analysis of the report.

***Step 13.*** The NACP publishes information about the response measures taken in the public part of the ICS PFP (SM publication of information in the public part of ICS PFP).

The model of the BP(6) component, which is implemented as part of SM 3 "Workstation of NACP analytics", is shown in the figure below.




## 1.5. Main parameters of SS VFR-EFFP

In addition to Section 1.4. "Basic common parameters of SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG" the SS VFR-EFFP has the following individual functional parameters, namely:

- Category of funds: money of election funds in the elections of the President of Ukraine.
- Estimated number of external users of the closed part of the SS VFR-EFFP (EFA managers) - up to 70 people (in the last presidential elections of Ukraine in 2019, a total of 44 candidates were registered - a record number).
- Only authorized managers of the EFA, who will be appointed by the candidates for the post of the President of Ukraine, will have access to work with this SM.
- NACP carries out a mandatory analysis of the reports of EFF managers within 60 days from the date of the end of the deadline for their submission on the subject of (1) the timeliness of the submission of reports, (2) the compliance of the reported data with the information received from the banks in which the EFA is opened, (3) reliability (correctness) of the information provided in the reports, (4) legality of the sources and origin of the funds received by the EFA.

## 1.6. Main parameters of SS VFR-EFFPD

In addition to Section 1.4. "Basic common parameters of SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG" the SS VFR-EFFPD has the following individual functional parameters, namely:

- Category of funds: money of election funds in the elections of People's Deputies of Ukraine.
- Estimated number of external users of the closed part of the SS VFR-EFFPD (EFA managers) - up to 15,000 people (in the last parliamentary elections in 2019, a total of 5,966 candidates were registered; in addition, it is necessary to take into account the increase in the number of election participants after the deoccupation of the Autonomous Republic of Crimea and other temporarily occupied regions of the country).
- Only authorized EFA managers appointed by parties or candidates for People's Deputies will have access to work with this SM.
- NACP carries out a mandatory analysis of the reports of EFA managers within 60 days from the date of the end of the deadline for their submission on the subject of (1) the timeliness of the submission of reports, (2) the compliance of the reported data with the information received from the banks in which the EFA is opened, (3) reliability (correctness) of the information provided in the

reports, (4) legality of the sources and origin of the funds received by the EFA.

### 1.7. Main parameters of SS VFR-EFFLE

In addition to Section 1.4. "Basic common parameters of SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG" the SS VFR-EFFLE has the following individual functional parameters, namely:

- Category of funds: money of election funds in local elections.
- Estimated number of external users of the closed part of the SS VFR-EFFLE (EFA managers) – up to 550,000 people (in the last regular local elections in 2020, a total of over 282,000 candidates for deputies of local councils of territorial communities and candidates for the post of city mayor were registered; in addition, it is necessary take into account the increase in the number of election participants after the deoccupation of Crimea and other temporarily occupied regions of the country).
- Only authorized managers of the EFA, who will be appointed by political parties, candidates for deputies of local councils of territorial communities and candidates for the position of mayor, will have access to work with this SM.
- NACP carries out a mandatory automated analysis of the reports of the EFA managers within 120 days from the end of the deadline for their submission in order to determine the timeliness of the submission of the specified reports.

### 1.8. Main parameters of SS VFR-RFFUA

In addition to Section 1.4. "Basic common parameters of SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG" the SS VFR-RFFUA has the following individual functional parameters, namely:

- Category of funds: money of all-Ukrainian referendum funds.
- Estimated number of external users of the closed part of the SS VFR-RFFUA (RFA managers) - no more than 5 people annually (from 1991 to the present time, only two all-Ukrainian referenda have been held in Ukraine).
- Only authorized managers of the RFA, who will be appointed by political parties or public organizations, will have access to work with this SM. The decision to appoint an RFA is made by a political party or public organization, which is required to send a package of documents on the appointment of an RFA to the NACP with its personal data.
- NACP creates manager accounts, activates/deactivates/edits them in SS VFR-RFFUA according to the data received through SM exchange of information with banks and based on the information contained in the package of documents sent by the political party (public organization).
- The manager of the RFA within two days, from the day of appointment, undergoes two-factor authentication in the ICS PFP (SS VFR-RFFUA) according to the data contained in the system, received through the SM exchange of information with banks and based on the information contained in the package of documents, sent by a political party (public organization).
- NACP, within fifteen days from the date of the expiration of the period for collecting signatures or the termination of the initiative, performs a mandatory automated analysis of the RFA managers' reports on their submission for the timeliness of their submission and compliance of the reported data with the information received from the banks where the fund accounts are opened .

### 1.9. Main parameters of SS VFR-RFFL

In addition to Section 1.4. "Basic common parameters of SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG" the SS VFR-RFFL has the following individual functional parameters, namely:

- Category of funds: money of local referendum funds.
- The estimated number of external users of the closed part of the SS VFR-RFFL (RFA managers) is no more than 2,000 people annually (from 1991 to the present, only five local referendums have been held in Ukraine, not including the pseudo-referendums held in 2014 and 2022 in the east and southern Ukraine). At the same time, the total number of external users is calculated based on the fact that 1,469 territorial communities have been created in Ukraine today, as well as on the assumption of holding local referendums in all territorial communities at the same time.
- Only authorized RFA managers appointed by political parties or public organizations will have access to work with SM 2 “Workstation of the manager of EFA/RFA”. The decision to appoint an RFA is made by a political party or public organization, which is required to send a package of documents on the appointment of an RFA to the NACP with its personal data.
- NACP creates manager accounts, activates/deactivates/edits them in SS VFR-RFFL according to the data received through the SM exchange of information with banks and based on the information contained in the package of documents sent by the political party (public organization).
- The manager of the RFA within two days, from the day of appointment, undergoes two-factor authentication in the ICS PFP (SS VFR-RFFL) according to the data contained in the system, received through the SM exchange of information with banks and based on the information contained in the document package, sent by a political party (public organization).
- NACP, within fifteen days from the date of the expiration of the period for collecting signatures or the termination of the initiative, performs a mandatory automated analysis of the RFA managers’ reports on their submission for the timeliness of their submission and compliance of the reported data with the information received from the banks where the fund accounts are opened.

