Estimation of the protection of information
(type of services the provision of which is subject to licencing)

Complex diagnostics of information systems of the Verkhovna Rada Secretariat

(technical specifications)

1. Goal and scope of diagnostics of information systems:

Definition of the list and analysis of existing information systems, processes of their use. Construction of schemes of interaction of information systems, identification of problem and bottlenecks of their operation, including in terms of information security.

2. Outcome expected by the customer:

Reports and series of presentations that will provide answers to the questions about the list of available information systems, processes for their management and support, schemes of interaction with information systems, the extent of their implementation and impact on existing administrative processes, existing risks and bottlenecks both at the moment of diagnostics and in the medium term, possible ways of addressing the identified problems and further development in the medium term, solving other issues listed in these technical specifications and Terms of Reference that will be agreed between the customer and the contractor in preparation for diagnostics.

3. Key studies and recommendations to be documented on the results of the project:

Efficiency of the use of existing information systems, including those already procured but not implemented or partially implemented. Existing risks and bottlenecks identified at operation (including information security status of these systems), their impact on administrative processes.

4. Initial data for diagnostics:

Information provided by the customer, public procurement reports in ProZorro system, access to customer information systems to be diagnosed. Number of main data centres is 1, reserve data centres – 1, number of detached units – up to 5, number of workplaces – up to 1,900 (1,000 – employees of the Secretariat, 900 – MPs and their assistants), workplaces are diagnosed selectively. Number of key information systems – up to 15, number of key databases – up to 10.

5. Requirements for the report to be produced based on diagnostics:

The reports should include both fully detailed research summaries with recommendations and smaller summary presentations with links between them that will help drill down.

The recommendations provided should take into account the requirements and limitations of the current legislation in the field of ensuring the operation of information systems in public authorities and the requirements for the protection of information in information and telecommunication systems.

The report shall be submitted in hard copy and in electronic form. The specific composition of the reporting documents and other technical, organizational and methodological documents to be produced during the provision of services will be determined when preparing the Terms of Reference.

6. Stages of service provision

Start in March 2020. The number of service delivery stages will be determined when preparing the Terms of Reference.

7. Requirements to services, expected results and procedure of implementation:

Prior to commencement of works, the contractor should on the basis of these technical specifications and consultations with the customer develop the Terms of Reference for the provision of services. The Terms of Reference should include a complete list of the stages of the work, as well as the goal, objectives and detailed tasks for each stage. Please, see section 8 of these technical specifications for examples. The Terms of Reference are subject to mandatory approval by the customer prior to commencement of work. After the commencement of the works, changes and adjustments to the Terms of Reference, which do not contradict these specifications can be made upon approval by both parties.

Diagnostics and analysis are expected to include:

1. Diagnostics of data centres and technical infrastructure
2. Diagnostics of equipment
3. Software diagnostics
4. Analysis of continuity of service provision
5. Assessment of information security status
6. Analysis of implementation of the e-Parliamentary Strategy for 2018-2020
7. Analysis of costs for information systems support

7.1 Diagnostics of data centres and technical infrastructure

- Analysis of current technical infrastructure management processes;
- Analysis and documentation of the scheme of existing data centres and communications between them;
- Analysis and documentation of high-level communication scheme between locations;

- Surveying the availability of the necessary uninterruptible power supply, cooling systems, fire safety, etc.

Diagnostics should show a high-level diagram of all components (including isolated components) of the information systems infrastructure, identify the bottlenecks and problems, and provide recommendations for their correction.

7.2 Diagnostics of hardware

7.2.1. Analysis of workplaces and computer hardware

- Analysis of current accounting and management processes for workplace equipment;
- Selective workplace, computer, and peripheral hardware diagnostics.

Diagnostics should investigate current workplace equipment management processes, show the total volume of workplace computer equipment available at the workplaces, its current condition, obsolescence, and the need for updating, study warranty and post-warranty service available, and identify risks in the operation of existing equipment and ways to address them.

7.2.2. Diagnostics of server (including network) hardware

- Analysis of current accounting and hardware management processes;
- Collection of information on available server and network equipment (functions, availability of support, obsolescence);
- Analysis of the conformity of the available equipment to the procurement made in the last three years.

Diagnostics should investigate existing accounting and management processes for hardware, show the current condition of server and network hardware, hardware obsolescence, load, and available resources (as of the time of the audit and mid-term forecast), bottlenecks that do not allow make full use of the potential of existing equipment, study warranty and post-warranty service available, identify operational risks and how to address them.

7.3. Diagnostics of hardware

7.3.1. Diagnostics of workplace software

- Analysis of current record and management processes for workplace software;
- Analysis of current record and license management processes for system (operating systems) and client (office, applications) workplace software;
- Analysis of software distribution processes and policies;

- Selective testing of software for licenses and use rights.

