

APPENDIX II: BUSINESS AND TECHNICAL REQUIREMENTS

FOR THE COMPLAINT TRACKING AND DENUNCIATIONS PLATFORM FOR THE CENTRAL ELECTION COMMISSION IN ALBANIA”

March 2025

The activity is carried out in the framework of the Council of Europe project “Strengthening Election’s Integrity in Albania” implemented by the Council of Europe Office in Tirana’

TABLE OF CONTENTS

1	INTRODUCTION.....	5
1.1	Background	5
1.2	Project scope and Objectives	5
1.3	Out of Scope.....	5
1.4	Beneficiary and Stakeholders.....	5
1.4.1	Presentation of the CEC relevant directorates / departments.....	5
1.4.2	Stakeholders.....	7
1.5	Business processes	7
1.5.1	Existing (AS-IT- IS) processes.....	7
1.5.2	CEC IT Systems:	10
2	SOLUTION DESCRIPTION	11
2.1	Business requirements.....	13
2.2	Non-Functional Requirements	23
2.3	Interface requirements.....	24
2.4	User profiles.....	25
3	TECHNICAL REQUIREMENTS.....	26
3.1	Operational environment Standards.....	26
3.2	Hardware and infrastructure requirements	27
3.3	Access modes and security requirements.....	27
3.4	Operational Security.....	28
3.5	Business Continuity plan (Disaster recovery)	28
3.6	Backup and Archiving.....	28
3.7	Service level: availability, performance and support	28
3.8	System Documentation.....	29
4	SYSTEM IMPLEMENTATION AND REALIZATION.....	30
4.1	System Schedule	30
4.2	Location.....	31
4.3	System Costs	31
4.4	Bidder profile requirements	32
5	CRITICAL CONSIDERATIONS.....	33
5.1	Assumptions	33
5.2	Constraints	33
5.3	Risks	33
6	DATA REQUIREMENTS.....	35
6.1	Data inputs	35
6.2	Data Outputs and Reporting Requirements	36
6.3	User Documentation and Training Requirements	36
7	REGULATORY REQUIREMENTS.....	37
7.1	Privacy Requirements	37
7.2	Audit Requirements	37
7.3	Legislation	37

8	REPORTING AND EXPECTED DELIVERABLES	38
8.1	Reporting Requirements	38
8.2	Expected Deliverables.....	38
	LIST OF APPENDICES.....	39

ABBREVIATIONS

TERM	DESCRIPTION
CEC	CENTRAL ELECTION COMMISSION
COE	COUNCIL OF EUROPE
NAIS	NATIONAL AGENCY OF INFORMATION SOCIETY
TOR	TERMS OF REFERENCE
RFP	REQUEST FOR PROPOSAL
XML	EXTENSIBLE META LANGUAGE
EFORMS	ELECTRONIC FORMS
EAZC	ELECTION ADMINISTRATION ZONE COMMISSION

1 INTRODUCTION

1.1 Background

The Council of Europe is implementing the Project “Strengthening Elections Integrity in Albania” (SEI), funded by the Federal Republic of Germany. It aims at supporting the Central Election Commission (CEC) regulatory framework and institutional capacities related to the professionalization of election administration, voters’ education programmes, with a focus on first-time voters, and efficiency and transparency of the Election Dispute Resolution (EDR) process. This would contribute to enhance elections’ integrity, trust of citizens in the electoral process and ultimately increase turnout of voters. The Project will focus also on strengthening the CEC instruments and IT tools to effectively track election-related complaints through establishing the CEC Complaint Tracking and Denunciations Platform/Module.

In this context, this document represents the detailed business and technical requirements to develop an IT solution for CEC Complaint Tracking and Denunciations. The document stems from the CEC needs and takes into the consideration the requirements of the CEC, the regulatory framework defined by the Albanian National Agency for Information Society (NAIS) and is in compliance with data protection standards.

1.2 Project scope and Objectives

All organizations need to organize the processes they operate most and at the same time keep records of business decisions and transactions to meet the demands of accountability.

CEC processes run on information created by CEC or other stakeholders. This information is created, collected, processed, distributed, stored, managed, retrieved, maintained and disposed as an integral part of every business process and activity of the organization.

CEC spends an immense effort to increase the effectiveness and efficiency, but it cannot be achieved without creation of business applications and systems that can process vast volumes of processes and information.

The Action aims to support the CEC to digitalize the process of Complaint Tracking and Denunciations.

1.3 Out of Scope

Purchase of the hardware and other related components are not in the scope of this document.

1.4 Beneficiary and Stakeholders

The Contracting Authority for this tender is the Council of Europe, whereas the beneficiary is the Central Election Commission in Albania.

1.4.1 *Presentation of the CEC relevant directorates / departments*

The Central Election Commission is the highest permanent state institution in charge of administering elections with a view to guaranteeing and respecting the principles, rights, guarantees, constitutional and legal, in the conduct of elections. In order to accomplish the above goal, the CEC is adhered to:

- Correct and full implementation of Constitutional and legal norms in the organization and administration of elections.
- Supervise, monitor and audit the funds benefited and spent by political parties, during election campaign, outside the election campaign and draft by laws for the implementation of the Electoral Code and the law “On political parties”.
- The dissemination and consolidation of a new electoral culture to voters, through ongoing civic education campaigns.
- Increase the capacities and performance of commissioners of electoral commissions through qualitative, professional and periodic training.
- Increase control and transparency of election campaign funding.
- Encouraging legal reforms to improve electoral legislation.

CEC, in carrying out its functions, is assisted by the CEC administration, which consists of civil servants and support staff.

The Complaints and Sanctions Commission (CSC), located near the Central Election Commission (CEC) in Albania, is an independent body established to oversee and handle disputes, complaints, and legal challenges related to electoral processes. Its key functions typically include:

Handling Complaints: The CSC addresses complaints filed by political parties, candidates, or other stakeholders about alleged irregularities in electoral procedures, campaign activities, or voting processes.

Imposing Sanctions: If violations of electoral laws or regulations are confirmed, the CSC has the authority to impose sanctions, which may include fines, reprimands, or even the disqualification of candidates or parties from participating in elections.

Ensuring Fair Practices: The CSC ensures that elections are conducted fairly and transparently, adhering to legal frameworks and democratic standards.

Collaboration with the CEC: While the CSC is independent, it works closely with the Central Election Commission, as its decisions and actions are directly related to electoral administration.

Judicial Oversight: Decisions of the CSC can typically be appealed to higher judicial bodies, ensuring an additional layer of legal oversight and fairness.

The CSC serves as an essential part of Albania's electoral framework, promoting accountability and fairness in the process.

Election Administration Zone Commission (EAZC) is a key administrative and decision-making body within Albania's electoral system, operating at the regional level. Composition of EAZC aim to ensure a balance to maintain impartiality and trust in the electoral process.

