

Terms of Reference

Regarding

**Request for bid for auditing
the Information and Telecommunication System
of the High Anti-Corruption Court of Ukraine**

# Abbreviations

|  |  |
| --- | --- |
| DSTU | State Standard of Ukraine |
| EU | European Union |
| EUACI | European Union Anti-Corruption Initiative |
| GOST | Set of technical standards maintained by the Euro-Asian Council for Standardisation, Metrology and Certification (EASC) |
| HACC | High Anti-Corruption Court of Ukraine |
| HW | hardware |
| IT | Information Technology |
| ICT | Information and Communication Technology |
| ITS | information and telecommunication system — an organizational and technical system that implements information technology and combines a computer system, the physical environment of its location and operation, personnel (user environment), and processed information, including the technology for processing thereof |
| ITS Owner | High Anti-Corruption Court of Ukraine |
| IS | Information Security |
| KSZI | comprehensive information protection system, a set of organisational, engineering and technical measures aimed at ensuring the protection of information from disclosure, leakage, and unauthorised access |
| MFA | Ministry of Foreign Affairs of Denmark |
| ND TZI | regulatory instrument of technical information protection system |
| OS | Operating System |
| SSSCIP | Administration of the State Service of Special Communications and Information Protection of Ukraine |
| SW | software |
| TOR | Terms of Reference |
| assessment | determining the degree of compliance of the inspected item’s features with the set criteria and requirements |

# Background and context

EUACI is the comprehensive EU anti-corruption program in Ukraine financed by the EU and Denmark and implemented by the MFA of Denmark.

The work of the EUACI is streamlined through its 3 components: (1) strengthening the operational and policy-making capacities of state institutions dealing with the prevention and fight against corruption; (2) enhancing the capacity of local self-government, civil society, media, and business to contribute to the fight against corruption; and (3) increasing culture of integrity issues in Ukraine through the engagement of the business sector, the civil society and the media.

Within component 1 the EUACI is working with the National Anticorruption Bureau of Ukraine (NABU), National Agency for Corruption Prevention (NACP), Assets Recovery and Management Agency (ARMA), Special Anticorruption Prosecutor’s Office (SAPO), State Financial Monitoring Service (SFMS), High Anti-Corruption Court of Ukraine (HACC), Parliament’s Committee on Anti-Corruption Policy (CAP).

In order to analyse the current state of the Information and Telecommunication System of HACC (hereinafter referred to as HACC ITS), collect and summarize information about it, identify problem areas and issues that need to be addressed, develop recommendations on the directions for the development of HACC ITS, the HACC requests the EUACI assistance to conduct HACC ITS audit.

In response to the HACC's request and to support HACC’s further needs for IT capacity building, the EUACI included this activity in its Workplan for the transition period June-December 2022. Moreover, the results of the audit will serve as input data for the development of HACC's IT strategy to ensure the safe operation and sustainable development of HACC in the field of IT.

The High Anti-Corruption Court of Ukraine is the Beneficiary of this assignment.

This TOR contains key requirements for auditing the Information and Telecommunication System of the HACC, the relevant technical and quality characteristics, the scope of work and timeframes.

The HACC ITS audit shall be restricted by the physical boundaries of HACC where the HACC ITS components are located.

The contracting authority is the European Union Anti-Corruption Initiative in Ukraine, implemented by the Ministry of Foreign Affairs of Denmark, hereinafter referred to as the Customer.

**Purpose**

The purpose of the HACC ITS audit is the analysis of the HACC ITS current status, collect and summarise information thereof; identify gaps and issues to be addressed; preparing recommendations on the HACC ITS development areas.

The main tasks of the HACC ITS audit are the following:

* drafting recommendations on the optimal development (upgrade) of the network, server, and operational ITS infrastructure and the technology for data processing in ITS;
* determining the feasibility and practicality of unifying the hardware and software of the ITS components, drafting recommendations on business process automation;
* determining the need to create information protection systems, including KSZI in ITS; drafting recommendations on the development of information protection systems in compliance with the international information security standards.
* developing the description of the ITS operation environment, identifying its elements capable of affecting IS, identifying the interaction between elements of various environments, and documenting audit results for possible further use (in particular, for developing the HACC IT strategy);
* providing recommendations on enhancing the organizational structure of the ITC information security and taking additional regulatory, organizational and/or organizational and technical measures to ensure the safe operation of ITC.

# Objective

The overall objective of this assignment is to conduct an audit of HACC ITS (including a penetration test for IP addresses on the Internet side), taking into account the above purpose and the fulfilment of the requirements described in this TOR.