## 1.10. Main parameters of SS VFR-RFFG

In addition to Section 1.4. “Basic common parameters of SS VFR-EFFP, SS VFR-EFFPD, SS VFR-EFFLE, SS VFR-RFFUA, SS VFR-RFFL and SS VFR-RFFG” the SS VFR-RFFG has the following individual functional parameters, namely:

- Category of funds: money of local referendum funds.
- Estimated number of external users of the closed part of the SS VFR-RFFG (RFA managers) – no more than 4,000 people (2,000 RFA managers of initiative groups + 2,000 RFA campaign managers) annually (from 1991 to the present, only two all-Ukrainian referenda have been held in Ukraine and five local referendums). At the same time, the total number of external users is calculated based on the fact that 1,469 territorial communities have been created in Ukraine today, as well as on the assumption of holding an all-Ukrainian referendum and local referendums in all territorial communities at the same time.
- Only authorized managers of the RFA, who will be appointed by political parties or public organizations, will have access to work with this SM. The decision to appoint an RFA is made by a political party or public organization, which is required to send a package of documents on the appointment of an

RFA to the NACP with its personal data.

- NACP creates manager accounts, activates/deactivates/edits them in SS VFR-RFFG based on the data received through the SM exchange of information with banks and based on the information contained in the package of documents sent by the political party (public organization).
- The manager of the RFA within two days, from the day of appointment, undergoes two-factor authentication in the ICS PFP (SS VFR-RFFG) according to the data contained in the system, received through the SM exchange of information with banks and based on the information contained in the package of documents, sent by a political party (public organization).
- NACP, within fifteen days from the date of the expiration of the period for collecting signatures or the termination of the initiative, performs a mandatory automated analysis of the RFA managers' reports on their submission for the timeliness of their submission and compliance of the reported data with the information received from the banks where the fund accounts are opened.

## 2. MAIN PARAMETERS SS CSM

SS CSM occupies a special importance in the structure of ICS PFP, which due to its specific function interacts with all other SS (VFR-PP, VFR-EFFP, VFR-EFFPD, VFR-EFFLE, VFR-RFFUA, VFR-RFFL and SS VFR-RFFG) and includes a set of such SMs:

- SM writing the rules of risk operations;
- SM of information exchange with banks;
- SM works with accounts;
- SM of logic and arithmetic control (analytics);
- SM information exchange with other ICS (registries, databases, etc.);
- SM publication of information in the public part of ICS PFP;
- SM e-monitoring.

### 2.1. Description of the parameters of SM writing the rules of risk operations

***Purpose***

SM writing the rules of risk operations should implement a convenient tool for creating logical and arithmetic control rules for subsequent automatic data analysis of both the received reports of responsible persons (managers and SS) and at the stage of obtaining information about transactions during the election process.

The module is designed to automate processes:

- creation of verification rules for preliminary (before reporting) detection of transactions that may be illegal (for example, receiving financing from persons under 18 years of age, etc.) and informing managers of possible violations;
- adjusting (adding and editing) existing rules and forming new rules for logical and arithmetic control of reporting forms to determine their risk rating;
- implementation of logical and arithmetic control rules approved by NACP decisions;
- optimization of the process of determining the risk rating of reporting forms by NACP personnel.

***SM writing the rules of risk operations should provide for the following technical features:***

- functioning of the office for certain groups of users;
- creation, editing, activation/deactivation of rules of risk operations;
- a section for placing statistical information on the identification and marking of

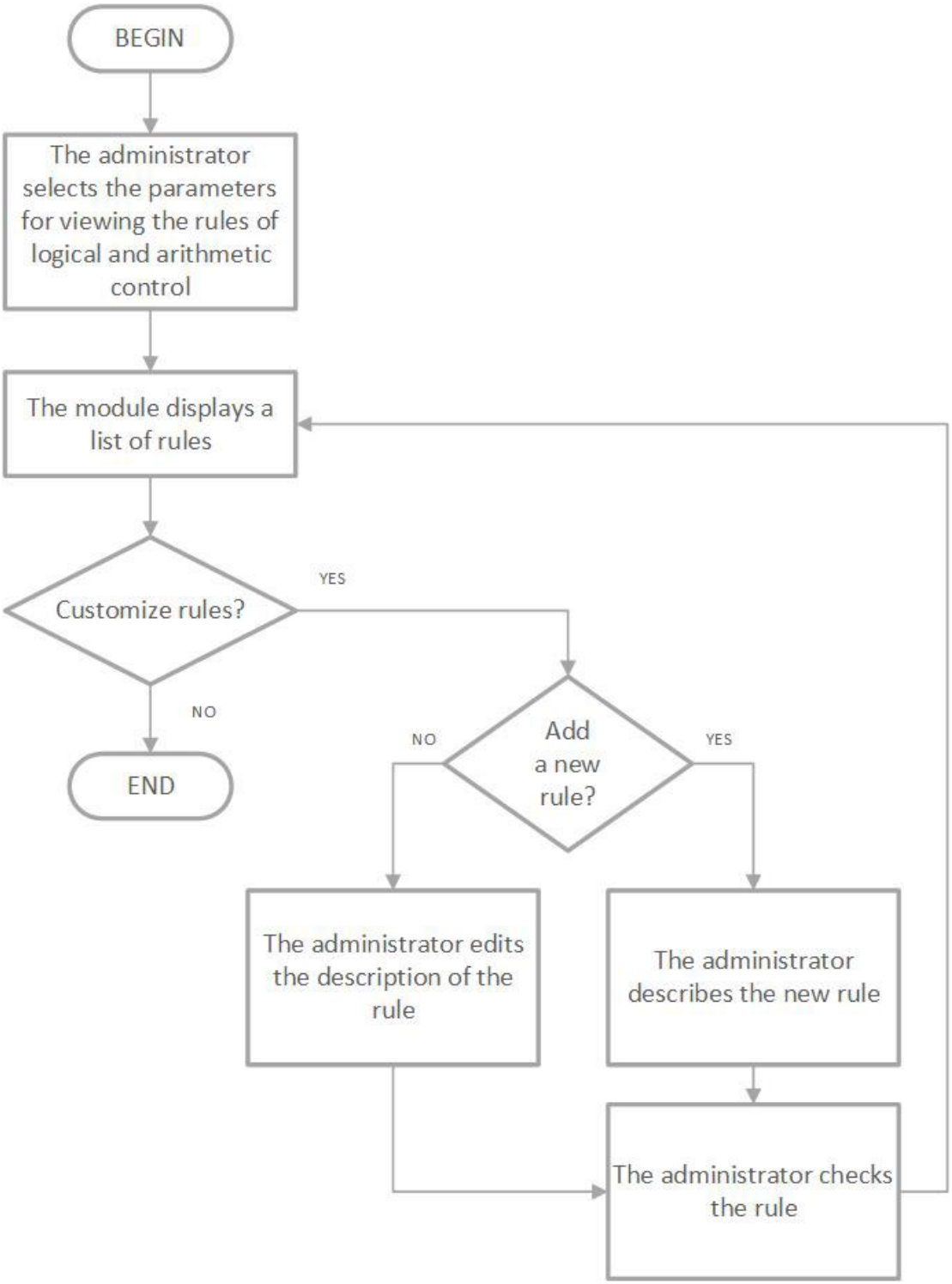
operations, the criteria of which correspond to a set of signs/characteristics of risky operations;
- a section for placing general background information on issues of system operation and data entry.