The EAZC is responsible for managing and overseeing all electoral activities within a specific Election Administration Zone. These zones are geographic subdivisions established to facilitate the organization and implementation of elections.

EAZC is responsible for Election Preparation:

- Organizing and setting up Voting Centres within its zone.
- Supervising the logistics and distribution of voting materials (e.g., ballots, ballot boxes, etc.).

Supervision During Elections:

- Ensuring proper functioning and legal compliance at Voting Centres.
- Addressing any issues or disputes arising during the voting process.

Vote Counting:

- Receiving and verifying ballot boxes from Voting Centres.
- Supervising the vote counting process to ensure transparency and accuracy.
- Compiling and transmitting the results to the CEC.

Enforcement of Regulations:

- Monitoring the application of electoral laws within its jurisdiction.
- Resolving minor complaints or irregularities locally and escalating significant issues to higher bodies (e.g., CEC or CSC).

Collaboration:

- Working with election observers, political parties, and other stakeholders to maintain fairness and transparency.

In summary, the EAZC plays a crucial role in the effective execution of elections at the regional level in Albania, ensuring that electoral processes run smoothly, fairly, and in compliance with national laws.

1.4.2 Stakeholders

The new module will digitalize the activities of the processes where are involved the following Stakeholders:

- Central Election Commission (CEC): Primary owner and main user of the system.
- CSC/EAZC – as a beneficiary user of the system.
- General Public/voters: Denunciation from Citizens and accessing the information for transparency.
- Political Parties
- Candidates
- Observers
- Media and Civil Society Organizations: Observing and reporting.

1.5 Business processes

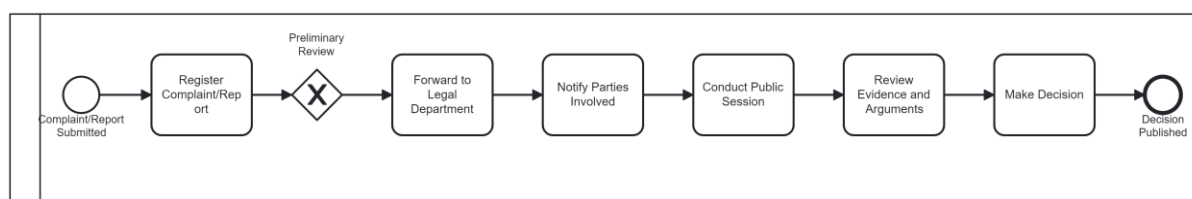
1.5.1 Existing (AS-IT- IS) processes

In Albania, the Complaints and Sanctions Commission (CSC) handles complaints related to elections, and the process is governed by the Electoral Code. Here is an overview of who can file complaints and how the process works:

- Political Parties: Parties participating in elections can file complaints if they observe or experience violations during the electoral process.

- Candidates: Individual candidates for elections have the right to complain about issues affecting their campaigns or results.
- Observers: Accredited domestic or international election observers can lodge complaints if they witness irregularities.
- Voters: In some cases, individual voters can file complaints about violations of their electoral rights or irregularities during voting or counting.

Currently, the process relies on paper-based submissions and email communication, which are time-consuming, prone to errors, and lack centralized oversight. Tracking report statuses or verifying compliance is challenging without an integrated system. A short description of the process as per regulation is below:



Submission of the complaint

- Submitted to the protocol or can also be sent via email. (In cases where it is sent by email, the administration submits it to the protocol for registration.)
- Within 8 hours of registering the complaint, the CEC notifies the EACC.
- Within 12 hours of registering the complaint, the administration of the CEC, represented by SP, conducts a session to hold a lottery for determining the rapporteur.
- The preliminary session for verifying the form and content elements of the complaint is held no later than 24 hours from the moment of its registration. (If the Complaint is incomplete, the rapporteur decides to return it for completion. The Complaint Request must be resubmitted within 24 hours.)
- The review session is held no earlier than 24 hours and no later than 48 hours from the announcement of the decision to accept the Complaint Request.

The Complaint Request must include:

- The sequential number of the complaint;
- The date and time of the complaint submission;
- The complaint subject;
- The object of the complaint;
- A list of documents attached to the complaint.

Notes:

During the electoral period, against the decision of the CEC or EZAC, the deadline to submit a complaint is 3 days from the date of the decision's announcement. Outside the electoral period, that deadline is 30 days from the date of the decision's announcement.

Complaints against the CEC's decision to approve the Summary Table of Results, a must be submitted no later than 5 days from the announcement of this decision.

Complaint against the EZAC's decision to approve the Summary Table of Results for the Electoral Zone must be submitted no later than 5 days from the announcement of this decision.

Denouncement process to the CEC

Filing the Denouncement

Submission: Denouncements can be filed electronically, in person, or through official channels provided by the CEC.

Details Required:

- Identity of the person/organization filing the denouncement.
- A detailed description of the alleged violation.
- Evidence (photos, videos, witness testimonies, documents, etc.), if available.

Review and Verification:

CEC verifies the denouncement to determine whether it falls under its jurisdiction and is backed by sufficient information. If necessary, the CEC may request additional information or evidence from the filer.

Investigation

CEC may investigate the denouncement or refer the case to relevant bodies, such as the Complaints and Sanctions Commission or law enforcement authorities, if the issue involves criminal activities.

Resolution or Referral

If the denouncement is substantiated, the CEC can take actions within its competence, such as:

- Issuing warnings or sanctions to electoral participants.
- Correcting the irregularity (e.g., annulling a result in a specific area).
- Denouncements involving criminal violations (e.g., vote-buying or intimidation) are referred to the Prosecution Office for further investigation.

Notes:

Anonymity: While many cases require the denouncer's identity, the system may allow anonymous reporting, particularly for serious threats or violations.