# Scope of work

The scope of work of the assignment covers the implementation of all activities required for the achievement of its objective as outlined above, including but not limited to:

* 1. **Preliminary review of HACC ITS.**

The HACC ITS preliminary review shall include, but not be limited to the analysis and review of the following:

* the degree of HACC ITS’s conformity to the information provided;
* the completeness of the design, operating, regulatory and administrative documentation provided;
* proposals to the ITS audit plan and sequence of ITS audit activities.

Furthermore, recommendations on the need to refine the submitted documents may be given, develop additional documents or provide additional materials that should be used at subsequent audit stages.

* 1. **Planning the HACC ITS audit.**

The purpose of planning the HACC ITS audit is to develop the document "HACC ITS Audit Programme" (hereinafter, the Programme). Any materials submitted, analysed, and, where necessary, refined by HACC shall be used as input data. The Programme should be dully approved by HACC.

* 1. **HACC ITS audit and analysis of its findings.**

Performing the HACC ITS audit implies taking all actions as stipulated by the approved Programme.

* 1. **HACC ITS penetration test for IP addresses on the Internet side (pen-test).**

The test is intended to imitate an external cybercriminal/hacker/attacker and check the effectiveness of the HACC ITS trusted computing base (TCB). Testing the levels of applications will include the OWASP, 6.5 PCI DSS and NIST SP-815 requirements and the ISACA (P8) penetration testing procedure.

The pen-test should include the followings:

• analysis of system and application software settings;

• scanning ITS to identify open ports, unused services, available installed updates, checking for known vulnerabilities, etc.;

• identifying vulnerabilities related to the use of weak passwords, etc.

All critical/risky operations to be conducted during the test must be approved by HACC.

* 1. **Documenting and approving the HACC ITS audit findings**, including, but not limited to drafting and approving the following documents:
* Act of works on the HACC ITS audit.
* Summary report on the results of the HACC ITS audit.

By drafting the "Summary report on the results of the HACC ITS audit" the following should be taken into account:

* report be designated for the HACC senior management;
* report should include all main results of work performed;
* report should summarize all main identified deficiencies and problems of HACC ITS.
	1. **Drafting and approving Recommendations on developing (upgrading) HACC ITS.**

The work shall result in developing, agreeing upon and approving the document "Recommendations on developing (upgrading) HACC ITS".

By drafting the "Recommendations on developing (upgrading) HACC ITS" the following should be taken into account:

* recommendations be designated for the HACC senior management;
* recommendations should outline ways to eliminate deficiencies identified by the HACC ITS audit;
* suggestions on areas of the HACC ITS development (upgrade) should be included.

# Deliverables

As a formally documented output of the assignment, the following documents should be developed by a Contractor:

1. HACC ITS Audit Programme.
2. HACC ITS Penetration Test Report.
3. Act of works on the HACC ITS audit.
4. Summary Report on the results of the HACC ITS Audit.
5. Recommendations on developing (upgrading) HACC ITS.

The papers shall include, but not be limited to the results of the examination undertaken, with related findings and developed documents attached as annexes where appropriate.

All the documents mentioned in this section “Deliverables” must be prepared in paper and electronic forms. The language of the outputs is Ukrainian.

A detailed description of the expected outputs of the HACC ITS audit is given in [Appendix 1](#_Appendix_1_Website) of this TOR.

# Timing

The assignment shall start following a notification issued by the contracting authority, but not earlier than the date of signing the contract between the EUACI and the Contractor.

The intended commencement date of the conducting of the audit of HACC ITS is 25 August 2022. The estimated time for the examination is up to 3 months starting from signing the contract.

# Methodology

It is envisaged that the assignment will be implemented by a team of experts familiar with the context and experienced with similar assignments.

By conducting the HACC ITS audit, a contractor shall work in close cooperation with the appropriate HACC staff and shall perform on-site visits of the relevant services, desk reviews and consultations. The experts shall make use of all provided legislation, regulations, studies, reports and other relevant documents like statistics, and background materials provided by the HACC. Moreover, HACC shall provide in due time any additional data, reports, analysis, statistics, studies, etc. identified as relevant by the experts during the lifetime of the implementation of this assignment.

By putting forward a team of experts, the Contractor shall ensure that the task will be developed with as much straightforwardness as possible, the proposed approach and the methodology shall be fine-tuned and a detailed work plan shall be elaborated.