Diagnostics should investigate current record and management processes for workplace software, check for licenses, their obsolescence, and regular updates, including the availability and regularity of antivirus updates, identify problems and bottlenecks in the operation of existing software, the need for its updating or replacing.

7.3.2. Diagnostics of system server software (including virtual resource management and database management systems)

- Analysis of current processes for record and management of system server software;
- Analysis of workload monitoring and load management processes;
- Collecting information on existing system software (operating systems, virtualization systems, database management systems, monitoring systems, etc.);
- Hardware resource efficiency review (availability of all resources for virtualization system, operating systems, lack of license restrictions, etc.);
- Identification of the most resource-intensive components and exploration of load redistribution (if necessary);
- Checking the software for licenses, use rights, availability of support;
- Analysis of the conformity of the use of system software to the procurement done in the last three years.

Diagnostics should examine existing system server software management processes, check for limitations on the effective use of system software, and its compliance with existing hardware resources, analyse availability and validity of licenses for the right to use the software and availability of support, the extent of use of available resources (as of the time of diagnosis, and the mid-term forecast), determine problems and bottlenecks in the operation of existing system software, the need for its updating or replacing.

7.3.3. Diagnostics of information systems (application software)

- Analysis of current processes of record and management of information systems;
- Analysis and documentation of current information systems (including application software necessary for their functioning);
- Interviews with executives and staff involved in administrative processes, determining the degree of automation of administrative processes, and the most critical bottlenecks;
- Analysis of the need for automation of other administrative processes;
- Checking the implementation of current information systems (in test or industrial operation);
- Checking the availability of the necessary licenses and rights to use the information systems (including exclusive or non-exclusive rights, which software are subject to licensing and other restrictions on use);
- Analysis of the number of users who use information systems (planned and actual);

- Analysis of availability of necessary hardware (virtual hardware) resources necessary for the operation of information systems;
- Documentation of the architecture of interaction between information systems, detailing the internal interaction between IS components (modules);
- Analysis of the relevance of the use of application software to the procurement list in the last three years.

Diagnostics should investigate the current processes of record and management of information systems, show a list of available information systems (including application software necessary for the operation of these systems), analyse availability and validity of licenses, availability of support, identify and available resources (as of the time of the audit and mid-term forecast), problems and bottlenecks in the operation of existing software, the need for its updating or replacing.

7.3.4. Analysis of opportunities for development and updating of information systems

- Analysis of current processes for the development and refinement of information systems;
- Analysis of current information systems in terms of opportunities for further improvement and change;
- Checking the availability of raw codes of information systems;
- Checking the availability of development and testing tools: version control systems, bug-tracking systems, test environment, etc.;
- Verification of licenses, proprietary and non-proprietary rights for modification and further operation of modified versions of information systems;
- Exploring regulations for modifying, testing and updating information systems in a productive environment;
- Review of other (including technical) restrictions that make it difficult or impossible to further develop and improve information systems according to the needs of the operator.

The analysis should examine current processes for refining and development of information systems, identify limitations on the further development of information systems both from a technical point of view and from the side of licensing restrictions, and suggest ways to address these limitations.

7.4. Analysis of continuity of service provision

7.4.1. Business Impact Analysis (BIA) and analysis of compliance with current requirements to error tolerance (RTO, RPO)

- Conducting Business Impact Analysis, including determining the requirements for recovery time objective (RTO) and recovery point objective (RPO) for each key information system;
- Analysis of existing monitoring systems and notification of refusals to provide services;
- Analysis of common performance bottlenecks for 2 or more services;
- Identification of common failure points for 2 or more services;
- Forecast of threat of failure to provide services or loss of data upon failure of individual equipment.

The analysis should examine the adequacy of the expected and actual RTO and RPO indicators, identify bottlenecks and most risky locations from the point of view of continuity of service provision, verify the performance of monitoring systems and incident response regulations, and provide recommendations on how to resolve the identified issues.

7.4.2. Analysis of IT incident management and user feedback processing

- Analysis of incident response processes and service denials;
- Checking the availability of regulations and tools for fixing IT incidents (including cyber threats) and user complaints;
- Analysis of significant incidents (including cyber threats) that have occurred in the past and their consequences (over the previous three years).
- Analysis of the most common user feedback regarding IT services.

The analysis should check the availability and effectiveness of incident response regulations, and provide recommendations for resolving the identified issues.