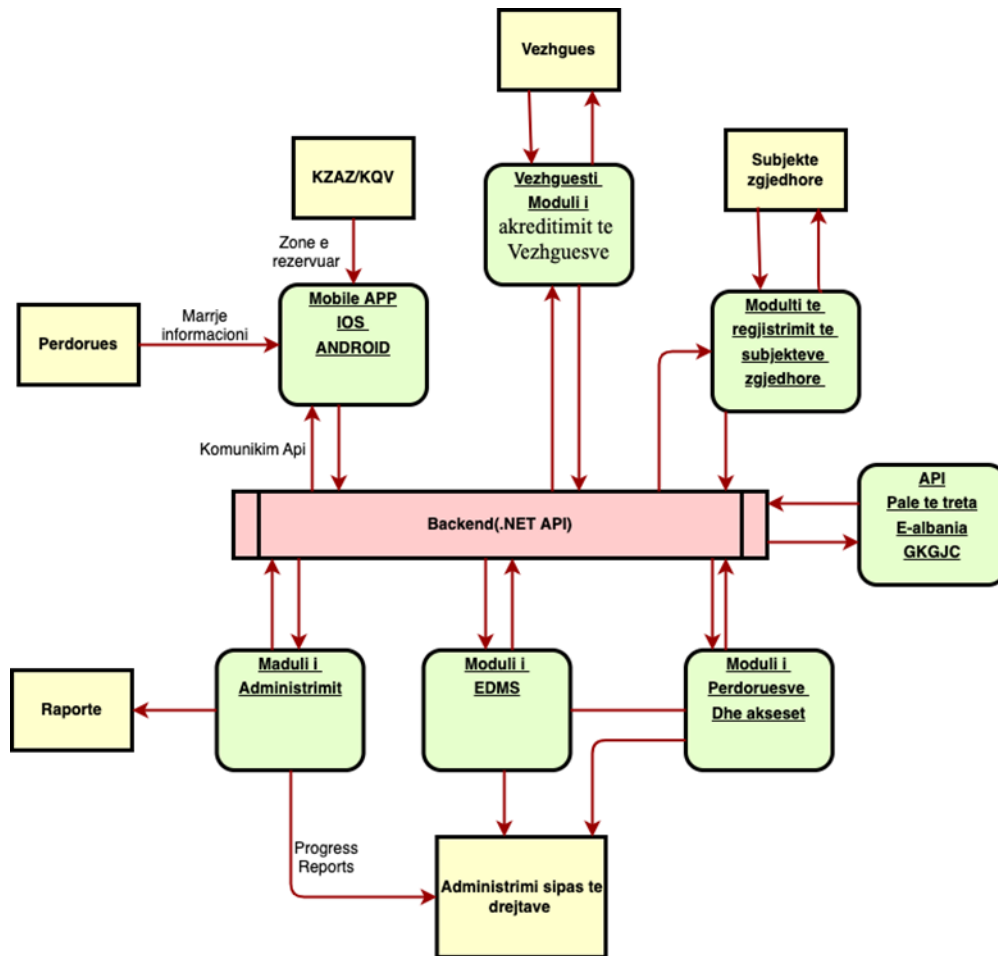
Deadline: Denouncements related to specific incidents (like vote counting or campaign violations) need to be submitted within a limited time frame to be considered valid.

Public Transparency: The CEC typically publishes decisions or actions taken in response to denouncements to uphold transparency.

This process ensures that citizens, organizations, and stakeholders have a mechanism to address concerns about the integrity of elections, contributing to a more robust democratic process.

1.5.2 CEC IT Systems:

CEC has in use existing modular ERDMS system which details are described below:



Backend (API):

Technology: .NET API 8

Description: The backend is built using .NET API 8 to create robust and secure RESTful services. It serves as the core for communicating between the database and frontend, handling key functionalities such as business logic execution, data processing, and integrations. Advanced features for security, authentication, and data management are fully leveraged, ensuring a scalable and reliable foundation for the system.

Frontend (Web Application):

Technology: React 18

Description: The frontend leverages React 18 to provide a modern, interactive, and user-friendly interface for web users. React's advanced state management features and performance improvements, such as hooks and concurrent rendering, enable seamless navigation and efficient user interactions within the application.

Database:

Technology: SQL Server 2022 Enterprise Edition

Description: SQL Server 2022 is utilized to handle all system data management requirements. This enterprise-level database system offers enhanced query performance, robust scalability, Big Data integration capabilities, and improved security measures to ensure data integrity and rapid access to information.

Mobile Application:

Technology: Flutter 3.24

Description: The mobile application is developed using Flutter 3.24, a modern cross-platform framework supporting both Android and iOS platforms. It delivers fast, responsive, and highly performant mobile interfaces, providing users with a consistent and intuitive experience across devices.

2 SOLUTION DESCRIPTION

This shall be a modular system that shall ensure efficiency, scalability, and adaptability while integrating and adhering to existing architecture and technologies.

IT systems/modules to handle complaints and denunciations in an integrated setup with the mentioned existing backend, frontend, database, and mobile architecture, that should have the following key modules and functionalities:

User Management: Manage user roles and permissions to ensure secure and appropriate access considering the following features:

- Role-based Access Control (e.g., admin, verifier, investigator, user/citizen, and observer).
- Secure user authentication (integrated with existing .NET authentication mechanisms), audit logs for user activity tracking and support for Multi-factor authentication.

Complaints and Denunciations Management: system for filing, processing, and tracking complaints and denunciation that will support the following key features:

Filing Interface: Allow users (web or mobile) to file complaints or denunciations with structured fields:

- Complainant details (optional for anonymity).
- Incident description.
- Category of complaint (e.g., campaign violation, vote tampering, etc.).
- Evidence upload (photos, videos, documents).

Workflow Automation:

- Automated assignment of complaints to relevant departments or officials.

- Notifications for status updates via email or SMS should be supported.

Complaint Tracking:

- Complainant access to view status (submitted, under review, resolved, etc.).
- Investigation notes and resolution history.
- Investigation Management that will facilitate the processing of complaints by authorized staff (e.g., CEC and CSC officials) with at least the following features:
Case allocation to investigators or teams.

Evidence Analysis Tools:

- View and organize uploaded evidence.
- Tagging and flagging of documents.
- Add internal notes and updates.
- Generate investigation reports.

Reporting and Analytics to enable data-driven decision-making and performance monitoring with the following requested features:

- Complaint trends (e.g., type, frequency, geographic distribution).
- Investigator performance metrics (e.g., resolution time, cases closed).
- Exportable reports (PDF, CSV).
- Dashboards for real-time metrics.

Integration - Connect the complaint system with existing external and internal systems considering the following features:

- Integration with the existing **.NET API 8** backend:
- Standardize API endpoints for secure communication.
- Reuse authentication, user data, and notifications features from existing systems.

Communication with external authorities:

- Law enforcement for criminal case referrals.
- Electoral bodies for results or complaint verification.
- Mobile Notification Integration:
- Use Flutter-based mobile interfaces for user notifications and updates.

Document Management Capabilities to handle storage and secure access to all documentation with the following features:

- Centralized storage for uploaded evidence and investigation documents.
- Categorized document retrieval (based on complaint, case, or complainant).
- Secure document access with logging.

System Integration recommendation references

The Successful bidder should make the necessary considerations for the best technology and approach for delivering the requested results. Meanwhile based on the existing CEC software environment the following recommendations can be made:

API-Driven Approach: Design modular API endpoints for complaint-related actions to integrate seamlessly into the .NET API 8 backend.

State Management: The new system can use **Redux** or React Query for the React 18 frontend to ensure efficient complaint tracking and updates in real-time.

Database: the new modules can leverage the SQL Server 2022 for:

- Relational data structure for complaints, complainants, and investigations.
- Implement row-level security to control data access.
- Use built-in encryption for sensitive fields (e.g., personal information).

