REQUEST FOR EXPRESSIONS OF INTEREST
(REoI# MF-IC-14)
(CONSULTING SERVICES – INDIVIDUAL CONSULTANT)

UKRAINE

STRENGTHENING PUBLIC RESOURCE MANAGEMENT PROJECT, PART B: SUPPORT TO PFM STRATEGY IMPLEMENTATION (PROJECT NUMBER P161586)

Grant No. TF0A5324

Assignment Title: Information Cybersecurity Consultant - Documentary Support

Reference No. MF-IC-14

The Government of Ukraine has received financing from the World Bank acting as administrator of the grant funds provided by the European Commission on behalf of the European Union under the EC - World Bank Partnership Program for Europe and Central Asia Trust Fund (EU Programme for the Reform of Public Administration and Finances (EURoPAF) toward the cost of the Strengthening Public Resource Management Project, and intends to apply part of the proceeds for consulting services.

The Ministry of Finance of Ukraine ("MoF") is responsible for the implementation of Part B of the Project and, to strengthen its capacity with regard to Project implementation, involves through competition an individual consultant - Information Cybersecurity Consultant - Documentary Support (hereinafter – the Consultant) for conduction of organizational and technical activities on development and implementation of a comprehensive information protection system within the information and telecommunication system of MoF.

The consulting services ("the Services") include support to MoF in frames of the stages of the process of development and creation of a comprehensive information protection system ("CIPS") of the MoF Information and telecommunication system ("ITS") on the following:

1) Conduction of pre-project study of the MoF ITS operational environment;
2) Design of MoF ITS CIPS in the part of developing the technical project documentation;
3) CIPS preparation for commissioning (does not include the state expertise examination).

The Services are to be rendered at Consultant`s place of residence.
The Consultant is expected to work throughout the period from November 2020 to March 2021. The expected working time spent generally shall not exceed 120 working days.

More detailed information is stipulated in the ToR which is attached.

The MoF now invites eligible individual international consultants – physical persons ("Candidates") to indicate their interest in providing the Services in the form of CV (in Ukrainian or English). Interested candidates should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services.

The candidates shall provide confirmation in the form of references to publicly confirmed and accessible information, or provide copies of relevant documents confirming the respective status or condition.
Interested Candidates are invited to submit any supplementary documents to evidence that Candidate meets with the qualification criteria for the position of the Consultant.

Mandatory qualification of the Consultant:

- higher technical education;
- at least 5 years of experience in the field of information protection, of which at least 2 years in the course of the last 5 years;
- availability of a qualification improvement certificate in technical and cryptographic protection of information, at least one certificate per each of the fields;
- experience in building up CIPS and preparation of documents for conduction of state expertises in the field of information technical protection within the last 5 years, with at least 3 implemented contracts/projects;
- knowledge and skills on practical application of the main Microsoft services, network services (DNS, DHCP, VLAN, VPN);
- experience of work with means of network security;
- fluent speaking and writing in Ukrainian.

The attention of interested Candidates is especially drawn to additional Consultants qualification requirements corresponding to the peculiarities of the assignment, meeting them would be an advantage:

- availability of a certificate of CISSP (Certified Information Systems Security Professional) or CISA (Certified Information Systems Audit) or CISM (Certified Information Systems Manager)
- availability of a certificate on successful completion of the training / training course on implementation and usage of the requirements of ISO / IEC 27001:2013 "Information Technology. Security Techniques. Information Security Management Techniques. Requirements" according to field of training "Implementor" and/or "Auditor";
- experience in implementation of comprehensive systems of protection of various types of information (AC1, AC2, AC3);
- availability of a scientific degree in technical sciences;
- availability of author patents for developments in information technical protection and comprehensive information protection;
- availability of a license from the State Service of Special Communication and Information Protection of Ukraine for performance of economic activity on rendering services in information technical protection;
- experience in CIPS build-up and preparation of documents for holding state expertises in information technical protection for public sector organizations;
- knowledge of English on a sufficient level for working through IT technical documentation without a dictionary.

The attention of interested Candidates is drawn to Section III, paragraphs, 3.14,3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers", July 1, 2016 with revisions as of

November 2017 and August 2018"("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

A Consultant will be selected in accordance with the Selection of Individual Consultants method (IC) set out in the Procurement Regulations.

