

ANNEX 2.2

Technical Requirements for the Preparation of the Detailed Technical Specification and Software Development Services for the Unified Automated Information and Analytical System of the Central Election Commission of Ukraine (Phase I)

1. Purpose of this Annex

This Annex defines the minimum technical requirements for the Contractor responsible for the preparation of the Detailed Technical Specification, software design, software development, deployment, testing, documentation, knowledge transfer and warranty support for the Unified Automated Information and Analytical System of the Central Election Commission of Ukraine (Phase I) (hereinafter referred to as the "CEC EIAS (Phase I)" or "System").

This Annex shall be read together with:

- Terms of Reference for the Procurement of Services for the Preparation of the Detailed Technical Specification and the Development of the Software for the Unified Automated Information and Analytical System of the Central Election Commission of Ukraine (Phase I);
- Technical Requirements for the Creation of the Unified Automated Information and Analytical System of the Central Election Commission of Ukraine (Phase I);
- Concept of the Unified Automated Information and Analytical System of the Central Election Commission;
- Architectural Principles of the Unified Automated Information and Analytical System of the Central Election Commission.

In the event of any inconsistency between this Annex and the approved Technical Requirements of the Central Election Commission, the Technical Requirements shall prevail unless otherwise agreed in writing by the Beneficiary and International IDEA.

2. General Objectives

The Contractor shall provide a complete end-to-end software engineering service covering the entire software lifecycle required for the implementation of the CEC EIAS (Phase I).

The overall objective is to deliver software for the CEC EIAS (Phase I) that complies with the approved Technical Requirements, the Architectural Principles, applicable Ukrainian legislation, the approved Detailed Technical Specification and the applicable acceptance criteria.

The Contractor shall be responsible for:

- analysis of the existing environment;
- preparation of the Detailed Technical Specification;
- architecture design;
- software design;
- software development;

- software integration;
- deployment;
- testing;
- documentation;
- knowledge transfer;
- warranty support.

The Contractor shall deliver all activities necessary to commission the software into production operation on the infrastructure provided by the Central Election Commission.

3. General Scope of Services

The scope of services includes all engineering, technical, analytical and implementation activities required for successful completion of Stage 1 and Stage 2 of the procurement.

The Contractor shall perform, at minimum, the following activities:

- business analysis;
- requirements engineering;
- architecture design;
- preparation of the Detailed Technical Specification;
- software design;
- software development;
- API development;
- data and metadata modelling;
- implementation of integrations;
- software configuration and deployment in the environments provided by the CEC;
- testing;
- documentation;
- preparation of training materials and delivery of training to the user groups specified in Section 13 of the Technical Requirements;
- knowledge transfer;
- warranty support.

The Contractor shall provide all professional services necessary to deliver a complete operational software solution.

4. General Software Engineering Principles

The Contractor shall perform the Services in accordance with the approved Technical Requirements and Detailed Technical Specification and shall ensure modularity, configurability, interoperability, requirements traceability, controlled source-code management, configuration management, documented build and deployment procedures, and application of information-security and cybersecurity requirements throughout the development lifecycle.

5. Preparatory Activities

Before commencing the preparation of the Detailed Technical Specification, the Contractor shall perform comprehensive discovery and assessment activities.

These activities shall include, but shall not be limited to:

5.1 Review of Project Documentation

The Contractor shall review all documentation provided by International IDEA and the Central Election Commission, including:

- approved Technical Requirements;
- Concept of the CEC EIAS;
- Architectural Principles;
- applicable legislation;
- existing ICT documentation;
- available architecture diagrams;
- existing integration documentation;
- available operational and information-security documentation relevant to the scope of the System.

The Contractor shall identify inconsistencies, ambiguities and implementation risks.

5.2 Assessment of Existing ICT Environment

The assessment shall cover the existing technical infrastructure, virtualized environments, network environment, cybersecurity tools, relevant existing systems, integration interfaces, monitoring and backup capabilities, insofar as they affect the design, deployment and operation of the CEC EIAS (Phase I).

The Contractor shall identify technical constraints that may affect implementation.

5.3 Business Analysis Workshops

The Contractor shall organize structured workshops with representatives of the Central Election Commission and International IDEA.