Features of the functional requirements for the module:

- editing the rules of logical and arithmetic control, changing the status (activation and deactivation of the rule) and the weight of the rules;
- managing versioning, including the possibility of using a specific version at the stage of control;
- editing parameters of exchange drivers, activation and deactivation of drivers;
- maintaining and further taking into account the values of chronological parameters (exchange rates, minimum wage, living wage, etc.);
- viewing the statistics of the verification rules with the specified number of triggered, non-triggered rules and verification errors.

Rules for logical and arithmetic control of reporting forms must contain the main attributes: rule identifier, identifier of the type of reporting form to which the rule applies, rule body, rule weight, rule status and version, rule name, rule description.

The process of setting the rules of logical and arithmetic control of reports by the administrator is shown in the diagram:




The administrator must be able to configure the rules for logical and arithmetic control of reports by creating new or editing existing rules. Parameters of logical and arithmetic control rules (name, description and weight) are defined by NACP. Checking the rule code is possible after filling in the rule code field of logical and arithmetic control and specifying the internal number of the arbitrary report.

The process of logical and arithmetic control of reports takes place in automatic mode, as a result of which the list of reporting forms is updated with information about the calculated risk rating of the reporting form, as well as a list of rules that "worked" or "did not work" for each reporting form is provided. The risk of the reporting form is determined in a numerical indicator, taking into account the number and weight of the rules involved in the process of logical and arithmetic control.

In the process of checking the reporting forms, the latest versions of the activated rules

are used.

When adding a rule, the first version of the rule is set each time, when editing rules, the version is increased by one.

## 2.2. Description of the parameters of SM exchange of information with banks

***Purpose***

SM of information exchange with banks should implement in automatic mode centralized processing of financial information received from banks and storage of its results for further processing by authorized employees of NACP and managers of EFA/RFA in SS(6).

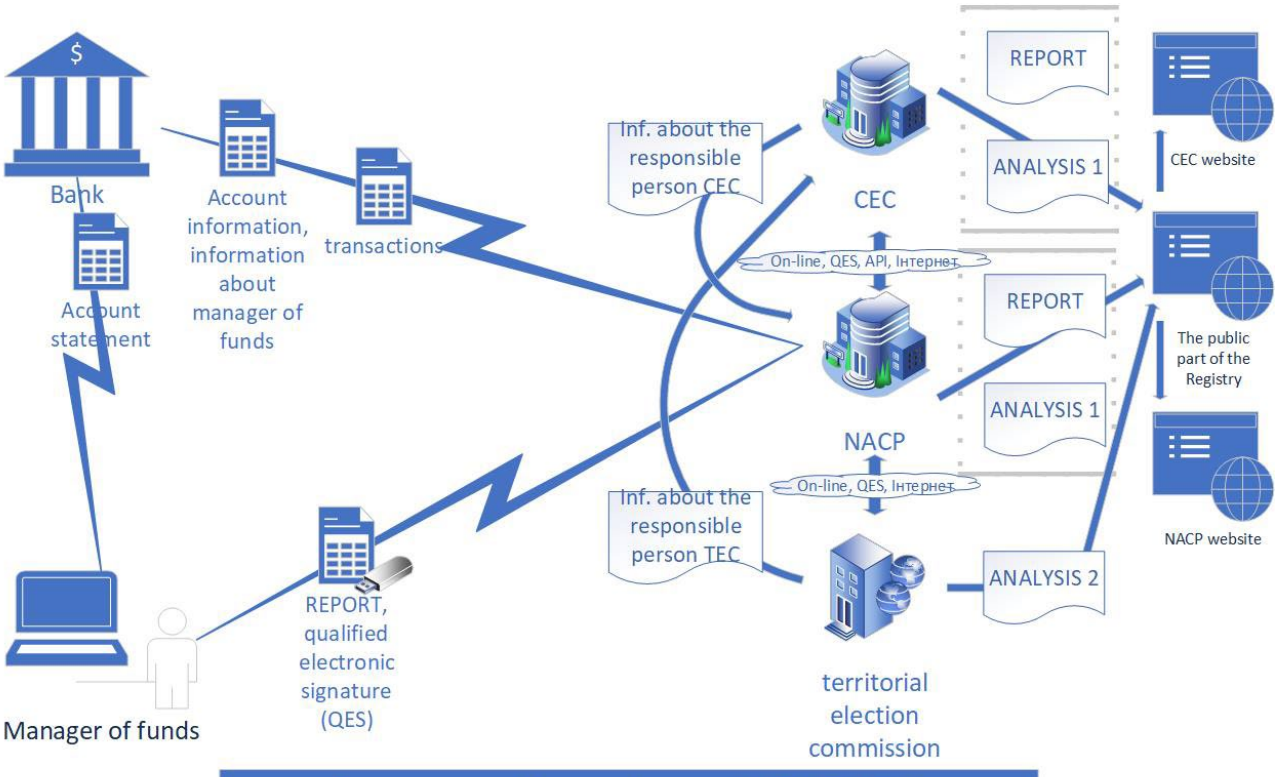
The exchange of information between NACP and banks is carried out in a secure form using the APM-NBU-information system.