7.4.3. Analysis of information systems backup policies

- Checking backup and recovery rules;
- Checking the results of the periodic backup test;
- Selective verification of the availability of critical services backups;
- Checking the storage regulations for backup media

The analysis should check the effectiveness of the data backup rules, make sure that the data recovery from backup procedures are periodically tested.

7.5. Assessment of information security status

- Checking the compliance of existing information systems with the requirements of effective legislation in the field of information protection;

- For information systems with a certificate of conformity, checking availability of necessary technical documents and regulations, making sure that responsible persons know these regulations;
- For information systems that do not have the certificate of conformity, carrying out the following checks (the list can be updated in the Terms of Reference):
    - Analysis of the adopted processes of information security management;
    - Checking the availability of information security requirements in the technical requirements and terms of reference for the development of each information system;
    - Checking the list of persons with physical and logical access to information systems (documentation of issuance, updating, and revocation of access rights);
    - Checking of existing secure domain policies on servers;
    - Checking domain policies on workstations (optional);
    - Checking for updating and antivirus policies;
    - Checking the requirements for network screens;
    - Checking of notification process when a virus or other threat is detected;
    - Checking the requirements for logging events;
    - Checking the list of services that can be accesses externally;
    - Checking the procedure for granting external access to services;
    - Checking the control over external access to services;
    - Review of privileged access management processes;
    - Checking policies for setting and changing passwords;
    - Checking the annual revision of user rights.
- Checking the availability of regulations and security systems.

Diagnostics should verify compliance of information security regulations and policies with the requirements of effective legislation and the requirements of information security management systems.

7.6. Analysis of implementation of the e-Parliament Strategy for 2018-2020

- Analysis of the implementation of the Strategy implementation plan (Annex 1 to the Strategy);
- Analysis of the implementation of the priority projects of the Strategy (Annex 2 to the Strategy);
- Analysis of the degree to which the information systems and their modules specified in the Strategy are put into industrial operation (including the analysis of the planned and actual number of users of systems);
- Analysis of compliance of technical conditions, terms of reference and related technical documents on information systems with the requirements specified in the Strategy;

- Analysis of the compliance of the implemented (and actually used) functional information systems of description and requirements specified in the terms of reference for the information system;
- Analysis of the readiness of information systems under development;
- Analysis of status of information systems that are tested.

The analysis should show the implementation of the e-Parliament Strategy, the effectiveness of use of already implemented information systems and their impact on administrative processes, identify bottlenecks in the operation of information systems already in place and obstacles in the implementation of commercially available but not used systems (in particular, those that are under testing), and provide recommendations for resolving issues that were identified.

7.7. Cost analysis of information systems support

- Analysis of regular (operational) costs for IT infrastructure support (except for payroll);
- Analysis of the regular costs required to support information systems (except for payroll).

The analysis should show the share of costs for supporting each of the information systems and IT infrastructure as a whole, to identify the most resource-intensive spots, and suggest ways to optimize costs.

8. Methods and stages of the works (*sample project for the development of ToR, the number and sequence of stages is determined by the contractor*)

8.1. Collecting information on the current status of IT systems

Goals of this stage are to:

- get information and understanding of the overall current IT architecture;
- identify the software and hardware used by the departments, its location;
- get information and understanding of the organization of the data centres, communication channels between them;
- identify the standard equipment used by the departments.

Key objectives of this stage:

1. Conduct working sessions and interviews;
2. Analyse documents (policies, regulations, schemes, diagrams, etc.)

Objective 1. Conduct working sessions and interviews:

- to gain understanding of IT architecture;
- to determine what software and hardware is used by the departments;
- to gain an understanding of how data centres work, the channels of communication between them;
- to collect information on existing equipment used for the operation of key IT systems of the departments, including the use of specialized software, in the presence of the staff employees.

Objective 2. Analyse documents (policies, regulations, schemes, diagrams, etc.):

- to gain understanding of the overall current IT architecture with identification of software and hardware used by the departments, their location, organization of data centres, communication channels between them;
- to build a detailed diagram of the network topology, indicating the location of server and network equipment, communication channels, etc.;
- to determine requirements for ensuring the stability and reliability of information systems and data storage.

Presentation of the results of this stage, including:

- conducting workshops to discuss the results of assessment of existing information systems with functional requirements within the framework of the Secretariat's strategy objectives and respective recommendations;
- approval of the final report.

Results of every stage of study/analysis should be presented.