Mobile Integration: The new system can use Flutter's local storage and push notifications should be used for offline support and real-time status updates.

Performance and Security: The modules will utilize SQL Server indexing and caching mechanisms for large datasets. Also should employ secure API keys and JWT-based authentication.

2.1 Business requirements

Future (TO BE) processes

This session contains a detailed description of the solution requested and outlines the functional requirements for the Complaint Tracking and Denunciation Module.

Bidder response	Description of how the requirements shall be met
A	Exists as a function and is already implemented with at least one client – may be presented on the client's premises
B	Exists as a function, but not implemented with any client – may be presented on the Bidder's premises
C	Function requires little modification /programming and may be realized in a set time limit
D	Function cannot be met

All the functions marked by the Bidder with A, B and C are the subjects of delivery and the Bidder must deliver these within the bid-price.

The tables show the main Business Requirements for the System, and the other tables show Non- Functional Requirements and Interface Requirements. The number of key requirements is 59.

Table 1:Business Requirements

No.	Category	Description	Required	Bidder Response
BR001	Administration and Configuration	The Module must provide administrator with tools to configure system's parameters.	R	
BR002	Archiving	The module should provide a mechanism for electronic archiving	R	
BR003	Configuration of parameters	System must let an administrator to manage quantitative parameters that are created by Law and CEC regulations	R	
BR004	Configuration of roles	System must let an administrator to create roles and define permissions on those roles. The module should support internal and external user roles.	R	
BR005	Configuration of users	System must let an administrator to configure users of the modules by creating, updating, resetting passwords and changing role membership.	R	
BR006	Password Administration	The module must support Password Encryption	R	
BR007	System Administration and Configuration	The module must provide user management capabilities for creating and updating user profiles	R	
BR008	User / Active Directory	The module should support Active Directory for authenticating its internal employees	O	
BR009	User / Authentication mechanism	System must provide a secure and reliable way for authenticating actors that interact with the system. System must provide a secure login mechanism.	R	
BR010	User / Authentication Provider and PKI	The module should be able to authenticate the users based on digital certificates issued by official PKI infrastructure of Albania	R	

BR011	User / Authorization mechanism	System must provide an authorization mechanism based on users and roles. The module must allow or deny access to different functionality of the module based on role membership. The module must support Role-based Access and Authorization. The module must allow the assignment of one or more specific roles to user account. System should provide role-based, folder-based and document level security.	R	
BR012	User / Identity Providers	The module should be able to relay on multiple identity providers by supporting claim-based authentication and authorization.	O	
BR013	User Account Management	The module must support 2-tier User Approval Process. The module must support Two-Factor User Authentications. The module must track all Login/Logout History	R	
BR014	User Account Security	The module must allow for approving, locking and unlocking of a specific user account; The modules must allow for updating user password and it should require a Strong Password as per best practices	R	
BR015	User Accounts	The module should offer the possibility for external users to apply to online for an account, and a form for them to provide the necessary justification	O	
BR016	Forms	System should provide the capability for authorized individuals to add user defined data fields, in addition to standard meta-tags.	R	

BR017	System	System should provide seamless integration between document management and web content management, and enable movement of content between systems for purpose of delivery, archiving, etc.	R	
BR018	System	System should support file compression when sending/transferring files.	R	
BR019	System	The modules should provide a single, unified storage space for all information types (files, transcripts of message board messages, emails, etc.), preferably in the form of a relational database management system (RDBMS).	R	
BR020	System	System should support the automatic generation of emails within the DMS and emailing of documents or groups of documents.	R	
BR021	Record Management	The module will support the records management process for documents. In the case of paper-based documents to be registered, they will have to be scanned before signoff or any further processing. It should function through a combination of a friendly user interfaces (UIs), form builders, and visual process modelling, so users can leverage it to produce a working application that can be used for different kind of purposes on an organization.	R	

BR022	Search	The module should provide search capabilities: all documents and other types of information stored within The module will be searchable. Search results will be security aware: users will only see documents in search results for which they have the appropriate access right (i.e. at least a “read” right). System should support search for related documents.	R	
BR023	Business Process	The modules should allow capturing process data through defined business process flow.	R	
BR024	Business Process	The module should offer the possibilities to create and administer high level business processes and sub-processes to support execution paths of the service logic flow.	R	
BR025	Business Process	The modules should support high level flows that call sub flows (exp. Selected request data from external users, trigger different processes to be executed)	R	
BR026	Document Workflow	The module should allow documents flow management capabilities through a business process flow and human workflows. The module should provide Workflow support: will provide built-in workflow support for document review and approval processes.	R	
BR027	Data	System should support automatic calculations for data within form fields. The module should support importing data from defined templates as MS word and MS excel. System should provide a method to collect and analyse form data, such as database tables. System	R	

		should provide for export of collected form data to database.		
BR028	Data analysis	The module must provide ability to collect, analyse data and apply predefined business rules.	R	
BR029	Data fields	The module must allow ability to add required fields to the data table from the gallery of available types which must include text, text area, date, date-time, integer, decimal, money, dropdowns, related fields, master-slave relations, etc.	R	
BR030	Data in doc templates	System should support the ability to merge collected data into document templates.	R	
BR031	Data processing	System should support forms processing, including the ability to extract data from boxes and lines to populate databases.	R	
BR032	Data Search	The module must provide ability to perform advanced search on case data by one or more fields, including simple text or number fields, as well as date ranges, values selected from dropdowns, etc.	R	
BR033	Data sort and search	The module must provide ability to search, sort and page through the reported data	R	
BR034	Data Validation	The module must have validation of the data input forms (or files) checks upon business rules provided by the beneficiary in order to avoid human errors.	R	

BR035	Data Validation	The module must provide ability to extend validation logic of entered data.	R	
BR036	Data visualization	The module must provide ability to show case data in the table/grid format. The module must allow system administrators and developers to customize visual tools such as Forms, Grids, Profiles and user interface of the module using online capabilities of the System.	R	
BR037	Data Web forms	The module should provide a HTML5 container to contain and load predeveloped electronic forms. System should support online form creation, publication and management. System should support the following form elements: checkboxes, radio buttons and data entry fields. The module should allow users to attach files (docs, images, media, etc) with web forms	R	
BR038	Document Generation	The module must provide ability to generate documents in multiple formats, such as MS Word (.doc), Adobe (.pdf), etc. by populating templates with "live" data from the database	R	
BR039	Document indexing	System should provide mechanisms for the identification of specific attributes of a document or database record to facilitate retrieval.	R	
BR040	Document Templates	The module must provide functionality for creating and updating templates for generating documents	R	