***Characteristics of the data***

The bank not later than the next working day after the day of opening the EFA/RFA current account notifies the NACP about the opening of the corresponding account and its details using the APM-NBU-information in accordance with the agreed Description of file structures to form a register of documents about the details of current EFA/RFA.

The only source of information for monitoring the functioning of the EFA/RFA is information from the banks in which EFA/RFA accounts are opened, on the receipt and use of EFA/RFA funds. The bank in which the EFA/RFA is opened provides information on the receipt and use of funds of the fund to the NACP every day no later than 12 o'clock using the APM-NBU-information in accordance with the Description of file structures for the formation of a register of documents for the transfer of the receipt and use of EFA/RFA funds and Instructions on the procedure for exchanging information between NACP and banks.

Information received from banks is processed exclusively automatically, is not subject to any correction and is stored in the ICS PFP database, where it becomes available for further processing by authorized NACP employees and EFA/RFA managers in SS(6).




Document flow scheme (DESIGNED)

***SM of information exchange with banks should provide for the following technical features:***

- functioning of the office for certain groups of users;
- formation of a set of information (data) from banks' information about the opening of EFA/RFA for further creation/activation of the personal account of the manager of EFA/RFA;
- creation, editing, activation/deactivation of the rules of receipt and storage for further processing of information from banks regarding the opening of EFA/RFA, conducted banking operations and closing of EFA/RFA (further transformation of accumulated information into a report of the manager of EFA/RFA according to the established form);
- a section for placing statistical information on the opening of EFA/RFA, conducted banking operations and closing of EFA/RFA;
- a section for placing general background information on issues of system operation and data entry.

The structure (set of details) of the information received from the banks about the conducted banking operations will differ depending on the group of the banking operation. In turn, groups of banking operations will be determined depending on the approved structure and forms of financial statements of EFA/RFA managers.

For example, consider the sets of details of banking operations that will be carried out by EFA/RFA within the framework of BP VFR-EFFPD.

Group 1: information on the receipt of the candidate's/political party's own funds to the EFF should be submitted according to the following structure (set of details):

- income article code;
- date of receipt of funds;
- settlement document number;
- type of receipt;
- Full name of the candidate / name of the political party;
- amount (UAH).

Group 2: information on the receipt of voluntary contributions from individuals and legal entities to the EFA should be submitted according to the following structure (set of details):

- article code;
- date of receipt of funds;
- settlement document number;
- full name of an individual/business entity/name of a legal entity;
- place of residence/location of the person who made the contribution;
- RNTAC/ passport series and number, ID card number/ legal entity identification code;
- date of birth of the natural person who made the contribution;
- amount (UAH).

Group 3: information on erroneous receipts of funds to the EFA should be submitted according to the following structure (set of details):

- article code;
- date of receipt of funds;
- settlement document number;
- full name of a natural person / business entity / name of a legal entity;

- place of residence of a natural person / private entrepreneur / location of a legal entity;
- RNTAC / passport series and number, ID card number / legal entity identification code;
- type of person;
- purpose of payment;
- amount (UAH).

Group 4: information on the return of funds from the EFA should be submitted according to the following structure (set of details):

- electoral region number;
- article code;
- refund date;
- type of return;
- EFF number;
- settlement document number;
- full name of a natural person / business entity / name of a legal entity;
- place of residence of a natural person / private entrepreneur / location of a legal entity;
- RNTAC / passport series and number, ID card number / legal entity identification code;
- type of person;
- details of the contract (date of conclusion, number and subject of the contract);
- purpose of payment;
- amount (UAH).

Group 5: information on the return (transfer) of voluntary contributions from individuals and legal entities should be submitted according to the following structure (set of details):

- article code;
- date of receipt of contribution;
- full name of a natural person / private entrepreneur / name of a legal entity;
- RNTAC, passport series and number, ID card number/ legal entity identification code;
- amount (UAH);
- article code;
- date of return (listing);
- type of person;
- full name of a natural person / private entrepreneur / name of a legal entity;
- RNTAC, series and passport number, number;
- ID cards / identification code of a legal entity;
- type of return (listing);
- refund amount (UAH);
- the amount transferred to the state budget (UAH).

Group 6: information about EFA payments is submitted according to the following structure (a set of details):

- electoral region number;
- article code;
- account type;

- payment date;
- settlement document number;
- type of expenses;
- information about the recipient;
- purpose of payment;
- amount (UAH);
- type of person;
- full name / private entrepreneur / name of the legal entity;
- RNTAC, passport series and number, ID card number / legal entity identification code;
- place of residence/ location of the person.

### 2.3. Description of the parameters of SM work with accounts

A mandatory condition for access to ICS PFP for all categories of users, with the exception of the "Visitor" role, is the use of a qualified electronic signature.

User authentication is performed using personalization options embedded in electronic identification systems, electronic signatures and seals. Authorization of access rights of all users of ICS PFP to the functions, services and information resources that concern them is carried out in accordance with the access profiles tied to the organizational structure of the NACP apparatus, roles and groups of rights assigned to them in ICS PFP.

Considering the large number of users in the role of EFA/RFA manager in SS(6), the registration of user data accounts in ICS PFP is performed in automated mode by automatically forming personalization parameters based on data received from banks through SM exchange of information with banks:

- the bank not later than the next working day after the opening of the EFA/RFA current account notifies the NACP about the opening of the corresponding account, its details and identification data of the EFA/RFA manager using the APM-NBU-information in accordance with the agreed Description of file structures to form a register of documents about the details current EFA/RFA;
- information received from banks is transformed into an electronic identification system for further authentication of users;
- the manager of EFA/RFA is registered in ICS PFP using an electronic key;
- SM work with accounts performs an automated search for the identification data of the electronic key of the EFA/RFA manager on all ICS PFP accounts and provides access to the corresponding SS(6);
- in the event that the ICS PFP user is simultaneously registered in several roles, SM work with accounts must offer to choose one of them and provide access to the corresponding SS(6) taking into account the user's choice;
- a registered user can work in only one role at the same time in one session; to register in a different role, the user must re-register in ICS PFP; simultaneous physical connection of a user in different roles to ICS PFP in different connection sessions is not prohibited.