The workshops shall validate:

- business processes;
- operational workflows;
- user roles;
- data flows;
- integration scenarios;
- security requirements;
- reporting and analytical requirements specified in the Technical Requirements;
- acceptance criteria.

The Contractor shall prepare workshop minutes and document identified issues, assumptions, dependencies and decisions in the workshop minutes and/or project registers required under the ToR.

5.4 Gap Analysis

The Contractor shall compare:

- approved Technical Requirements;
- current ICT environment;
- available infrastructure;
- operational procedures.

The Contractor shall identify:

- implementation gaps;
- infrastructure limitations;
- integration risks;
- cybersecurity risks.

The results shall be reflected in the Inception Report, Risk Register and Stage 1 work plan, as applicable.

6. Stage 1 – Preparation of the Detailed Technical Specification

The Contractor shall prepare a complete Detailed Technical Specification that transforms the approved Technical Requirements into a comprehensive engineering specification suitable for software implementation.

The Detailed Technical Specification shall become the primary implementation document for Stage 2.

The following items may be provided as sections or annexes of the Detailed Technical Specification, unless otherwise agreed in the approved Stage 1 work plan.

The Technical Specification shall include, at minimum:

- Detailed functional requirements, business processes and algorithms;

- Data and metadata models, including entities, attributes and relationships;
- Role-based access model;
- APIs, message formats and integration contracts;
- Key user-interface wireframes;
- Non-functional requirements;
- Information-security and cybersecurity requirements;
- Logging, monitoring and audit requirements;
- Test scenarios and acceptance criteria;
- High-level architecture design;
- Testing Strategy and Test Plan;
- Documentation Plan;
- Training Plan;
- Deployment Plan;
- Stage 2 Work Breakdown Schedule;
- Resource allocation plan;
- Dependency map;
- Risk Register;
- Requirements Traceability Matrix.

7. Requirements Traceability

The Contractor shall establish and maintain a Requirements Traceability Matrix (RTM) linking every requirement contained in the approved Technical Requirements with:

- software modules;
- business processes;
- APIs;
- databases;
- integrations;
- user interfaces;
- test cases;
- acceptance criteria.

The RTM shall remain updated throughout the implementation lifecycle and shall form part of the project documentation.

8. Stage 2 – Software Design and Development

Following the successful completion and formal approval of Stage 1, the Contractor shall commence software design, software development, configuration, integration, deployment, testing and implementation activities for the Unified Automated Information and Analytical System of the Central Election Commission of Ukraine (Phase I).

All software shall be developed strictly in accordance with the approved Detailed Technical Specification and the Official Technical Requirements of the Central Election Commission.

The Contractor shall ensure that every software component is designed, implemented, tested and documented as a production-ready software product.

Development activities shall follow an iterative delivery approach, allowing the Central Election Commission and International IDEA to review intermediate results throughout the implementation period.

The detailed functional behaviour of each software component shall be implemented in accordance with the approved Technical Requirements and the Detailed Technical Specification. The functional descriptions provided in this Annex are intended solely to define the scope of services and shall not replace or modify the approved Technical Requirements.

8.1 General Development Requirements

At minimum, the Contractor shall:

- maintain source code using a version control system;
- maintain complete configuration management;
- implement secure coding practices;
- apply consistent development standards across all software components;
- perform internal code review and quality-control activities in accordance with the Contractor's approved development methodology;
- provide repeatable deployment procedures;
- maintain complete traceability between requirements, source code and testing.

The Contractor shall ensure that all developed software remains maintainable, extensible and reusable for future implementation phases of the CEC EIAS.

8.2 Development of Common Platform Mechanisms

The Contractor shall design, develop, configure and implement all Common Platform Mechanisms required for operation of the CEC EIAS.

These mechanisms constitute the shared software platform used by all functional components and shall not be implemented independently by individual modules unless explicitly approved by the Beneficiary.

The scope shall include, but shall not be limited to:

- Form Builder;
- Metadata Builder, including dynamic data models;
- Checks and Validation Rules Builder;
- Report and Analytical Selection Template Builder;
- Centralized Reference Data and Classifiers;
- Unified Metadata and Data Structure Model;
- Logging Mechanisms;
- Monitoring Mechanisms;
- User Cabinet Platform;
- Unified APIs and Message Exchange Mechanisms;
- Event Integration Bus;
- Shared user interface components, to the extent defined in the Technical Requirements.