Interested Candidates may obtain further information at the address below during office hours: 10:00 to 18:00.
Contact person: Volodymyr Vorotyuk
Tel: +38 044 206 5773, 380 50 4100340
E-mail: vorotyuk@outlook.com

Expressions of interest must be delivered by mail, fax or e-mail to the address below by 5 pm on November 4, 2020.

For EoIs submission:
Ministry of Finance of Ukraine
Attn: Mr. Igor Shevliakov, Head, Expert Group for EU Integration, Directorate for Strategic Planning and European Integration
The letter subject is – "Expression of interest on - MF-IC-14, Information Cybersecurity Consultant - Documentary Support"
E-mail: shevliakov@minfin.gov.ua mandatory copy to: vorotyuk@outlook.com.

Attachment to REoI # MF-IC-14

TERMS OF REFERENCE

for provision of consulting services:

Information Cybersecurity Consultant - Documentary Support

(Individual consultant)

Contract reference No.: MF-IC-14

1. BACKGROUND INFORMATION

The Government of Ukraine has received financial assistance from the International Bank for Reconstruction and Development ("World Bank"), acting as administrator of the grant provided by the European Commission on behalf of the European Union ("Donor") under the EC-World Bank Partnership Program for Europe and Central Asia Programmatic Single-Donor Trust Fund (EU Programme for the Reform of Public Administration and Finances (EURoPAF) three million thirty thousand six hundred sixty-one Euros (EUR 3,030,661) ("Grant") to implement the Strengthening Public Resource Management Project ("Project"). This Project consists of two parts: Part A "Strengthening Human Resource Management in Public Administration Institutions"; and Part B "Support to PFM Strategy Implementation".

Part B of the Project, total amount of which is one million one hundred ten thousand six hundred eighteen Euros (EUR 1,110,618), supports the activities aimed at implementing the PFM Strategy for 2017-2020 and identifies future investments in ICT for PFM through carrying out the audit of ICT; modernization of existing ICT equipment for business continuity at the Ministry of Finance of Ukraine ("MoF"); and strengthening ICT system capabilities, etc.

To achieve the objective, one of the main tasks of the PFM Strategy is wide application of reliable IT solutions and automation of the existing processes in the field of public finance management with the purpose of minimization of human impact and related corruption challenges.

MoF is responsible for implementation of Part B of the Project and, to strengthen its capacity with regard to Project implementation, involves through competition an individual consultant - Information Cybersecurity Consultant - Documentary Support (hereinafter – the Consultant) for conduction of organizational and technical activities on development and implementation of a comprehensive information protection system within the information and telecommunication system of MoF.

2. PROBLEM DESCRIPTION

Currently in Ukraine each state body and company must ensure maximum automation of their life processes, prompt interaction and information exchange in the course of managerial decision making.

Dependence of organization on information systems, which ensure its life processes, is causing serious risks with regard to protection of information resources processed by means of such information systems. Failure of such an information system or unauthorized interference into its operation may lead to disastrous consequences for both the organization and the country on the

whole. That is why, simultaneously with implementation of information systems ("IS"), large attention is drawn to their security, fault tolerance, and protection of information, which circulates within the systems.

The information and telecommunication system of MoF ("ITS") constitutes a service-oriented hardware and software platform for implementation and fulfillment of typified applied information services, which are implemented based on a common hardware and software platform, support a common information processing technology, and ensure mechanisms for implementation of the provisions of the uniform security policy approved by MoF.

The ITS hardware and software platform implements the strategy of a common integration system, which comprises technologies and hardware enabling to sustain a functionally closed and self-sufficient data processing system in frames of created (implemented) applied services (automated systems), with support of specified fixed (for all ITSs) types of objects of protection, access subjects (user groups and roles), and basic operation conditions.

Under Article 6 of the Law of Ukraine "On Access to Public Information" and Article 21 of the Law of Ukraine "On Information", requirements are raised to information processed by means of information systems of the state bodies and stored in state registers, with regard to ensuring its confidentiality, integrity, and accessibility in the course of its processing.

Thus, to ensure the ITS security policy in compliance with the requirements of the current legislation of Ukraine and to exclude or minimize losses caused by unauthorized access to information resources, a comprehensive information protection system (hereinafter – the CIFS) shall be created, with confirmed compliance in accordance with Article 8 of the Law of Ukraine "On Information Protection in Information and Telecommunication Systems". Compliance shall be confirmed based on the results of the state expertise in the procedure set by the legislation.