Registration of accounts of other categories of users in ICS PFP is done by Registrar or Administrator or NACP Security Administrator according to manual registration regulations.

The functionality of SM work with accounts should include:

- authorization by means of QES for administrative accounts of political parties and local organizations;
- authorization by means of QES for party employees authorized to fill out the

report;

- authorization by means of QES for managers of EFA/RFA;
- authorization by means of QES for the accounts of the Head of Analysts and Analysts of the Agency;
- authorization by means of QES for the System Administrator;
- authorization by means of QES for the Security Administrator;
- restoration of access to the cabinet in case of termination of the key with saved data.

Implementation is provided as follows:

- users must be authorized using the OAuth 2.0 protocol with support for authorization using an electronic signature.
- based on QES tools, including a strengthened QES public key certificate and a secure private key carrier.
- cryptographic libraries for qualified electronic signature must be used for authorization. For this, the "IIT User CSK-1" libraries should be used, which should work as a separate service, which will be accessed by the authorization service.
- the service must work as a separate independent service with the possibility of scaling to several servers.
- a separate database must be used for the service.
- the mechanism for restoring access to the cabinet in case of termination of the key does not require confirmation. This mechanism means providing user access to the cabinet with a new key issued by QPETS. At the same time, the System checks the data of the person's RNTAC key, which allows logging in under a new key.
- the service should automatically access the QPETS that issued the user's key to check the lists of revoked certificates and also to determine the timestamp.
- key authentication must be provided in accordance with the Electronic Trust Services Act. To use the hardware key, you need to install a browser plug-in.
- during registration, validation of the user's e-mail address must be ensured by sending a message with a confirmation code to this address.
- during registration, the key data must be read automatically - the RNTAC key data of the person, which allows entering under a new key.
- automatic logging of the authorization service should be provided. To do this, the following data about each user action must be recorded in the logs: user ID, timestamp of the operation, browser, IP address, data of the user's device and the code of the operation that was performed.
- all QPETS keys that have the appropriate certificate at the time the System is put into trial operation must be supported.

### 2.4. Description of the parameters of SM of logic and arithmetic control (analytics)

The purpose of creating SM of logic and arithmetic control (analytics) is to provide automatic analysis of data from reports of political parties (funds), in accordance with the needs of NACP.

The module allows you to automate the process of logical and arithmetic control of reports of political parties (funds) with the preservation of data of control results.

Logical and arithmetical control of the reports of political parties (funds) involves clarifying the correspondence of the information specified in the report to information from

registers, databases and other information and communication systems of state bodies.

Interaction with external registries to obtain the specified information takes place in accordance with approved automated exchange protocols.

The module uses data received from the exchange system with external state registers and a set of rules for automatic analysis and verification of reports on:

- violation of legal requirements;
- presence of risky operations that require additional verification.

The output of SM of logic and arithmetic control (analytics) is a comprehensive and visual log of violations found, rules that worked, and links to specific report entries and/or register responses detailing the violations and providing the NACP analyst with maximum information for further investigation.

SM of logic and arithmetic control (analytics) ranks reports by the value of the sum of the weighting factors from the highest degree to the lowest.

Report verification algorithm:

1) The head of analysts opens access to the party (fund) report for the analyst who was selected by the autodistribution system. If necessary, the head of analysts can give this analyst access to previous reports of this party or reports of other parties.
2) The system of exchange with external state registers sends requests regarding the information provided in the report to external registers and accumulates the responses of the registers.
3) The party report analysis and verification system performs an automatic analysis of the report information and the attached responses of the registers and generates a detailed verification protocol, which indicates the violations and risks found, indicating the rules of risk analysis that worked, and a link to the records of the report and the responses of the registers, on the basis of which the system found a violation.
4) The NACP analyst accesses the report, supporting documents, and protocol of its automatic analysis and registry responses and begins its review in accordance with the order. If necessary, the NACP Analyst has the ability to create a comment on a specific report.
5) Based on the results of checking the reports, the NACP analyst draws up a conclusion in the established form, which is signed by the head of the structural unit and approved by the NACP order outside the ICS, with subsequent uploading of photocopies of the conclusion to the System.

Algorithm for verifying transactions during the election process:

1) All transactions are subject to automatic verification for violations of the direct prohibition against making voluntary contributions to the election fund (for example, a transaction initiated by a citizen of Ukraine who has not reached the age of 18).
2) The system of exchange with external state registries sends requests for information obtained from transactions to external registries and accumulates the responses of the registries.
3) The system of analysis and verification of party reports performs an automatic analysis of transaction information and the attached responses of the registers and generates an appropriate information message to the manager of the EFA/RFA regarding a specific transaction with an indication of the rules of risk analysis that worked and a reference to the responses of the registers, on the basis of which the system found violation.

4) The manager of the EFA/RFA gets access to the information message about the automatic detection of a possible violation and starts its verification according to the procedure.
5) Information on possible violations detected automatically and the results of their processing by EFA/RFA managers is available to NACP analysts when drawing up conclusions according to the prescribed form.

## 2.5. Description of the parameters of SM information exchange with other ICS (registries, databases, etc.)

### 2.5.1. General requirements for SM information exchange with other ICS

API-interfaces for importing data from other ICS or exporting data to other systems must be implemented in ICS PFP. The ICS PFP software must provide informational exchange and interoperability with other ICS.

SM information exchange with other ICS should automatically collect and accumulate information from external sources, which can then be used by NACP analysts and the system of analysis and verification of party and fund reports.