**Professional requirements**

The Contractor shall possess the following:

* 5+ years of proven experience in the field of information protection (information security);
* completed projects (at least 3 projects), similar to this one;
* valid licenses from SSSCIP to deliver cryptographic (other than electronic digital signature) and technical information protection services according to the list set out in [Appendix 2](#_Appendix_2._The) of this TOR;
* special permit for carrying out activities associated with state secrets. The classification level specified in the special permit must correspond to the classification level of the information to be used during the ITS audit;
* confidential records unit within its structure;
* qualified experts sufficient to conduct the ITS audit.

The services should be provided by representatives of the Contractor.

The Contractor shall be required to provide information about the experts engaged in the provision of services, namely: a list of documents evidencing their qualifications in the relevant field and the grounds for the provision by them of respective services.

Experts engaged in the HACC ITS audit that includes disclosing state secrets must be provided with duly executed security clearances for access to state secrets. The form of such security clearance must correspond to the classification level of the information that such experts will be allowed to access (their access will be provided for).

The Contractor shall be required to sign an agreement on non-disclosure of confidential information that will become known to it during the HACC ITS audit.

The Contractor’s team is expected to comprise the following profiles:

**Key qualifications of the Team Leader/Project Manager:**

General qualifications

* Relevant education with at least a Bachelor's degree in telecommunication, IT, Information Security or another related technical field;
* Minimum 5 years of professional experience with IT projects, experience with ICT solutions in the public sector institutions;

Adequacy for the assignment

* Project management and planning skills in the field of IT and information protection (information security);
* Expert level of understanding and analyzing regulations in the field of IT and information protection (information security);
* Experience in conducting IT audit of the customer’s infrastructure;
* Experience in state examination of the complex system for information protection in a customer’s ITS;
* Experience in a foreign donor-funded project would be an asset;

Experience with the region and languages

* Relevant working experience from the region;
* Fluency in Ukrainian, knowing of English on a working level.

**Key qualifications of the Technical Expert/Infrastructure:**

General qualifications

* Relevant education with at least a Bachelor's degree in telecommunication, IT or another related technical field;
* At least 5 years of professional working experience in telecommunication, IT, information security or another related technical field;

Adequacy for the assignment

* Experience in conducting IT audit of the customer’s infrastructure;
* Experience in designing technical specifications for the supply of ICT equipment/solutions in the public sector;
* Understanding and analyzing regulations in the field of IT and information protection (information security);
* Experience in a foreign donor-funded project would be an asset.

Experience with the region and languages

* Relevant working experience from the region;
* Fluency in Ukrainian.

**Key qualifications of the Technical Expert/Penetration Tester:**

General qualifications

* Relevant education with at least a Bachelor's degree in telecommunication, IT, information security or another related technical field;
* At least 3 years of professional working experience in software testing for information system intrusion and/or auditing, and/or information systems security or cybersecurity.

Adequacy for the assignment

* Experience in software penetration testing and/or information system audit confirmed by relevant certificates, for instance OSCP (Offensive Security Certified Professional), CISSP (Certified Information System Security Professional), CEH (Certified Ethical Hacker) or similar;
* Proven experience in at least three completed intrusion testing, information system auditing, information system security, or cybersecurity projects;
* Experience in a foreign donor-funded project would be an asset.

Experience with the region and languages

* Relevant working experience from the region;
* Fluency in Ukrainian.

Nevertheless, the contractor can propose a composition of an experts’ team, which, in his opinion, is most appropriate for the assignment.

**Estimated budget**

The maximum budget for this assignment all included may not exceed DKK 148,878 (approximately EUR 20,000).

# Reporting and management

The performance of the Contractor will be judged upon reaching the purpose of this assignment as well as obtaining its results, as indicated in the section “Scope of work” and “Deliverables” herein respectively.

By signing the contract, the Contractor agrees to hold in trust and confidence any information or documents, disclosed to the Contractor or discovered by the Contractors or prepared by the Contractors in the course of or as a result of the implementation of the contract, and agrees that it shall be used only for the task implementation and shall not be disclosed to any third party.

In the period until acceptance, the EUACI, Contractor, and HACC will hold working meetings to exchange information and seek to clarify any questions of whatsoever nature. The purpose of the meetings is to ensure follow-up on any activities between the meetings, to maintain a common overview of the current stage of the assignment at a detailed level, and to ensure the day-to-day progress.

# Background documents

The implementation of the assignment shall meet provisions of laws and regulations of:

* requirements of the Laws of Ukraine, resolutions of the Cabinet of Ministers of Ukraine and other regulatory and statutory instruments on technical security and cryptosecurity of information;
* international information security standards.