On the whole, the comprehensive information protection system ("CIPS") can be defined as a set of organizational and engineering and technical measures, legal and legislative norms, as well as physical and hardware and software means of information protection. The need to apply the CIPS is set by the legislation of Ukraine, and the procedure of their creation is determined by the Administration of the State Service of Special Communication and Information Protection of Ukraine.

In the course of development and management of the ITS CIPS, an integrated approach shall be applied to implementation of the ITS architecture on all presented levels, which envisages:

- Implementation of a uniform information protection policy, which shall be confirmed with the compliance certificate for the ITS CIPS and development of rules and procedures for growth of functionalities and hardware and software in the course of scaling and upgrade of ITS infrastructure and computing resources;
- Shortening of the periods for implementation of additional information systems (functional services) and increase of the number of automated workstations of service users through application of typical design solutions for ensuring security services and approval by the Administration of the State Service of Special Communication and Information Protection of Ukraine of the procedures for their implementation (set of protection mechanisms of the implemented service (automated workstations) is included into the ITS security management system);

- Possibility of dynamic growth of ITS computing capacities and users' environment without the need for an additional/repeated expertise;
- Reduction of system support due to avoidance of duplication of typical documents (models, designs, manuals, codes etc.) and security organizational and technical activities (audit, update etc.).
- Reduction of costs connected with holding additional expertises.

The ITS CIPS shall be developed in accordance with the typical procedure of CIPS creation in automated systems (ND TZI 3.7-003-05), with account of the integrated approach to implementation of the components of its architecture.

The objective of creation of the ITS comprehensive information protection system is to ensure protection of information processed by means of the ITS, through prevention of and combating unauthorized access, disclosure, distortion, and loss of information during its processing and transmission. Information protection shall be ensured on all technological stages of its processing and in all functioning modes of ITS components. The CIPS is an integral part of the ITS.

The CIPS is a set of software and technical means as well as organizational activities, aimed at ensuring the established level of information protection in accordance with the conditions of ITS operation environments and requirements to ensuring the main security characteristics defined in the security policy of the System and the administrator organization. The ITS CIPS is designed for implementation of the information protection policy provisions with regard to:

- identification and authentication of System users during access to and usage of protected objects;
- management of authorized users and division of powers on usage of ITS information and software resources;
- ensuring confidentiality and integrity of information circulating within the ITS and/or transmitted between its components;
- ensuring identification and authentication of ITS units during an interaction session;
- ensuring confidentiality and integrity of information provided to external users/systems;
- ensuring identification and authentication of external systems' units during an interaction session;
- ensuring confidentiality, integrity, and accessibility of technological information on system functioning;
- ensuring accessibility of information circulating within the ITS, for authorized users and processes;
- registration and processing of all events within the ITS, related to information security;
- monitoring of the current status of security and operability of ITS components;
- control of all security mechanisms via the relevant administration interface, which shall be accessible only to authorized staff.

3. OBJECTIVES OF THE ASSIGNMENT

The objective of the assignment is rendering services to the MoF in the development and creation of the MoF ITS CIPS, with focus on the following:

- Conduct of pre-project study of the MoF ITS operational environment;
- Design of MoF ITS CIPS in the part of developing the technical project documentation;
- CIPS preparation for commissioning (does not include the state expertise examination).

4. SCOPE OF SERVICES AND TASKS

The Consultant shall perform the following tasks according to the stages below:

4.1 At the stage of pre-project study of the MoF ITS operational environments, the Consultant shall:

4.1.1. Examine the MoF ITS operational environment (in particular, ITS computing system, information and physical environment, users' environment), determine the overall structural scheme and composition (list and composition of equipment, hardware and software, peculiarities of configuration, architecture, and topology, hardware and software means of information protection, mutual location of items etc.), types and characteristics of communication channels, peculiarities of interaction of specific components.

4.1.2. Analyze vulnerabilities of the hardware and software for implementation of ITS components, operational environments, and information processing technologies in accordance with the defined levels of architecture presentation, using generally accessible sources and program and technical documentation of developers.

4.1.3. Based on the results of the analysis, prepare the documents as per para. 1 of Section 5 of the present Terms of Reference.