9. List of information systems to be diagnosed

9.1. List of priority information systems:

- Software and technical complex "Electronic voting and counting system "Rada-3"
- Intranet portal of the Verkhovna Rada of Ukraine:
  - Automated system (AS) "Automated Document Management System of the Verkhovna Rada of Ukraine"
  - AS "Electronic Draft Law"
  - AS "Electronic Personal Dashboard of the Member of Parliament of Ukraine, an employee of the Secretariat of the Verkhovna Rada of Ukraine"
  - AS "Monitoring the Passage of Draft Laws"
  - AS "Unified system for accounting and control of requests for information"
  - AS "Requests of MPs, Instructions of the Verkhovna Rada of Ukraine"
  - AS "Automated workplace "Appeals of MPs"
  - AS "Electronic Conciliation Council"
  - AS "Electronic Committee"
  - AS "Electronic Meeting Hall of the Committee and Factions"
  - AS "Electronic meeting of the Verkhovna Rada Committee"
  - AS "Electronic Petitions"
  - AS "Citizens' Requests"
  - AS "Requests for Information"
  - System of electronic interaction between the subjects of the legislative initiative: the MPs of Ukraine, the Cabinet of Ministers of Ukraine and the President of Ukraine.

9.2. List of public web-resources of the Verkhovna Rada of Ukraine:

- Official public web portal of the Verkhovna Rada of Ukraine
- Website of the Chairperson of The Verkhovna Rada of Ukraine;
- Websites of the Verkhovna Rada Committees (28);
- Websites of departments of the Secretariat of the Verkhovna Rada of Ukraine (6);
- The Verkhovna Rada of Ukraine's open data portal;
- Web-portal of electronic petitions of the Verkhovna Rada of Ukraine;
- Web-portal of public discussion of draft laws of the Verkhovna Rada of Ukraine
- Web-portal "Citizen's Electronic Dashboard"

9.3. List of information systems (including to be created in future) stipulated by the e-Parliament Strategy for 2018-2020:

- AS "Electronic voting and vote counting of new generation"
- Information automated system "Electronic Plenary Meeting Hall"
- Mobile workplace (tablet) of the MPs of Ukraine;

- System of automation of shorthand/record of committee meetings and plenary sessions of the Verkhovna Rada of Ukraine;
- Ukrainian version of Eurovoc thesaurus;
- Technological database of regulatory legal information "Legislation"
- Modernized official website of the Verkhovna Rada of Ukraine (with the introduction of adaptive web design and support of modern types of screens)
- Website of digital representation of the MP of Ukraine for communication with voters and reporting of the MPs of Ukraine;
- Automated system of publishing open data of the Verkhovna Rada of Ukraine in structured (machine-readable) formats.

9.4. List of internal information systems of the Verkhovna Rada Secretariat:

- AS to register all types of information produced in the VRU Secretariat
- AS "Passage of draft laws in structural departments of the Secretariat"
- AS "Electronic agenda of plenary a meeting"
- AS "Law-maker"
- AS "Letters and requests of citizens"
- AS "Electronic requests of citizens"
- AS "Automatization of the activities of the Department of Inter-Parliamentary Relations"
- IS "Electronic library and archives of the Verkhovna Rada of Ukraine"
- AS "Legislation"
- AS "Staff"
- AS "Entrance permits of the VRU"
- AS "Record of periodicals and publications for the MPs"
- AS "Foreign passports"
- AS "International business trips"
- AS "Computer hardware and software"
- System of registration and record of the words of the Department of Computerized Systems of the VRU Secretariat
- System of tender and contractual works
- E-mail server of the VRU, mailboxes of the MPs and employees of the Secretariat
- AS "Requests to visit open plenary meetings"
- Software for maintaining the record of funding and consolidation of reporting
- IS "UFD Library"
- AS "Recordkeeping"
- AS on Accounting
- Phone directory
- Directories of local self-government
- Software and technical complex "Archives"

10. Indicative list of procurement from ProZorro public portal:

- UA-2018-08-21-002591-c Development of an automated system “Electronic Draft Law” of the Verkhovna Rada of Ukraine
- UA-2018-08-29-001564-a Software for the Verkhovna Rada of Ukraine Automated System “Electronic Draft Law”
- UA-2017-10-03-002911-b Services on updating the electronic document flow system
- UA-2018-08-23-000956-a Update of software and continued technical support for the VmWare vSphere data centre virtualization centre
- UA-2019-08-12-001381-a Main data centre server equipment
- UA-2017-11-30-001927-c Services for the provision of backup software for data centres
- UA-2018-11-15-003524-a Procurement of software modules with installation for structuring and design of the official website of the Verkhovna Rada of Ukraine
- UA-2017-11-16-003631-a Services on development of the Intranet portal of electronic document flow of the Verkhovna Rada of Ukraine
- UA-2017-11-16-003667-a Services on development of software for management of resources, libraries and web-applications of electronic document flow of the Verkhovna Rada of Ukraine
- UA-2017-11-02-001549-a Software development services.