The Contractor shall ensure that all platform mechanisms are reusable across future implementation phases.

8.3 Development of AIKS "Elections"

The Contractor shall develop the core business component responsible for automation of election processes.

The software shall support, at minimum:

- election process initialization;
- election calendar management;
- territorial organization;
- election commission management;
- processing and registration of candidates and other participants in the electoral process, including representatives, authorized and trusted persons, official observers and members of election commissions, in accordance with the Technical Requirements;
- document processing;
- election preparation;
- election day activities;
- vote counting;

- protocol preparation;
- electronic protocol validation;
- result aggregation;
- publication of information required by electoral legislation;
- reporting;
- analytics;
- transmission of electronic data and documents between election commissions;
- preparation for voting, including the relevant ballot-related processes specified in the Technical Requirements;
- automation of budget planning, allocation, accounting and control over the use of funds allocated for the preparation and conduct of elections, within the scope defined by the Technical Requirements.

The Contractor shall ensure compliance with the Electoral Code of Ukraine.

8.4 Development of AIS "Electronic Services"

The Contractor shall develop the electronic interaction platform enabling secure communication between election participants and the Central Election Commission.

The system shall support:

- electronic user accounts;
- secure authentication;
- qualified electronic signatures;
- document history;
- submission, signing, automated verification, processing, status tracking and notification concerning electronic documents and copies of documents submitted by electoral-process participants;
- secure interaction with other components;
- closure of electronic user accounts in accordance with the applicable procedures;
- transmission of verified data to the relevant components of the CEC EIAS (Phase I).

The Contractor shall ensure accessibility and usability for external users.

8.5 Development of AIS "Participants in Election and Referendum Processes"

The Contractor shall develop the centralized registry responsible for management of election participants.

The registry shall support:

- candidates;
- political parties;

- authorized representatives;
- trusted persons;
- official observers;
- election commission members;
- historical records;
- status management;
- training records.

The registry shall support secure data exchange with all software components.

8.6 Development of AIS VIS

The Contractor shall develop the centralized integration platform responsible for communication with external governmental information systems.

The solution shall provide:

- standardized APIs;
- secure communication;
- message validation;
- routing;
- audit trail;
- retry mechanisms;
- error handling;
- monitoring;
- logging.

Interaction with external state electronic information resources shall be implemented through AIS VIS. Direct point-to-point integrations may be used only where expressly approved by the Client or required by law.

8.7 Development of AIKS UDIB

The Contractor shall develop the centralized identity, access management and information security component.

The component shall provide:

- authentication;
- authorization;
- role management;

- permission management;
- policy management;
- session management;
- access auditing;
- authorization traceability;
- security event logging;
- management of information-security incidents related to access.

The Contractor shall ensure integration with all software modules.

8.8 Development of Protected Automated Workstations (ARM)

The Contractor shall develop secure client software for operation of Protected Automated Workstations.

The software shall support:

- kiosk mode;
- offline-first operation;
- synchronization;
- qualified electronic signature;
- secure printing;
- encrypted communications;
- controlled loading from an approved environment;
- integrity verification of the software environment;
- controlled distribution and updating of system images in accordance with the approved Detailed Technical Specification;
- controlled data exchange.

The Contractor shall ensure compatibility with the standard access, identification, signing and communication equipment specified in the Technical Requirements and supplied or made available for testing.

For testing, acceptance and debugging of the ARM client software, the Contractor shall provide the limited set of equipment specified in the Technical Requirements, including:

- secure data storage devices — 10 units;
- secure personal key storage devices — 10 units;
- 4G/LTE cellular modems — 10 units;
- 4G LTE MIMO antennas — 10 units.

The supplied equipment shall be used exclusively for testing, acceptance, debugging and verification of compatibility with the ARM client software.

8.9 Modification of AIS “CEC SED”

The Contractor shall implement the modifications to AIS “CEC SED” necessary for the exchange of official documents, registration details, election-process documents and related information. The modifications shall be limited to the integration scope defined in the Technical Requirements and shall not include a restructuring of the underlying architecture of AIS “CEC SED”.