4.1.4. Preparer and submit the relevant report on pre-project study and amend it, if required.

4.2 At the stage of MoF ITS CIPS design, the Consultant shall:

4.2.1 Develop the general design solutions required for implementation of the Terms of Reference requirements according to threat scenarios, solutions on the ITS CIPS structure, functioning algorithms, and conditions for usage of protection means, and determine the following within them:

- CIPS functions on the whole and those of its separate component parts;
- composition of comprehensive protection means;
- detailed diagram of CIPS components and scheme of interaction between its component parts;
- algorithms of functioning and terms of usage of protection means;
- solution on the architecture of comprehensive protection means, with account of the approved levels and system integrated components, and also mechanisms of implementation, determined by the functional profile of information security services; composition and technical requirements to CIP means.

4.2.2. Based on the results of the analysis, prepare the documents as per para. 2 of Section 5 of the present Terms of Reference.

4.2.3. Prepare and submit the relevant report on creation of the CIPS technical detailed project design documentation and incorporate amendments to it, if required.

4.3 At the state of CIPS preparation for commissioning, prepare documents, as specified in para. 3 of Section 5 of the present Terms of Reference, namely:

- Work out draft organization and administrative documents on development and implementation of ITS CIPS (orders, minutes, acts, etc.).
- Work out packages of operational documents and technological manuals as per approved design solutions on comprehensive protection means and organizational structure.
- Prepare training materials for briefing MoF ITS users with regard to compliance with the requirements of ITS CIPS (the training principle shall be interactive course with duration of not more than 4 hours).
- Conduct preliminary testing of MoF ITS CIPS and prepare the relevant report based on preliminary testing results.
- Prepare and submit the relevant report on CIPS preparation for commissioning and incorporate amendments to it, if required.

5. DELIVERABLES AND TIMING FOR THEIR PROVISION

The Consultant shall prepare and provide to MoF the following results[1]:

No.	Result	Deadline for submission *(from the date of contract signing)*
1	Report on conduction of pre-project inspection of the MoF ITS operational environments: • Threats model and breacher model for the MoF ITS DPC • Threats model and breacher model for the MoF ITS OTMS • Threats model and breacher model for the SAS • Threats model and breacher model for automated workstations • Regulation on ITS Information Protection Service; • Report and draft act of examination of ITS operational environments; • Information Security Policy;	Within 90 working days
2	Report on preparation of MoF ITS CIPS technical project, including: a. Design documentation of CIPS technical detailed project:	Within 100 working days

[1] The mix of deliverables and the timing of fulfillment of the assignment may be precised during the contractual negotiations with the Consultant, as per the proposed methodology of services rendering.

	• Description of the set of technical means for ensuring information protection of the MoF ITS the CS • Description of the set of cryptographic means for ensuring information protection • Code on installation of the CIPS means and generation of the basic parameters of the MoF ITS DPC security policy components • Code on installation of the CIPS means and generation of the basic parameters of the MoF ITS OTMS security policy components 1) Technical design text description. 2) Project of separate technical solutions of CIPS local user – employee of MoF. 3) Project of CIPS separate technical solutions of the automated workstation of a remote user – employee of MoF and/or subordinate structures. 4) Project of CIPS separate technical solutions of the automated workstation of a remote user – user of external information systems, which interact with ITS SAS. 5) Code on installation of comprehensive protection means and generation of the basic parameters of CIPS separate technical solutions of the automated workstation of a local user – employee of MoF. 6) Code on installation of comprehensive protection means and generation of the basic parameters of CIPS separate technical solutions of the automated workstation of a remote user – employee of MoF and/or subordinate structures. 7) Code on installation of comprehensive protection means and generation of the basic parameters of CIPS separate technical solutions of the automated workstation of a remote user – user of external information systems. b. CIPS regulatory documentation: • job description of the system administrator; • job description of the technical administrator; • ITS operation manual with regard to information protection; • procedure of upgrade of comprehensive means of protection; • procedure of management of the configuration of comprehensive means of protection;	

	• technological (operational) instructions (codes) on fulfillment of tasks on CIPS administration and maintenance: - instruction on the procedure of information reservation and recovery; - instruction on the procedure of operational recovery of functioning; - instruction on organization of control over CIPS functioning; - instruction on the procedure of ensuring anti-virus protection; instruction on the procedure of connection of automated workstations of administrators and respondents.	
3	Report on preparation of MoF ITS CIPS for commissioning: a. Documentation on CIPS tests conducted: • program and methodology of preliminary testing of CIPS in ITS; • report on preliminary testing of CIPS in ITS. b. CIPS regulatory and administrative documentation: • draft order on appointment of the Information Protection Service; • draft order on conduction of examination of the ITS operational environments; • draft order on conduction of preliminary tests and trial operation of ITS CIPS; • draft act of acceptance of ITS CIPS into trial operation; • training materials for briefing MoF ITS users in terms of observance of ITS CIPS requirements; • draft act of completion of ITS CIPS trial operation; c. CIPS supporting documentation: • log-book.	Within 110 working days