# Evaluation criteria

Bids will be evaluated under the criteria provided below:

|  |  |  |
| --- | --- | --- |
| **#** | **Criteria** | **Weight** |
| 1 | Key delivery team members - relevant experience, skills and competencies | 40% |
| 2 | Completed projects, quality and relevance of past work | 20% |
| 3 | Proposed methodology | 20% |
| 4 | Proposed budget | 20% |

# How to apply

The deadline for submitting the proposals is **12 August 2022, 17:00 Kyiv time**.

All interested companies must submit the following information to be considered:

1. Brief company profile (maximum 2 pages).
2. Experts’ CVs (no more than 3 pages for each expert).
3. List of projects with a short description (up to 3 projects), similar to this one, in which the experts involved in this project took part in the last 3 years.
4. Short methodology (max 3 pages) of the proposed consultancy.
5. Financial offer with a budget in Euros.
6. Copies of certificates and permits as specified in [Appendix 2](#_Appendix_2._) of this TOR.

The proposals shall include the aforementioned information and should be submitted within the above deadline to: serkon@um.dk, CC: vikkyl@um.dk indicating the subject line “HACC ITS audit”,

Bidding language: English.

Any clarification questions for the bid request should be addressed to: serkon@um.dk, CC: vikkyl@um.dk no later than **5 August 2022, 10:00 Kyiv time.**

# Appendix 1 Requirements for the deliverables

1. **Preliminary review of HACC ITS**

Working materials on the preliminary review of HACC ITS should include but not be limited to the following:

* preliminary analysis of the input data on ITS, as provided by HACC;
* ITS review in its actual operating environment to determine whether it is ready for the audit;
* preliminary analysis of the design, operational, regulatory and administrative documentation provided by HACC for conformity of the structure thereof with the requirements of applicable regulatory instruments;
* preliminary identification of HACC's requirements for the ITS’s current and future operation;
* documenting the findings and deciding on proceeding with further work.

Following the analysis of these materials, a preliminary set of data shall be developed, but not be limited to the following:

* HACC ITS architecture;
* class and subclass of ITS as an automated system under the provisions of the regulatory instruments of Ukraine;
* information resources available in ITS, their compliance with the requirements of applicable laws, solutions for their processing and security;
* information classification in accordance with the legal regime and the access regime established by the Law of Ukraine "On Information" and other legislative acts;
* requirements of applicable regulatory instruments for the security of certain properties (confidentiality, integrity, availability) of information processed in ITS that the information protection and/or security system must comply with;
* ITS functional structure that should be validated during the audit, the list of organizational, physical, and other security measures, etc.;
* the location, category, and other general ITS characteristics.
1. **Planning the HACC ITS audit**

The Programme shall include but not be limited to the description of the following:

* objectives of and basis for the HACC ITS audit;
* ITS Owner's requirements for HACC ITS;
* procedure for performing the HACC ITS audit to confirm compliance or non-compliance with the requirements of applicable Ukrainian laws and the ITS Owner;
* sequence and time frames of the ITC audit activities.

The following analyses should be taken into account while developing the Programme:

* analysis of the documentation available within ITS and its components and subsystems;
* analysis of the available terms of reference for the ITS design (and/or their elements);
* analysis of the ITS design documentation and materials with the findings of the state expert examination (certification) of individual components (constituent parts) of ITS;
* analysis of the operational documentation and its components with regard to ITS;
* analysis of the regulatory and administrative documents with regard to ITS;
* analysis of the available documents about the completed tests of ITS and its components;
* analysis of the executive documents with regard to ITS;
* analysis of the implementation of organizational, physical, and other non-technical protection measures within ITS;
* analysis of the qualification of the ITS staff and users.

When developing the Programme, experts should observe the requirements of GOST 19.301-79, DSTU 2853-94, and other applicable standards and regulatory instruments in the field of IT and information protection that apply to the preparation and conduct of the HACC ITS audit.

1. **HACC ITS audit and analysis of its findings:**

In the course of the HACC ITS audit, the following characteristics, without limitation, shall be analysed and described:

* overall structural arrangement and composition of ITS (list and composition of equipment, technical and software tools, their interconnections and configuration, architecture and topology features, software and hardware/software information protection facilities, mutual siting of facilities, etc.);
* types and features of communication channels;
* specifics of inter-component interaction and influence;
* potential restrictions on the use of certain tools, facilities, etc.
* computer system components that contain or lack information protection tools and mechanisms, the potential of such tools and mechanisms to protect the information, their respective properties, and features, including those set by default, etc.
* information that ITS processes and stores, its classification by the access and legal regimes and the identified and described forms of its representation in ITS.