SM information exchange with other ICS should have a modular architecture that will allow:

- send requests for specified identification fields in accordance with the concluded protocols of interaction with the holders of registers and databases;
- aggregate requests for batch processing;
- perform batch requests to external registries according to the schedule (for example, at night) or in ad-hoc mode (for registries that do not have load restrictions);
- receive and interpret the responses of external registries, generate a visual representation of such responses and attach the received to the batch report;
- exchange with external registries according to the exchange protocols used by such registries and in a protected manner defined by law.

Electronic data exchange is carried out on the basis of:

- Law of Ukraine "On electronic trust services";
- Law of Ukraine "On Electronic Documents and Electronic Document Management";
- Law of Ukraine "On information protection in information and communication systems";
- Law of Ukraine "On Public Electronic Registers".

According to clause $1^2$ of part 1 of article 12 of the Law of Ukraine "On Prevention of Corruption", in order to fulfill the powers assigned to it, NACP has the right to have direct access to information databases of state bodies, authorities of the Autonomous Republic of Crimea, local self-government bodies, to use state databases, including government communication and communications systems, special communication networks and other technical means.

The procedure and regulations for multilateral information interaction between the ICS PFP and other ICS, the use of access technologies to information resources (databases), information exchange files, the composition of their details will be determined by contracts concluded between the NACP and the ministries and departments that are holders of other ICS.

A prerequisite imposed on the interoperability architecture is consistency with usage

regulations developed for other systems.

The classification and coding system should support the process of accumulating and storing information, as well as solving functional problems with minimal memory consumption and maximum speed due to the use of local ICS PFP directories.

**SM information exchange with other ICS provides electronic data exchange with:**

1) State Tax Service of Ukraine.
2) Ministry of Justice of Ukraine.
3) Ministry of Internal Affairs of Ukraine.
4) State Migration Service of Ukraine.
5) Ministry of Economy of Ukraine, State Enterprise "Prozorro".
6) State Judicial Administration of Ukraine.

**Electronic data exchange is implemented (or planned to be implemented) with the following information systems:**

1) "Tax block" information and telecommunication system.
2) "State register of natural persons - taxpayers (Database 1-DF)".
3) "Unified state register of legal entities, individual entrepreneurs and public organizations."
4) "State register of property rights to immovable property".
5) "State register of acts of civil status of citizens".
6) "Unified state register of vehicles".
7) "Integrated interdepartmental information and communication system regarding the control of persons, vehicles and goods crossing the state border."
8) "Unified state demographic register".
9) "Electronic public procurement system of Ukraine ProZorro".
10) "Unified state register of court decisions".
11) "Unified judicial information and telecommunication system".
12) "Unified state register of declarations of persons authorized to perform the functions of the state or local self-government".

It should be noted that SM information exchange with other ICS also provides electronic data exchange with the "Unified state register of declarations of persons authorized to perform the functions of the state or local self-government", the holder of which is the National Agency on Corruption Prevention.

Between ICS PFP and other ICS, there will be an electronic exchange of information (data), which is the property of the state and is created in the course of the current activities of executive authorities and may be subject to protection.

According to the access mode, the information exchanged between ICS PFP and other ICS is divided into:

- open information;
- information with restricted access.

Legally restricted information is confidential information.

For its part, the NACP must ensure the exchange of information using secure communication channels and the experience gained during the creation of similar interactions for the system of logical and arithmetic control of the register of declarations.

### 2.5.2. Interaction with other IT systems

**State ISEV id.gov.ua**

Provides authentication and authorization to the registry using QES and signing reports.

**Address register**

Ensures validation of the addresses entered when filling out the draft report and their codification. The integration of such a register (in the scope of KOATUU or a deeper register, such as the address register of ATU BP NAIS) will allow for effective codification of geographic information and will simplify further analysis of data on contributions to geographic anomalies.

**Open data portal data.gov.ua**

Ensures the publication of submitted reports in the form of open data and provides quick access to all reports in machine-readable formats. A semi-automated interaction is possible, in which ICS PFP provides the export of public data reports in a machine-readable format, followed by manual download of these files by an authorized NACP employee.

**System of self-distribution of NACP cases**

The internal document management system of NACP has a built-in functionality of auto-allocation of cases between NACP analysts. ICS should automatically generate and send an e-mail with the details of submitted reports to the incoming correspondence processing and registration department for further registration in the auto-distribution system.

### 2.5.3. External registries for checking reports

**Unified state register of legal entities, individual entrepreneurs and public organizations**

The holder of the register is the Ministry of Justice of Ukraine.

This database is necessary for verification in accordance with parts nine and fifteen of Article 17 of the Law of the reliability of the data included in the Report regarding:

- the full name of the political party (hereinafter referred to as the Party), local organizations of the political party, which in accordance with the established procedure acquired the status of a legal entity (hereinafter referred to as the LO);
- organizational and legal form (political party, structural formation of a political party);
- presence/absence/quantity in case of presence/ of such LOs;
- identification code of the Party/LO;
- addresses of the location of the Party/LO;
- dates and numbers of entries in the Unified State Register regarding the Party/LO;
- information about the head of the Party/LO, etc.: surname, first name, patronymic, date of election (appointment), data on the presence of restrictions on the representation of a legal entity;
- data on registration actions.

Also, this database is necessary for verification, in accordance with Article 15 of the Law, of legal entities that have contributed to the support of the Party/LO, regarding:

- the existence of such a legal entity in the Unified State Register (namely: is the legal entity that provided support to the Party/LO an unregistered public association, charitable or religious association (organization);
- organizational and legal form, type of public formation, list of founders (participants), information about the ultimate beneficial owner (controller) of such a legal entity (legal entities whose ultimate beneficial owners (controllers) are the persons indicated in subparagraphs "a", "c "-"i" of paragraph 1 and in subparagraph "a" of paragraph 2 of the first part of Article 3 of the Law of Ukraine "On Prevention of Corruption").

**The unified state register of declarations of persons authorized to perform the functions of the state or local self-government**

The holder of the register is NACP.

This database is necessary for verification, in accordance with Article 15 of the Law, of legal entities that have contributed to the support of the Party/LO, regarding:

- whether the ultimate beneficial owner (controller) of the legal entity that provided support to the Party/LO is not a person authorized to perform the functions of the state or local self-government, in accordance with the Law of Ukraine "On Prevention of Corruption" (who belongs to such persons is defined in clause 1 of Part 1 of Article 3 of this Law).