BR041	Files - Documents	System should support functionality- ability for system to receive documents via internet. As incoming documents are received. The module should support the ability to receive incoming documents and automatically route the document based on configurable rules. System should support drag 'n drop functionality for moving files into the repository.	R	
BR042	Files - management	System should support export of scanned images to a document repository. System should provide a mechanism for assuring that new files created from templates are saved as separate files.	R	
BR043	Files management	The module must allow input forms to have ability to upload different type of files as docs, images, media and to assign to web forms. System should support the attachment of related content items to a form record, including related documents or images.	R	
BR044	Form based documents	System should support form-based generation of documents.	R	
BR045	Templates	System should provide tools for template management, and the ability to associate workflow with specific templates.	R	
BR046	Calendar	The modules must possess a calendar for the contact list of the users. This component will allow future coordination regarding reporting timelines as per Law and regulations.	R	
BR047	Task scheduling	System should let an administrator to manage	R	

		parameters of The module like task schedule, deadlines, etc.		
BR048	Email integration	System should support email distribution of forms, integrating with CEC mail server (i.e. MS Exchange). They must support usage of registered users emails for different notification and authentication services	R	
BR049	Integration with existing Portal	The module will integrate and enhance the existing CEC portal and ease publishing of the reports.	R	
BR050	SMS gateway	The module should support integration with SMS gateway for sending notifications or (two factor) authentication services	R	
BR051	Audit	The Module should provide detailed audit-track functionality. Audit of the following actions will be provided: object creation, modification, deletion, registering the name of the user performing the action and the exact time of the action.	R	
BR052	Incident tracking	The module must contain an Incident tracking component serving as a “virtual help desk” which must allow administration of functions in relation to system incidents. The incident tracking component must include ability to control and manage incidents and errors efficiently including the possibility to update incident settings, browse incidents, browse errors, manage incidents type, review, route, assign and respond to them.	R	

BR053	Indexing	System should provide the ability to automatically assign a unique number for each document created and include this number in an automatically generated footer. This should facilitate association of hard copy/printed documents with their corresponding electronic records. System should provide a mechanism for tracking hard copy versions of electronically filed documents. System should provide a mechanism for indexing and tracking offline hard copy documents, including offline archives.	R	
BR054	Notification	The module should allow controlled access to its folder structures via the said web services technology, so that it can receive automatic notifications on changes to the contents of folders on its watch list.	R	
BR055	Secure communication	The module must support HTTPS/SSL	R	
BR056	Security Mechanism	System must provide a security mechanism that comprises authentication, authorization, and auditing.	R	
BR057	Digital Signature	The module should be able to support digital signature for the messages and documents, based on digital certificates issued by official PKI infrastructure of Albania.	R	
BR058	Reporting	The reporting component should produce statistical reports for the Categories of data captured by the declaring and reporting processes as:- Parties and candidates (Election Financing, Annual	R	

		Reports) - CEC activity Observers reporting- External Auditors reporting- CEC internal processes reporting		
BR059	Reporting	Must allow access to the data, reports or analyses based on the user profile. Data could be accessed by User interfaces. or by Web Services. Must present numeric reports or graphics and diagrams, which can be general or detailed ones. Must ensure precision in the report presentation. Reports/graphic printing and exporting functionality.	R	

2.2 Non-Functional Requirements

Table 2: Non-functional requirements

No.	Function	Requirement	Required	Bidder Response
NFR 1	Data upload	The module could offer the possibility to upload existing structured data as CEC standards.	R	
NFR 2	Web Base	The module must be web-based and accessible via intranet.	R	
NFR 3	Session lifetime	The module must provide session expiration setting. If a user is not active for a specified period, he must be automatically logged off. The period must be configurable via system parameters by the module administrator.	R	
NFR 4	Data Custody	The whole set of documents generated during the process of declaring and inspecting must be stored as per Data Protection Law requirements.	R	
NFR 5	System Availability	The module availability must be at least 99% in peak periods.	R	

NFR 6	Source Code	Source code developed in the scope of the project must be delivered in electronic format. The Source Code ownership will be passed to the CEC free from copyright.	R	
NFR 7	System	The module could be a Commercial-Off-The-Shelves (COTS) software application that provides workflow engine via easy web interface with no or little coding skills.	R	
NFR 8	Expandability.	The module is expected to cover a wider scope in the future, and to offer to its users extended access to new features and new data. Therefore, the architecture of the module shall support distributed solutions. Additionally, the module should permit technical ways to extend its provided functionality, robust SDK and enable integration with other systems providing APIs.	R	
NFR 9	Number of Documents and Records	The software should put no limits to the number of documents and records that can be archived and indexed, which should be limited only by hardware and storage size.	R	
NFR 10	Network Topology	The module should be able to work in intranet topology in a WAN, while end users will access it through secure connectivity.	R	

2.3 Interface requirements

Table 3: Interface requirements

No.	Description	Required	Bidder Response
IR 01	The module should have as an integral part a development environment equipped with the right tools for personalizing menus, objects, forms, pages and reports.	R	
IR 02	The solution must provide a professional and appealing look and feel for all Modules and sites. The final design will be validated in collaboration with CEC	R	

IR 03	User interfaces of the web Modules should be web based, intuitive and simple to use.	R	
IR 04	The supplier should provide Front-end and back-end developments of the Web Based Modules of The module to enable the creation of a simple user interface for internal and external users, based on the experience of CEC	R	
IR 05	The module must enable users to see and navigate an overall map of a site's content and structure.	R	
IR 06	The module should be accessible though all major browser (Internet Explorer, Firefox, Chrome)	R	
IR 07	The module must provide an improved mobile user experience, easily to navigate and view in touch enabled devices.	R	
IR 08	The module interfaces should be based on Responsive Web design approach and should respond to the user's behaviour and environment based on screen size, platform and orientation.	R	

2.4 User profiles

Different user profiles/roles should be created for the internal users, in accordance with their job position they work in. Main user roles are as following:

User Roles in the "Denunciations Module"

- Individual (Physical Person)/Reporter - Users who can submit denunciations through the online interface.
- Legal Entity/Reporter - Legal subjects who can also submit denunciations online.
- TIP User - Authorized CEC employee who uploads denunciations submitted to the protocol.
- Unit Users - Employees who process denunciations uploaded by TIP or the system.
- Supervisor - User responsible for assigning cases and managing the review process.

Roles in the "Electoral Compliant Module"

- Compliant/Appellant/Reporter - Individuals or legal entities who submit appeals against decisions by clicking the link sent via email or submitting the appeal in writing.
- TIP (Authorized User) - Authorized CEC employee who uploads submitted pleas and completes the data in the module.
- Appellant/Political Party/Electoral Subject - Representatives of political parties or electoral subjects who submit appeals against decisions by SEC or EAZC.
- Appellant/Individual (Physical Person) - Individuals appealing decisions made by SEC/EAZC.
- Appellant/Legal Entity - Legal entities submitting appeals against decisions made by SEC/EAZC.
- Appellant/Other - Other subjects involved in prior decisions, such as observers, NGOs, etc.