The ITS audit should assess the sufficiency of information security and the efficiency of the information security management system. In terms of information security management, the following, without limitation, should be determined:

* existing information security processes and security measures;
* methods for their monitoring, measurement, analysis and assessment that can be used to ensure well-founded results;
* effectiveness of the chosen control and monitoring methods;
* availability of regulatory instruments and administrative measures to control the information security;
* availability of methods for documenting findings from information security assessments;
* availability of mechanisms and methods for internal information security control under an approved regulation and/or specific plans;
* availability of an internal security audit programme;
* availability and comprehensiveness of the analysis of essential processes that are subject to review during audits, audit criteria, etc.;
* availability of controls by the senior management intended to check the information security and the efficiency of the information security management system to ensure that it is always applicable, adequate and effective.
1. **HACC ITS penetration test for IP addresses on the Internet side (pen-test):**

The deliverable from performing the HACC ITS penetration test for IP addresses on the Internet side (pen-test) shall be the "The HACC ITS penetration test report," including but not limited to the following:

* the list of system components within the pen-test framework;
* the methodology of penetration;
* the list of tools used to search for vulnerabilities;
* the test flow description;
* the list of identified vulnerabilities, their risk rating and recommendations for reducing them;
* vulnerability proofs and reproduction stages;
* detailed recommendations on reducing all identified vulnerabilities.
1. **Documenting and approving the HACC ITS audit findings:**

The deliverables from drafting the "Act of works on the HACC ITS audit" should be a prepared and approved document that includes all findings of the HACC ITS audit.

The deliverables from drafting the "Summary Report on the HACC ITS Audit" should be a prepared and approved document that should include but not be limited to the following sections:

1. findings of the analysis of the ITS computer system:
* network infrastructure;
* server infrastructure;
* operational infrastructure;
* security infrastructure;
1. findings of the analysis of the ITS operational environment:
* informational environment (including the processing solution);
* physical environment;
* user environment (personnel);
1. findings of the ITS organizational structure analysis:
* rules for the ITS operation;
* the structure and role composition of functional ITS user teams;
1. findings from the analysis of information security provisions;
2. assessment of ITS assets and suggestions for the optimal development (upgrade) of the ITS network, servers, and operating architecture and the technology for information processing in ITS;
3. suggestions for the unification of the HACC ITS components’ software and hardware;
4. recommendations for the development (upgrade) of the KSZI in HACC ITS, in the form of a description of each HACC ITS’s operating environment, listing the components of various environments, which may, either directly or indirectly, affect IS;
5. conclusions of the findings from the audit of the HACC ITS and its operating environments.

The “Summary Report on the HACC ITS Audit” shall be finalized and submitted according to the requirements of DSTU 3396.1-96, ND TZI 3.7 003-05 and DSTU ISO/IEC 27001:2015.

The “Summary Report on the HACC ITS Audit” must be signed by the experts who performed the examination and duly approved by HACC.

1. **Drafting and approving recommendations on developing (upgrading) HACC ITS:**

The deliverables from drafting the "Recommendations on developing (upgrading) HACC ITS" should be the document that contains suggestions for the HACC ITS development (upgrade) and should be further applicable for:

* drafting the IT development strategy;
* drafting the HACC ITS development concept;
* drafting the plan of the information infrastructure development (upgrade);
* ensuring safe operation and sustainable development of the information infrastructure;
* recommendations on hardware and software with the post-warranty support;
* planning and conducting the comprehensive penetration test (comprehensive pen-test) of HACC ITS;
* planning of advanced training for employees responsible for the functioning of HACC ITS.

# Appendix 2. The list of licenses from SSSCIP

The list of licenses from the Administration of the State Service of Special Communications and Information Protection to deliver cryptographic (other than electronic digital signature) and technical information protection services to be held by the Contractor for the HACC ITS audit:

1. **License in the field of technical information protection:**

The license for the commercial delivery of cryptographic (other than electronic digital signature) and technical information protection services in accordance with the list approved by the Cabinet of Ministers of Ukraine, with respect to an assessment of information protection.

1. **License in the field of cryptographic information protection:**

The license for the commercial delivery of cryptographic (other than electronic digital signature) and technical information protection services in accordance with the list approved by the Cabinet of Ministers of Ukraine, with respect to the following:

* developing and drawing up a design and other technical documentation, production of cryptosystems and cryptographic information protection tools (with the right to operate in the field of cryptographic protection of privileged information);
* supply, installation (deployment), configuration, technical maintenance (support), repair and/or disposal of cryptosystems and cryptographic information protection tools (with the right to operate in the field of cryptographic protection of privileged information);
* thematic reviews and expert studies of cryptosystems and cryptographic information protection tools (with the right to operate in the field of cryptographic protection of privileged information).