8.10 Modification of AICS “State Voter Register” (AICS DRV)

The Contractor shall implement the modifications and integration mechanisms necessary for access to and use of State Voter Register information within electoral-process verification procedures. Such modifications shall not alter the purpose or core internal logic of AICS DRV and shall be limited to the scope defined in the Technical Requirements.

9. Integration Requirements

The Contractor shall design and implement all software integrations required by the approved Technical Requirements.

The integration scope shall include:

- AICS "Elections";
- AIS Electronic Services;
- AIS “Participants in Election and Referendum Processes” (AIS UVPR);
- AIS VIS;
- AICS UDIB;
- Common Platform Mechanisms;
- AIS “CEC SED”;
- AICS “State Voter Register” (AICS DRV);
- state electronic information resources specified in the Technical Requirements;
- any additional integration interfaces formally included in the approved Detailed Technical Specification or subsequently approved in writing through the Change Management procedure.

The Contractor shall document every integration using standardized interface specifications.

The Contractor shall verify integrity, consistency and traceability of the exchanged data in accordance with the approved data and integration models.

9.1 API Requirements

All application interfaces shall be documented using OpenAPI, AsyncAPI or an equivalent specification agreed during Stage 1.

Each API shall include:

- endpoint description;
- request structure;
- response structure;
- authentication;
- authorization;
- error codes;
- versioning;
- performance and access-control requirements, where applicable;
- audit requirements.

The Contractor shall provide complete API documentation as part of project deliverables.

9.2 Data Migration and Data Integrity

Where migration or controlled transfer of existing data is expressly required by the approved Detailed Technical Specification, the Contractor shall prepare and execute the relevant migration activities.

The migration process shall include:

- migration strategy;
- data-transfer or migration scripts, where required by the approved Detailed Technical Specification;
- validation procedures;
- reconciliation reports;
- rollback procedures;
- data integrity verification.

No production migration shall be performed without written approval from the Beneficiary.

9.3 Configuration and Release Management

The Contractor shall establish controlled procedures governing software releases.

These procedures shall include:

- release planning;
- release approval;

- version numbering;
- release notes;
- deployment packages;
- rollback procedures;
- configuration baselines;
- environment consistency verification.

Production releases shall be approved and deployed in accordance with the agreed release, deployment and acceptance procedures.

10. Infrastructure Preparation and Deployment

The Contractor shall prepare, configure, deploy and validate the software solution within the ICT infrastructure of the Central Election Commission.

The deployment activities shall ensure that the developed solution is fully operational, secure, scalable and maintainable throughout its operational lifecycle.

The Contractor shall prepare deployment procedures covering every environment used during software development and production operation.

10.1 Development Environment

The Contractor shall configure and use a controlled Development Environment hosted on infrastructure provided or approved by the CEC, subject to the availability of the necessary resources.

The Development Environment shall support, at minimum:

- source code management;
- controlled development, compilation, initial configuration, unit testing, software packaging and verification of software components.

The Development Environment shall remain isolated from all testing and production environments.

10.2 Test Environment

The Contractor shall establish a dedicated Test Environment for validation of software functionality.

The Test Environment shall support:

- Qualified Electronic Signature creation and verification testing;
- printing scenarios;
- functional testing;
- regression testing;
- integration testing;
- API testing;

- security testing;
- load testing;
- offline/online and synchronization scenarios;
- recovery scenarios.

The Contractor shall ensure that software versions deployed within the Test Environment correspond to approved release packages.

10.3 Pre-production Environment

Prior to deployment into production, the Contractor shall configure the Pre-production Environment in accordance with the approved Deployment Plan and the documented environment parameters.

The Pre-production Environment shall be used for:

- final system validation;
- deployment verification;
- production simulation;
- performance verification;
- operational readiness assessment;
- rollback validation.

10.4 Production Deployment

The Contractor shall perform controlled deployment into the Production Environment in accordance with the approved Deployment Plan and agreed acceptance procedures.

Production deployment shall include:

- software installation;
- configuration;
- database deployment;
- approved data-transfer or migration activities, where applicable;
- interface activation;
- security configuration;
- monitoring activation;
- backup configuration;
- operational validation.