- Unit User - Employee responsible for handling and updating the status of appeals in the module.
- Supervisor - Manager responsible for overseeing and undoing actions if necessary.
- Archive User - Dedicated user managing and updating data for archived cases.

3 TECHNICAL REQUIREMENTS

3.1 Operational environment Standards

User workstations at CEC have the following characteristics:

- Operating system Microsoft Windows 10 and above;
- Web browser latest version (-2) of the following browsers Edge (for Microsoft Windows operating systems 64 bits), Mozilla Firefox, Google Chrome, Opera, Safari.

Meanwhile the external users might have a wide variety of devices and software, and because of that is important that the solution to have a responsive design.

The Bidder must list in their offer all the specific hardware and software requirements that are appropriate for the given solution, and which vary from the mentioned resources provided.

All the potential additional costs stemming from the need to order additional hardware and software components must be included in the bidding price.

The Bidder must adjust their application solution to the abovementioned resources provided by CEC, in order to ensure the normal functioning of the application and database.

Normal functioning, i.e. acceptable performances, is defined as response time of application not longer than 3 seconds when entering, changing, viewing and deleting data, and the response time of application not longer than 10 seconds for receiving summarized and periodical reports.

Bidders should consider that the existing CEC HW infrastructure might need to be redesigned based on upcoming situations. CEC could reconsider their hardware configurations based on their specific needs and the periodic changes in the volume of transactions during elections. Additionally, CEC can explore moving solutions to cloud service providers (private or public cloud), so bidders should ensure that the solution will be adaptable for cloud environments and taking into account all necessary legal restrictions.

This means that the module design will focus exclusively on the software components that are integral parts of the core system functionality. All back-office-type IT functionalities and capacities (AAA services, network services, etc.) could be provided by NAIS or third parties. This system design document will refer to these services and capacities as “granted”, but they will be listed explicitly, as a reference, so as to allow for CEC to prepare the potentially missing or incomplete system components by the time system implementation actually starts.

From IT architectural aspects, this system design focuses on designing the product with additional modules to complete the functionalities requested by CEC. While it is a well-definable, standalone application, there are many services that it needs be integrated with in order to be fully functional and reasonably secure.

To be considered important aspects as AAA-type services must be provided by the underlying back-office architecture – otherwise, the module will not function.

The module will be implemented to be fully compliant with the Albanian law on Electronic Documents (no. 10273) and the corresponding by laws.

3.2 Hardware and infrastructure requirements

In order to implement the System, CEC will provide the necessary hardware and networking infrastructure (in house, private or public cloud), which will host CEC new software.

The following server capacity will be provided by NAIS or CEC for initial installations and testing of the System.

Table 4: Hardware and infrastructure requirements

Role	Quantity	RAM	CPU	HDD
Web	2	Minimum: 32 GB Preferred: 64 GB	Minimum: 4 core @ 2.2 GHz Preferred: 8 core @ 2.2 GHz	Minimum: 2x300GB Preferred: 2x600GB
DB	2	Minimum: 32 GB Preferred: 64 GB	Minimum: 4 core @ 2.2 GHz Preferred: 8 core @ 2.2 GHz	Minimum: 2x300GB for OS Preferred: 2x300GB for OS + 2x600GB for the content

Note: The bidder should provide its estimation for the needed capacity based on their proposed technical solution and technology.

3.3 Access modes and security requirements

The module should be accessed by internal users of public administration employees and other external users through:

Internet. Web-based services (responsive design suggested) for non-sensitive information available to any user, referenced or anonymous.

Intranet. Development of web-based services; intranet and extranet applications that will be presented in the internal pages (if applicable) and other pages of local institutions, all these should be available to employees and to the staff of certain organizational units for information management purposes.

The Reporting module must support the following requirements related authentication and authorization:

- It should control user access to the module through security groups, level of rights and the hierarchy of rights.
- Users must be able to assign permissions at a variety of levels within the System, e.g. at the folder, or item levels.

- The module must enable IT to delegate the ability to assign authorization policy to trusted non-IT users.
- The solution must provide an audit trail for changes to authorization policy.
- The module must support HTTPS access.
- The module should have the possibility of logging, traceability.
- The ability to encrypt the information transmitted (thick client communicates with a server and a web browser with the server).
- The basic access should not require the installation of specific plug-ins or extensions to the web browser.

3.4 Operational Security

The module hardware will be hosted on the datacentre administered by CEC. Additionally, taking into consideration the periodicity of the election cycles in Albania, the infrastructure should be flexible and easy expandable in the peak time. In such cases CEC can consider deploying it in cloud environment (private or public) that are compliant with Albanian regulation for data protection.

3.5 Business Continuity plan (Disaster recovery)

Implementation of a disaster recovery site is not part of the current project scope and will be handled by CEC IT department based on existing rules and regulations.

3.6 Backup and Archiving

Backup of all primary system and user database content will be performed on a periodic schedule by CEC staff.

3.7 Service level: availability, performance and support

The Bidder must include in the price the maintenance of the information system with a warranty period of at least 12 months, which will secure the normal operation of the application and database. The warranty period begins with the date of acquisition (delivery and acceptance) of the information system.

Note: Bids with a warranty period shorter than 12 months will not be accepted.

If the Bidder fails to meet their obligations and deadlines stipulated in the technical specification, the Ordering Party has the right to activate the promissory note submitted as a guarantee of the completion of their obligations within the guaranteed period.

The Bidder must specify the price for the annual maintenance of the offered solution for every year following the offered warranty period for 1 year.

Upon the completion of the project, the Bidder is expected to continue to perform the following:

- After receiving a written notification from the Recipient/CEC regarding the irregular functioning of the software solution, they must come to the premises and identify the problem, fix the problem/make an intervention so the programs can function correctly, or recommend how the problems can be overcome.

- All the irregularities in the functioning of the software that impact CEC's capacity to use the module productively must be eradicated within 2 working days; more serious irregularities must be eradicated within 3 working days.
- The Bidder must expand or enhance smaller solutions, as requested by the Recipient/CEC and which are the subject of this procurement, which includes alterations of the existing and the creation of new reports, minor changes in the data entry application, modifications and viewing, and change in the data access policy. "Minor changes" are defined as engaging the supplier up to 2 days per month, with no additional charge.
- To expand and enhance their solution at the Client's request (major intervention), which are the subject of this public procurement, and to create/modify the user documentation and to offer training to all the relevant users, with additional payment.
- To perform additional training of users (whether new or current) regarding issues and areas which are specified and particularly requested by the Ordering Party, with additional payment.

3.8 System Documentation

System documentation and user documentation must be in the Albanian language.