6. COORDINATION, ACCOUNTABILITY AND REPORTING

The Consultant shall work under the supervision of the Project Coordinator from the MoF and shall be accountable/report to him/her. All documents prepared by the Consultant, may further be included into the documents package, which will be approved on the level of a MoF regulatory act.

The Consultant shall coordinate his/her work with the MoF IT Coordinator in terms of development of coordinated solutions for working through and building up a conceptual model serving as basis for the Strategy of Development of Information Technologies of MoF for the

Years 2020-2022, and provide to MoF representatives output information on fulfillment of the assignment.

In the course of operational interaction, the Consultant shall be subordinated to the Lead Information Cyber Security Consultant (individual consultant) and cooperate with the MoF specialized subdivision authorized with the functions of the information protection service.

Lead Information Cyber Security Consultant (individual consultant) is entitled to:

control the timing and quality of preparation of all consultants' reports;

provide (if any) comments to the documents attached to the consultants' reports, check the fact of correcting these comments;

The Consultant shall prepare and submit to the MoF the following reports:

- Report on conduction of pre-project inspection of the MoF ITS operational environments;
- Report on preparation of MoF ITS CIPS technical project;
- Report on preparation of MoF ITS CIPS for commissioning;

1. The Consultant shall submit the Report on conduction of pre-project inspection of the MoF ITS operational environments not later than the deadline set for result No. 1 in Section 5 of the present Terms of Reference. The report is to be prepared based on the results of tasks fulfillment and shall contain the following information:
    - information on the first stage of the works performance as per the list of documents provided in para. 1 of Section 5 of the present Terms of Reference;
    - problematic issues which the Consultant considers to be obstacles for timely and quality services rendering and proposed measures on elimination of such issues;
    - general information on readiness of the whole set of documents specified in para 1 of Section 5 of the present Terms of Reference;
    - other information upon the Consultant's discretion.

The documentation prepared by the Consultant, as specified for Result No. 1 in clause 5 of the present Terms of Reference, shall be attached to the Report.

2. The Consultant shall submit the Report on preparation of MoF ITS CIPS technical detailed project not later than the deadline set for result No. 2 in Section 5 of the present Terms of Reference. The report is to be prepared based on the results of tasks fulfillment and shall contain the following information:
    - general information on the second stage of the works performance;
    - design documentation for the CIPS technical detailed project as per the list of documents specified in para 2 of Section 5 of the present Terms of Reference;
    - problematic issues which the Consultant considers to be obstacles for timely and quality services rendering and proposed measures on elimination of such issues;
    - general information on readiness of the whole set of documents specified in para 2.3 of Section 5 of the present Terms of Reference;
    - other information upon the Consultant's discretion.

The documentation prepared by the Consultant, as specified for Result No. 2 in clause 5 of the present Terms of Reference, shall be attached to the Report.

3. The Consultant shall submit the Report on MoF ITS CIPS commissioning not later than the deadline set for result No. 3 in Section 5 of the present Terms of Reference. The report is prepared based on the results of tasks fulfillment and shall contain the following information:

    - information on readiness of the set of documents specified for result No. 3 in Section 5 of the present Terms of Reference;
    - problematic issues which the Consultant considers to be obstacles for timely and quality services rendering and proposed measures on elimination of such issues;
    - other information upon the Consultant's discretion.

The documentation prepared by the Consultant, as specified for Result No. 3 in clause 5 of the present Terms of Reference, shall be attached to the Report.

4. Requirements to the reports

All reports are compiled in Ukrainian language. Any appendices to them shall be in the original language.

All reporting documents shall be submitted by the Consultant in the following manner:

- The Consultant shall submit the reporting documents in electronic form via email: _____ for review and comments by the MoF (reports shall be signed by the Consultant, scanned in pdf format and sent from Consultant`s e-mail indicated in para. 5 below). Supporting documents shall be in the MS Word, MS Excel or MS PowerPoint format or any other form previously agreed with or acceptable to the MoF, depending on the type of a document.
- If the MoF agreed reporting documents submitted via email, the Consultant shall submit them in paper form in 2 hard copies signed by the Consultant. The Paper version shall be submitted on the following address: Kyiv, 04071, Mezhegirska str., build. 11, Attn to Mr. Igor Shevliakov.