11. Testing Requirements

The testing programme shall be structured in accordance with Section 15 of the Technical Requirements and shall include preliminary testing, acceptance testing and trial operation. Unit, functional, integration, load, security, regression and recovery testing shall be performed as applicable under the approved Testing Strategy and Test Plan.

The Contractor shall prepare and execute a comprehensive testing programme covering every developed software component.

Testing shall demonstrate that the developed solution satisfies all approved functional and non-functional requirements.

Testing activities shall be fully documented.

11.1 Unit Testing

The Contractor shall perform Unit Testing for every software module.

Unit Testing shall verify:

- business logic;
- validation rules;
- error handling;
- database interaction;
- API behaviour.

Unit Test results shall be documented.

11.2 Integration Testing

The Contractor shall perform Integration Testing covering all interfaces between software components.

Integration Testing shall include:

- API communication;
- database synchronization;
- workflow execution;
- data exchange;
- authentication;
- authorization.

11.3 Functional Testing

Functional Testing shall verify complete compliance with the approved Detailed Technical Specification.

Functional Testing shall include:

- user scenarios;
- business processes;
- document processing;
- workflow execution;
- reporting;
- search functions;
- administration functions.

11.4 Performance Testing

The Contractor shall perform performance testing demonstrating that the solution satisfies expected operational workloads.

Testing shall include:

- concurrent users;
- response times;
- database performance;
- transaction processing;
- scalability verification.

Performance bottlenecks shall be corrected prior to production deployment.

11.5 Security Testing

The Contractor shall perform information-security and cybersecurity assessment in accordance with the approved Testing Strategy, Test Plan and Technical Requirements.

Security testing shall include:

- authentication testing;
- authorization testing;
- access control verification;
- session management;
- encryption verification;
- verification of compliance with the information-security and cybersecurity requirements specified in Sections 8–11 of the Technical Requirements;
- audit logging.

The Contractor shall remediate identified security vulnerabilities prior to production deployment.

11.6 Acceptance Testing and Trial Operation

The Contractor shall support the CEC during trial operation, resolve identified non-conformities and provide the documentation and technical assistance required for subsequent acceptance testing.

Following successful completion of trial operation, the Contractor shall support the CEC in conducting acceptance testing in accordance with Section 15 of the Technical Requirements.

The Contractor shall:

- prepare test scenarios;
- provide testing support;
- analyse defects;
- implement corrective actions;
- repeat testing where necessary.

Acceptance shall be documented in accordance with the acceptance procedures specified in the ToR, the Technical Requirements and the Contract.

12. Documentation Requirements

The Contractor shall prepare complete technical and operational documentation covering every developed software component.

All documentation shall be delivered in editable electronic format and PDF.

12.1 Technical Documentation

The mandatory documentation package shall include:

- design documentation;
- operational documentation;
- administration and maintenance documentation;
- information-security documentation.

These documentation categories shall include, as applicable, the approved architecture description, data and metadata models, API and integration documentation, deployment documentation, configuration descriptions, administrator manuals, user manuals, maintenance procedures and recovery procedures.

12.2 Operational Documentation

Operational documentation shall include:

- Administrator Guide;
- Operator Guide;
- Backup Procedures;

- Disaster Recovery Procedures;
- Maintenance Procedures;
- Monitoring Procedures;
- Troubleshooting Guide;
- Operational Manual.

12.3 User Documentation

User documentation shall include:

- User Manuals;
- Quick Reference Guides;
- Process Descriptions;
- Training Materials.

Documentation shall be prepared in Ukrainian unless otherwise agreed by the Beneficiary.

13. Knowledge Transfer

The Contractor shall ensure complete transfer of knowledge required for sustainable operation and future maintenance of the software solution.

Knowledge Transfer shall include structured technical sessions, workshops and practical demonstrations.

13.1 Administrator Training

Training shall be provided for designated system administrators.

Training topics shall include:

- system architecture;
- deployment;
- configuration;
- monitoring;
- backup;
- troubleshooting;
- maintenance;
- security administration.

13.2 Technical Knowledge Transfer

The Contractor shall provide technical knowledge transfer covering:

- software architecture;
- source code structure;
- database design;
- API architecture;
- configuration management;
- release procedures;
- maintenance procedures.