The module documentation will include:

- Logic data model;
- Physical data model, i.e. a complete database scheme (which includes all the objects in the database);
- Functional model of the system, with a description of each function;
- Model of roles, as a method of controlling data access;
- A built design, which includes:
 - A description of the requested system environment and its establishment,
 - A description of the application system installation,

A description and detailed specification of all the necessary and performed system settings for the module to function efficiently in the production regime, which includes but is not limited to:

- all the settings on the "client" application side,
- all the settings of the client operating system
- all the settings of the server operating systems,
- all the settings of the web environment,
- all the settings of the ancillary system software,
- all the settings within the application system,
- all the settings in the database.

4 SYSTEM IMPLEMENTATION AND REALIZATION

4.1 System Schedule

The period of system implementation and realization must not be longer than 150 calendar days.

The bidder/ economic operator must detail the technical offer, including the implementation and optimization of the services.

The Bidder shall give details of their suggested methodology of implementation, as well as the most detailed plan of system realization possible with all its relevant activities, performers of activities, deadlines, and potential bottlenecks and key points. It is expected that the Supplier offers a plan of the implementation realization of the software solution in phases:

- Inception report;
- Analysis;
- Design;
- Software solution development;
- Implementation of production environment
- Implementation of testing environment;
- Testing of software solution;
- Producing the as-built documentation, project documentation and user instructions;
- Completed training of administrators and system users;
- Establishment of production environment;
- Production.

The Bidder shall also compile a **list of potential risks** that can jeopardize the project realization, as well as suggestions for their minimization/elimination.

Upon signing the contract, the Ordering Party will send the Supplier the following set of documents:

- System architecture
- Description of workflows (including the existing documentation and forms that are currently being used in CEC),
- Printed glossary of data – containing exact data sets regarding the equipment from the subject of the bid to be conducted in the new system.

It is expected that this set of documents will contribute to a faster and more effective phase of Software Solution Development Analysis.

In accordance with the characteristics, available functionalities and options for expanding the chosen software solution, and all this in agreement and collaboration with the Supplier, the Ordering party will also define in detail the new processes that will be the basis for the complete realization of the software solution.

In establishing the module environment and necessary infrastructure, CEC's appropriate technical service will play a significant role.

The period of implementation of the contract will be no longer than 150 days. Below, the graphic of the project implementation is shown, according to the respective phases:

Table 1: Project schedule

No.	Phase Description	M1	M2	M3	M4	M5
1	Design the technical solutions based on the Business and Technical Requirements indicated in Appendix II and pilot the Complaints Tracking and Denunciation module integrated with the CEC's existing systems (beta version).					
2	Develop: -Operational Modules with stakeholder access. -User Manuals for public institutions and CEC staff. -Training Sessions for end-users					
3	Provide Comprehensive Testing and Bug Fixing report					
4	Finalize Fully functional Complaints Tracking and Denunciation Platform integrated with the CEC's existing systems and post-implementation Monitoring Framework and support plans					
5	Acceptance and Warranty					

4.2 Location

The service is required in Tirana, Albania.

4.3 System Costs

Based on approximate calculations for the volume of work the cost of the system will be:

Table 2: System estimated Cost

No	Description	*Qty	*Price per unit	Value
		(days)	(Euro)	(Euro)
1				
2				

3				
4				
5				
6				
7				
System cost Total				

4.4 Bidder profile requirements

To ensure the successful completion of the project, the bidders should demonstrate their capacities and resources.

- At least 3 (three) years of experience in design and implementation of electronic/information systems.
- The bidder should have carried out over the last 3 (three) financial years, similar services at a total value no less than 40% of the project budget. The similar services should be proved by the respective documentation as specified below:
 - When similar services are carried out for state institutions, the Bidder must submit the signed contract, as well as the certificate issued by the state institution proving the successfully realization of supplies and/or,
 - When similar services are carried out for private entities, the Bidder must submit the signed contract and the corresponding sales tax invoices where the dates, amounts and quantities of the supplied goods should be written.
- The Bidder must have certificates according to the standards below:
 - ISO 9001 (or equivalent): Quality management system
 - ISO 27001 (or equivalent): Information security management system
 - ISO 20000-1 (or equivalent): IT service management system.

These certificates must be within their validity period. The certificates and different authorization that will be provided, must contain full details of the certifying organization such as telephone, fax, e-mail, website, in case the contracting authority needs to verify it.

- The economic operator must have at least three employees holding degrees in relevant fields (Electronic Sciences, IT, Computer Science, Telecommunications, etc.) and certified according to the following standards:
 - 1 employee certified in Project Management (PMP or equivalent).
 - 1 employee certified in Information Security Systems Management (CISM or equivalent).
 - 1 employee certified in Systems Testing Analysis (CSTA or equivalent).

These criteria aim to ensure that bidders / economic operators are qualified and capable of executing the procured contract. For any further clarification or additional details, please refer to the relevant procurement documentation.

5 CRITICAL CONSIDERATIONS

5.1 Assumptions

This document is prepared considering the following assumptions:

- CEC and other Actors (institutions and Individuals) take responsibility to use the system.
- CEC and other Actors prepare and approve the necessary legislation and regulation changes in order to use the System.
- All involved actors should have internet access.
- Intranet actors should access directly or through VPN.
- Users should have basic knowledge of the PC, internet, browsing and using a word processor
- Engagement of the key stakeholders in the process.
- Institutions involved are willing to use and participate in the System.
- Support by 3rd party vendors related to integration with external systems.
- All internal users will have at least an active email

5.2 Constraints

The bidders should consider any constraints identified and documented in this document and address them in their technical proposal. Examples of constraints might include:

- As a Web Based application, users must have access in internet to work in it.
- CEC implementation environment should be prepared and tested before peak usage (election period)
- Periodicity of the necessity to use the software which has high load on peak time (elections) and little or no use during the rest of the year. This cause overload of the IT staff and Infrastructure.

5.3 Risks

The purpose of risk identification and assessment is to enable avoidance or mitigation and it is essential that unacceptable risks are mitigated by senior management prior to project commencement. Beyond this, risks and threats should be continually evaluated throughout the life of the work. The bidders should consider the risks listed here, which are identified during the business requirements phase. For each risk, indicate its probability, impact and possible mitigation measures.

Probability reflects how likely a risk is to materialize and impact indicates the magnitude of exposure represented by the risk (from 1=Low to 4=High). Overall rating reflects the combination of probability and impact. By definition, unacceptable risks are almost certain to occur and will severely impact, if not prevent, completion of the initiative.