**The only database of the State tax service of Ukraine**

The holder of the register is State tax service of Ukraine.

This database is necessary for verification in accordance with parts nine and fifteen of Article 17 of the Law of the reliability of the data included in the Report regarding:

- availability of full-time employees in Parties/LOs and amounts of income accrued (paid) to them and withheld taxes.

**Unified state demographic register**

The administrator is the state enterprise "Dokument", which belongs to the sphere of management of the State Migration Service in accordance with the order of the CMU dated 07.12.2016 No. 931.

This database is necessary for the verification in accordance with Article 15 of the Law of natural persons who have contributed to the support of the Party/LO regarding:

- citizenship and age.

**State register of property rights to immovable property**

Website: https://kap.minjust.gov.ua/.

The holder of the Register is the Ministry of Justice of Ukraine.

This database is necessary to verify, in accordance with parts nine and fifteen of Article 17 of the Law, the reliability of the data included in the Report regarding:

- presence/absence of immovable property (except land plots) in the ownership of the Party/LO;
- information about the owners of the property, which is in the Party/LO with the right of use.

**Unified state register of vehicles of the Ministry of Internal Affairs**

Website: https://igov.gov.ua/service/1397/general.

The holder of the Register is the Ministry of Internal Affairs of Ukraine.

This database is necessary for verification in accordance with parts nine and fifteen of Article 17 of the Law of the reliability of the data included in the Report regarding:

- the presence/absence of vehicles owned by the Party/LO.

**State land cadastre**

Website: https://e.land.gov.ua/.

The holder of the State Land Cadastre is the State Geocadastre in accordance with the Resolution of the CMU of October 17, 2012 No. 1051 "On Approval of the Procedure for Maintaining the State Land Cadastre."

This database is necessary for verification in accordance with parts nine and fifteen of Article 17 of the Law of the reliability of the data included in the Report regarding:

- presence/absence of land plots in the ownership of the Party/LO.

**Information database of the national securities and stock market commission on the securities market**

Website: http://smida.gov.ua/.

The information database on the securities market is created and maintained by the State institution "Agency for the Development of the Infrastructure of the Stock Market of Ukraine" in accordance with the decision of the National Commission for Securities and the Stock Market dated 03.06.2014 No. 733 "On approval of the Regulation on the formation of an information database on the securities market papers".

This database is necessary for verification in accordance with parts nine and fifteen of Article 17 of the Law of the reliability of the data included in the Report regarding:

- presence/absence of securities owned by the Party/LO.

**PROZORRO central public procurement database**

Website: http://bi.prozorro.gov.ua/.

This database is necessary for verification, in accordance with Article 15 of the Law, of legal entities and individuals who have contributed to the support of the Party/LO, regarding:

- their conclusion of contracts on the procurement of works, goods or services to meet the needs of the state or territorial community in accordance with the Law of Ukraine "On Public Procurement".

**Unified state register of court decisions**

Website: http://www.reyestr.court.gov.ua/.

The holder of the Register is the State Judicial Administration.

This database is necessary for verification, in accordance with Article 15 of the Law, of individuals who have contributed to the support of the Party/LO regarding:

- the presence of a court decision on recognition of such persons as incapacitated.

### 2.5.4. Data import to the unified automated information and analytical system of CEC

Resolution of the CEC dated August 12, 2022 No. 90 (including taking into account the planned changes) "On some issues of submitting financial reports provided for by the Election Code of Ukraine on the receipt and use of money from election funds of political parties, their local organizations, candidates in national and local elections" requires separately agreeing with the Central Election Commission on the requirements for the format and structure of open data, which will be uploaded to the Unified Automated Information and Analytical System of the Central Election Commission using API.

In case of approval of CEC access exclusively to depersonalized reports of political parties and managers of EFA/RFA, the development of a separate API is not required, but the functionality of SM publication of information in the public part of ICS PFP will be used.

In case of consenting to CEC access, including to reports that include personal data, the following options (and/or) must be implemented:

1. Create a separate user with the role of "CEC Administrator" with the possibility of open 24/7 viewing, copying and printing of information, saving electronic copies of documents outside ICS PFP, as well as in the form of a set of data (electronic document) organized in a format that allows their automated processing by electronic means (machine reading) for the purpose of reuse.
2. Separately agree with the Central Election Commission on the requirements for the format and structure of open data that will be uploaded to the Unified Automated Information and Analytical System of the Central Election Commission using API and implement the import of information from ICS PFP.

## 2.6. Description of the parameters of SM publication of information in the public part of ICS PFP

The public part of the ICS PFP provides convenient access to users (voters, members of the public and media) without registering with the role of "Visitor" to published depersonalized reports of political parties and EFA/RFA managers.

The public part of the ICS PFP should provide for the automatic publication of depersonalized reports after submission, including providing:

- search for the report using a filter by party, period, region, EDRPOU code, full name of the candidate for deputies;
- display and export of reports (separate from each office and a consolidated report collected from all separate) in the format of an electronic document (spreadsheet and/or PDF);
- export of reports in the format of machine-readable data (json and/or CSV).
- basic visualization, statistics and analytics;
- display of uploaded depersonalized photocopies of the conclusion in the link to the reports;
- simple end-to-end search among the contents of reports, including search for transactions by name and public part of the address of a natural person, name or code of legal entities, filter by dates and amounts of transactions;
- review of informational materials;
- availability of instructions for working with data (examples of API use, detailed description of data formats), links to regulatory documentation and other informational materials.

The public part of the ICS PFP must not have access to the private part of the ICS.

## 2.7. Description of the parameters of SM e-monitoring

***Purpose***

SM e-monitoring ICS PFP should automatically exchange information with the external ICS "Media Monitoring System", which implements extensive media monitoring using elements of artificial intelligence.

Only authorized NACP employees will have access to work with this e-monitoring SM, who will monitor the information space (online media, social networks, etc.) for the performance of the functional tasks of the NACP Political Corruption Prevention Department.