Training materials and other project artefacts shall be transferred to International IDEA and/or the CEC in accordance with the Contract.

13.3 User Training and Training Materials

The Contractor shall prepare training materials and conduct training for CEC administrators, CEC users and users of district and precinct election commissions in accordance with Section 13 of the Technical Requirements. Training shall be completed before the relevant components are accepted into production operation.

For external users of AIS “Electronic Services”, the Contractor shall prepare materials for independent familiarization and use of the electronic services, as required by the Technical Requirements.

13.4 Source Code Handover

Upon completion of the project, the Contractor shall transfer all project artefacts necessary for future maintenance and further development.

The handover shall include:

- complete source code;
- build scripts;
- deployment scripts;
- configuration files;
- database scripts;
- API definitions;
- documentation;
- third-party component inventory;
- software dependency list;
- issue tracker records;
- release notes;
- documented build and deployment instructions;

- administrator runbooks;
- operational monitoring procedures;
- warranty-support escalation procedures.

All artefacts shall be delivered in a structured repository together with the available repository history and release records maintained during the Project.

14. Warranty Support

Following the successful completion of the implementation and formal acceptance of the System, the Contractor shall provide warranty support for a minimum period of twelve (12) months unless otherwise specified in the Contract.

The warranty period for the relevant components shall commence on the date of signing the act confirming their commissioning into commercial (production) operation, unless another period is specified in the Contract.

The objective of the warranty support shall be to ensure the stable, secure and uninterrupted operation of the System during production use.

14.1 Scope of Warranty Services

The Contractor shall provide, at minimum:

- correction of software defects affecting or potentially affecting the required functions;
- correction of errors causing incorrect processing, storage or transmission of electoral or official information;
- restoration of operability following failures caused by design, development, configuration or implementation errors;
- preservation of data integrity, consistency and immutability during corrective work;
- troubleshooting and software configuration support;
- provision, testing and deployment of corrective releases where required;
- consultation for system administrators as a supplementary warranty-support activity.

Warranty support shall cover all software developed under this Contract.

14.2 Warranty Support Procedures and Escalation

Incident prioritization, response procedures and escalation arrangements shall be defined in the Warranty Support Plan in accordance with Section 12 of the Technical Requirements. During an election process taking place within the warranty period, the Contractor shall provide round-the-clock support without restrictions based on working hours, weekends or holidays.

14.3 Corrective Maintenance

Corrective maintenance shall be performed in accordance with the approved Warranty Support Plan and shall include investigation, correction, testing and controlled deployment of fixes, together with the necessary updates to the relevant documentation.

15. Deliverables

The Contractor shall deliver all project outputs required for successful implementation of the Project.

At minimum, the following Deliverables shall be provided.

Stage 1 Deliverables

Detailed Technical Specification, including:

- Solution Architecture;
- Business Process Models;
- Data and Metadata Models;
- Integration Specification;
- Requirements Traceability Matrix;
- Testing Strategy and Test Plan;
- Documentation Plan;
- Training Plan;
- Deployment Plan;
- Stage 2 Work Breakdown Schedule;
- Resource Allocation Plan;
- Dependency Map;
- Risk Register.

Stage 2 Deliverables

The Contractor shall deliver:

- complete software source code;
- compiled software packages;
- installation packages;
- database scripts;
- deployment scripts;
- configuration files;

- APIs;
- software integrations;
- monitoring configuration;
- release packages;
- test protocols and test reports;
- release notes;
- documentation packages;
- training materials;
- handover and knowledge-transfer artefacts.

Final Deliverables

Upon completion of the Project, the Contractor shall provide:

- complete project documentation;
- administrator documentation;
- operational documentation;
- user documentation;
- training materials;
- source code repository;
- third-party software inventory;
- approved Warranty Support Plan and warranty-support procedures;
- Stage 2 Final Delivery Report.

16. Acceptance Criteria

Each Deliverable shall be formally reviewed and approved by the Central Election Commission and International IDEA.

Acceptance shall be based upon compliance with:

- approved Technical Requirements;
- approved Detailed Technical Specification;
- Contract requirements;
- successful completion of testing;
- absence of defects classified as critical under the approved Testing Strategy and Test Plan, and resolution of other non-conformities to the extent required by the applicable acceptance procedures;

- satisfactory documentation;
- successful knowledge transfer.