If the Consultant's report refers to information or documents prepared earlier, such documents shall be attached to such a report. The structure and form of the reporting documents specified in Section 5 of the present Terms of Reference, is determined by the requirements of regulatory documents of the information technical protection system.

5. Review and approval of the Reports

The MoF reviews the submitted reporting and approves or provides comments within 10 working days from the date of receiving the relevant report about the results of the work. The comments on the reports are set out in writing and sent to the Consultant via email: _____ with the notification of delivery of the message. The Consultant confirms the receipt of the comments and sets the deadline for their consideration within a day after receiving MoF’s comments. The Consultant shall take into account the MoF’s comments and re-submit updated report(s) MoF no later than within 5 working days from the date of their receipt to the e-mail, specified by the Consultant.

In the absence of the MoF’s comments within the specified period, such reports are considered accepted.

7. CLIENT INPUTS

MoF provides the Consultant with:
i) all the relevant documents and data not marked as restricted access or not belonging to confidential information;
ii) access to the MoF premises.

8. RESTRICTIONS

The Contract with the Consultant contains a standard conflict of interests clause. Apart from that, all materials created during performance of the services under the Contract, shall remain the property of MoF and may be used only upon the official written consent of MoF.

Prior to commencement of the services, the Consultant jointly with MoF shall prepare a confidentiality statement, where he/she shall undertake not to disclose the confidential information he/she can receive in the course of fulfillment of the assignment. The provisions of the confidentiality statement shall comply with the requirements of the current legislation of Ukraine.

9. PLACE, DURATION, WORKING CONDITIONS AND REMUNERATION

The Consultant is expected to work throughout the period from November 2020 to March 2021 The expected working time spent generally shall not exceed 120 working days. The assignment envisages the Consultant's work at his/her place of residence.
The amount of the remuneration will be determined through negotiations with the selected person and payment for the services provided will be made against reports accepted.

The Consultant is responsible for all costs incurred in connection with the provision of services, including, but not limited to the following: accommodation at the place of service, translation, communication costs, printed materials

The selection of consultant will be done in accordance with the Bank's "Procurement Regulations for IPF Borrowers", July 1, 2016 with revisions as of November 2017 and August 2018 ("Procurement Regulations").

10. QUALIFICATION REQUIREMENTS

The Consultant shall meet the following qualification requirements:
Mandatory qualification for the Consultant:

- higher technical education;
- at least 5 years of experience in the field of information protection, of which at least 2 years in the course of the last 5 years;
- availability of a qualification improvement certificate in technical and cryptographic protection of information, at least one certificate per each of the fields;
- experience in building up CIPS and preparation of documents for conduction of state expertises in the field of information technical protection within the last 5 years, with at least 3 implemented contracts/projects;

- knowledge and skills on practical application of the main Microsoft services, network services (DNS, DHCP, VLAN, VPN);
- experience of work with means of network security;
- fluent speaking and writing in Ukrainian.

Additional qualification requirements corresponding to the peculiarities of the assignment, meeting them would be an advantage

Meeting the following qualification requirements by the Consultant would be considered by the MoF *as an advantage:*

- availability of a certificate of CISSP (Certified Information Systems Security Professional) or CISA (Certified Information Systems Audit) or CISM (Certified Information Systems Manager)
- availability of a certificate on successful completion of the training / training course on implementation and usage of the requirements of ISO / IEC 27001:2013 "Information Technology. Security Techniques. Information Security Management Techniques. Requirements" according to field of training "Implementor" and/or "Auditor";
- experience in implementation of comprehensive systems of protection of various types of information (AC1, AC2, AC3);
- availability of a scientific degree in technical sciences;
- availability of author patents for developments in information technical protection and comprehensive information protection;
- availability of a license from the State Service of Special Communication and Information Protection of Ukraine for performance of economic activity on rendering services in information technical protection;
- experience in CIPS build-up and preparation of documents for holding state expertises in information technical protection for public sector organizations;
- knowledge of English on a sufficient level for working through IT technical documentation without a dictionary.

The candidates shall provide confirmation in the form of references to publicly confirmed and accessible information, or provide copies of relevant documents confirming the respective status or condition.