***Characteristics of the data***

To determine the amount of information planned for exchange between the specified ICS, the key principles of the ICS "Media Monitoring System" will be taken into account:

- flexibility and the possibility of further development and adaptation to the new tasks of NACP and the changing landscape of the media space;
- interoperability for interaction with the Agency's existing and planned analytical products (ERP case management system, Data mining/Data Warehouse, etc.);
- high automation of routine tasks of analysis and categorization of texts and photos using artificial intelligence.

***SM e-monitoring should provide for the following technical features:***

- export of information from ICS PFP to ICS "System of media monitoring" in the amount necessary to set up operational monitoring of the activities of political parties and candidates, including during elections and referenda, to identify expenses that must be indicated in the relevant financial reports: names

of political parties, names of candidates for deputies, etc.;
- import of information from the ICS "System of media monitoring" to the ICS PFP (or provision of dynamic transition via the link) in the scope of the results of operational monitoring of the activities of political parties and candidates;
- creation, editing, activation/deactivation of the rules of receipt and storage for further processing of information necessary for operational monitoring of the activities of political parties and candidates.

## 3. MAIN PARAMETERS OF OTHER SM

### 3.1. Description of the parameters of SM Security Administrator ICS PFP

SM Security Administrator ICS PFP is a specialized module that occupies a special place in the structure of ICS PFP:

- the functionality of the module extends to the entire ICS PFP as a whole;
- functionality does not depend on the logic and features of business processes that are subject to automation.

SM Security Administrator ICS PFP has access to the ICS PFP administration and configuration subsystem without access to report data and implements the following functionality:

- management of ICS PFP system settings;
- control and management of the general state of ICS PFP functioning, including the occurrence of incidents related to information security;
- control over formation, maintenance and creation of backup copies of ICS PFP;
- configuration management of access to external registers and APM-NBU-information;
- viewing activity logs of registered users (both political parties and managers, and analysts and analysts' heads) and exporting them for further analysis;
- organization of demarcation of access to ICS PFP resources;
- ensuring the organization and implementation of modernization, testing, operational restoration of ICS PFP functioning;
- management (creation, deactivation, activation, change of contact data and passwords) of accounts of managers, external users, analysts and heads of analysts.

### 3.2. Description of the parameters SM Workstation of NACP administrator

SM Workstation of NACP administrator is a module whose functionality depends on the logic and features of the business processes to be automated.

SM Workstation of NACP administrator has access to the administration subsystem (within the scope of authority granted in the ICS PFP Security Administrator's SM) and configuration and has access to report data.

SM Workstation of NACP administrator implements the following functionality:

- managing basic settings of all SS (for example, specify deadlines for submission of reports, etc.);
- viewing activity logs of registered users (political parties and managers) and their export;
- management (activation/deactivation of party offices or individual accounts in these offices) of political party office accounts;
- manage (create, deactivate, activate, change contact data and passwords) manager accounts (within the agreed logic and features of business processes to be automated);

- authorization of requests to replace QES keys of political parties' accounts;
- setting up and administering the existing SS business functionality;
- creation of process configuration (takes place according to the basic rules of BPMN);
- management of ICS PFP directories.

### 3.3. Description of the parameters of SM Workstation of the responsible employee

SM Workstation of the responsible employee is a module whose functionality depends on the logic and features of the business processes to be automated.

The responsible employee can be a person of an external organization who has the appropriate authority to access (exclusively information viewing mode) via the Internet to the closed part of ICS PFP.

External user registration in ICS PFP is performed by the ICS PFP security administrator.

The responsible user has the right to:

- use ICS PFP around the clock and free of charge, having access to information (data) contained in its closed part;
- view, copy and print information posted in the closed part of ICS PFP;
- search, review and save electronic copies of documents and receive from ICS PFP data sets organized in a format that allows them to be automatically processed by electronic means (machine reading) for the purpose of reuse.

The responsible user shall:

- comply with the established procedure for using ICS PFP;
- not to use ICS PFP, as well as the information (data) obtained in its closed part, to commit illegal acts.

### 3.4. Description of the parameters of SM Workstation of the CEC administrator

SM Workstation of the CEC administrator is a module whose functionality depends on the logic and features of the business processes to be automated.

SM Workstation of the CEC administrator has access to the administration subsystem (within the scope of authority granted in the ICS PFP Security Administrator's SM) and settings without access to report data.

CEC Administrator registration in ICS PFP is performed by the ICS PFP Security Administrator.

SM Workstation of the CEC administrator implements the following functionality:

- management (activation/deactivation of CEC/TEC/DEC cabinets or individual accounts in these cabinets) accounts of CEC/TEC/DEC cabinets;
- manage (create, deactivation, activation, change contact data and passwords) accounts of responsible CEC/TEC/DEC employees (within the agreed logic and features of business processes to be automated);
- management of CEC/TEC/DEC directories.

### 3.5. Description of the parameters of SM Workstation of the responsible employee of the CEC/TEC/DEC

SM Workstation of the responsible employee of the CEC/TEC/DEC is a module, the functionality of which depends on the logic and features of the business processes to be automated.

The responsible CEC employee can be a CEC person who has the appropriate authority to access (exclusively information viewing mode) via the Internet to the closed part of the ICS PFP.

The responsible employee of the TEC/DEC can be a person of the TEC/DEC who has the appropriate authority to access (exclusively the mode of viewing information and exclusively within the limits of a specific TEC/DEC) via the Internet to the closed part of the ICS PFP.

Registration of the responsible employee of the CEC/TEC/DEC in the ICS PFP is performed by the CEC administrator.

The responsible user of CEC/TEC/DEC has the right to:

- use ICS PFP around the clock and free of charge, having access to information (data) contained in its closed part;
- view, copy and print information posted in the closed part of ICS PFP;
- search, review and save electronic copies of documents and receive from ICS PFP data sets organized in a format that allows them to be automatically processed by electronic means (machine reading) for the purpose of reuse.

The responsible user shall:

- comply with the established procedure for using ICS PFP;
- not to use ICS PFP, as well as the information (data) obtained in its closed part, to commit illegal acts.