No Deliverable shall be considered accepted without written approval.

16.1 Stage Acceptance

Acceptance shall be performed separately for each implementation stage.

Completion of Stage 1 shall require approval of the Detailed Technical Specification.

Only after formal approval shall the Contractor proceed to Stage 2.

16.2 Final Acceptance

Final Acceptance shall require successful completion of:

- software implementation;
- deployment;
- successful completion of preliminary testing, trial operation and acceptance testing, in that sequence, in accordance with Section 15 of the Technical Requirements;
- documentation;
- administrator training;
- user training;
- knowledge transfer;
- source code handover;
- provision of the relevant acceptance protocols and acts required for commissioning into production operation.

17. Quality Assurance Requirements

The Contractor shall perform internal quality-control activities necessary to ensure compliance of the Deliverables with the Technical Requirements, the approved Detailed Technical Specification, the Testing Strategy and the applicable acceptance criteria. Evidence of such activities shall be provided where required under the approved project methodology.

18. Secure Software Development Requirements

The Contractor shall apply secure-design, information-security and cybersecurity requirements throughout the design, development, testing, deployment and warranty-support activities. The implementation shall cover authentication, authorization, role-based access control, electronic trust services, protection of communication channels and stored data, logging, monitoring, auditing, incident handling and protection against unauthorized modification of critical election data, in accordance with Sections 8–11 of the Technical Requirements.

19. Project Governance and Reporting

The Contractor shall maintain effective communication with the Central Election Commission and International IDEA throughout the implementation period.

The Contractor shall participate in project meetings and provide regular progress updates.

At minimum, the Contractor shall submit:

- Inception Report;
- bi-weekly progress reports;
- Stage 1 Final Report;
- Stage 2 implementation reports;
- Stage 2 Final Delivery Report;
- Warranty Period Reports.

All project documentation shall be maintained throughout the duration of the Contract. All written deliverables and reports shall be provided in Ukrainian. The Inception Report, Phase 1 Final Report and Phase 2 Final Delivery Report shall additionally include an executive summary in English. All deliverables shall be provided in editable electronic formats and PDF.

20. Change Management

Any modification to the approved scope, architecture, functional requirements, implementation schedule or Deliverables shall be managed through a formal Change Management process.

Each proposed change shall include:

- description of the requested change;
- justification;
- impact assessment.

Any change to the approved scope or requirements shall be subject to prior written approval by International IDEA and the CEC and shall be managed in accordance with the Contract.

21. Assumptions and Dependencies

The successful implementation of the Project is based on the following assumptions:

- the Central Election Commission shall provide timely access to the required infrastructure, environments and technical documentation;
- designated representatives of the Central Election Commission shall participate in workshops, reviews and acceptance activities;
- the approved Technical Requirements shall remain the baseline specification unless formally amended;

- all Deliverables shall be reviewed within the agreed timeframes;
- software implementation shall comply with applicable legislation of Ukraine;
- the CEC shall designate technical representatives and, where required, facilitate interaction with the operators of existing CEC systems and relevant state electronic information resources.

Should any of these assumptions materially change, the Parties shall assess the impact on the Project and agree on appropriate corrective actions through the established governance and change management procedures.

Procurement of new server and network equipment is outside the scope, except for the limited testing equipment expressly specified in the Technical Requirements.

22. Ownership of Deliverables and Intellectual Property Rights

Unless otherwise specified in the Contract, all source code, configurations, documentation, test artefacts and results developed specifically under the Contract shall be transferred to International IDEA and/or the CEC in editable and reusable formats, with sufficient rights for operation, maintenance, modification and further development.

The Contractor shall identify all third-party software, open-source components, proprietary tools and licensing dependencies, including applicable licensing conditions and restrictions on future maintenance.

The Contractor shall ensure that all Deliverables are free from legal restrictions that would prevent their use, operation, maintenance, modification or further development by International IDEA, the CEC or a subsequent contractor acting on their behalf, in accordance with the Contract.

End of Annex

The Contractor shall acknowledge that submission of a Proposal constitutes confirmation that the requirements specified in this Annex have been reviewed, understood and accepted as the minimum technical requirements for the implementation of the Project.