Table 3: Risks

Category	RISK	Impact	Probability	Overall gravity	Proximity	Current Mitigation	Assigned to
What type of risk this is?	RISK TITLE in capitals followed by the risk description (Risk is a specific situation in the future, which is undesirable, can be avoided or mitigated and is measurable)	Severity of the risk occurring (from 1=Low to 4=High)	Likelihood of the risk occurring (from 1=Low to 4=High)	Overall rating reflects the combination of Probability and Impact	When is the risk likely to occur (in X months)	Specific measures in place to counter the risk	The person appointed to keep an eye on the risk
Infrastructure	Server infrastructure not ready	4	2	8	2	Coordinate the projects to synchronize the timeline Or consider cloud	Project Manager
Infrastructure	SERVER ROOM CONDITIONS - Lack of the appropriate environment and conditions of the Server Room where the hardware equipment will be located.	3	2	6	1	A site survey is necessary to be done in the very beginning of the inception phase, after the contract signing between Contractor Authority and Bidder.	Project Manager, IT Staff
Participation	DISENGAGEMENT OF KEY ACTORS - such as the availability of the CEC staff, the availability of the staff of the Bidder developing the CEC software that this infrastructure will host and the availability of the Bidder staff that will implement the hardware infrastructure.	4	2	8	1-4	Organize frequent meetings, keep Minutes of Meetings for documentation reasons.	Project Manager
Stakeholders	STAKEHOLDER CONFLICTS - Disagreement between stakeholders over project issues.	4	2	8	1-4	Identify issues as soon as possible, in the very beginning when they	Project Manager, Project Team from CEC and Bidder.

						may be identified. Discuss issues immediately with all the stakeholders involved and document minutes of meetings.	
Communication	MISUNDERSTANDING - Project team misunderstands requirements.	4	2	8	1	Organize and keep track of the project initiation meeting with all the necessary stakeholders. Organize periodical meetings for the status of each phase of the project. Organize meetings for requirements gathering and discussion between stakeholders. Require the Inception Report from the Bidder after the gathering of the requirements.	Project Manager (from CEC and Bidder)
Resources	INEXPERIENCED RESOURCES - Resources who are just out of school or who are new to your industry or profession tend to make more mistakes and be less productive.	4	1	4	1-4	Careful Evaluation of the team resources qualifications and experience.	Procurement Team

6 DATA REQUIREMENTS

6.1 Data inputs

Users will interact with the module through the browser. Depending on the intended user action and selected form, the module will display to the user the necessary fields to complete.

Required fields will be marked with a red asterisk and the appropriate warning message will be shown if the field is left empty or the provided value is out of the allowed data range. The fields that are not editable by the user will be greyed out and their value should remain unmodified. Upon successful submission of the completed form user will be notified with the appropriate success message or error message in case there is an error processing the data.

6.2 Data Outputs and Reporting Requirements

Based on the data entered by the user's reports will be implemented in the module as requested in this document.

Moreover, administrators will have access to reports about visitors (visits per period, most visited content, etc) and reports about usage of the module storage (number of files, files by extension type, tot space used, etc)

The reports will be accessible by the browser and exportable in different formats as: csv, .DOCX, xlsx, pdf, etc.

6.3 User Documentation and Training Requirements

User documentation must include:

- General instructions for using the application, i.e. user interface;
- User instructions (manual) for each of the installed and used modules, i.e. functions;
- "Online help ", which is accessed directly when working with the application by pressing the F1 key.

Verification of project and user documentation and instructions is ascertained by the delivery/availability of their electronic versions (*Word, HTML and/or pdf* files), as well as by the accessibility/availability of *on-line help* with the appropriate content during application use. A written protocol will be made thereof, which will serve as proof of the completion of the Supplier's contractual obligations.

The supplier should provide the necessary trainings based on the following requirements:

- Comprehensive training sessions for end-users to ensure effective utilization of the Complaint Tracking and Denunciation Module.
- Development of user manuals to provide step-by-step guidance on using the system.
- Hands-on training workshops to familiarize users with the operational modules and stakeholder access.
- Training on troubleshooting common issues and understanding the support plans for post-implementation monitoring.
- Regular refresher courses to keep users updated on any system upgrades or changes.

Target Group

- CEC staff who will be the primary users of the Complaint Tracking and Denunciation Module.
- Stakeholders such as political parties, candidates, and observers who will interact with the system. The list will be provided by CEC
- IT personnel responsible for maintaining and supporting the system.

- Trainers who will conduct further training sessions for new users or stakeholders.

For the training verification it is necessary that the Bidder:

- develops the training program based on the requirements listed in this Business and Technical Requirements,
- completes the training of all the course trainees, ,
- performs the testing of trainees (in the conditions which the Ordering Party must establish), supervised by the consultant.

Training is verified when all the requested trainings are completed and the testing of all the trainees is carried out. A written protocol will be made, serving as proof of the completion of contractual obligations by the Supplier.

7 REGULATORY REQUIREMENTS

7.1 Privacy Requirements

The module shall guarantee data integrity, accountability and accessibility and prevent any altering, damages and unauthorized access to module data.

Access to the module shall be realized by using the latest version of TLS protocol.

The module shall guarantee full data storage and integrity by using back-up mechanisms for database and the following mechanisms: The data entered into the module may not be edited, damaged or deleted without authorization.

Any unauthorized attempt to edit data shall be logged with further possibility to be subjected to audit.

The module should log each activity related to a unique subject (e.g., personal ID number), so that there would be a central insight of who did what and when from the first opening the case to the last entered into the system.

A specific system auditor role should be implemented to prevent data alteration and manipulations. The detailed log file should be prevented from deletion and accessible only where a privileged CEC official and the Auditor person role enter both their passcode.

This should prevent the log files from being manipulated by a single person.

7.2 Audit Requirements

Specification of what the product has to do (usually retain records) to permit the required audit checks.

7.3 Legislation

The module will be implemented to be fully compliant with the Albanian law on Electronic Documents (no. 10273) and the corresponding by laws.

The module shall be compliant with CEC Legislation and regulations.

8 REPORTING AND EXPECTED DELIVERABLES

8.1 Reporting Requirements

The contractor shall submit the following reports in English in original and 1 copy:

- **The Inception Report** of a maximum of ~15 pages must be produced within 5 days from the start of implementation. In the report, the Contractor must describe e.g. initial findings, progress, any difficulties anticipated or encountered and mitigation measures.
- **The Final Report** should consist of maximum ~30 pages. The report should contain a sufficiently detailed description of the implementation phases, potential challenges, detailed analyses supporting any recommendation and follow up measures. The final report must be provided along with the relevant invoice.

The report mentioned above must be submitted to the SEI Project Officer identified in the contract.

8.2 Expected Deliverables

The table below lists the expected deliverables:

No	Delivery
1.	Inception Report
2.	Fully functional Complaint Tracking and Denunciation Module integrated with the CEC's existing systems.
3.	Operational Modules with stakeholder access.
4.	User Manuals for public institutions and CEC staff.
5.	Training Sessions for end-users.
6.	Comprehensive Testing and Bug Fixing report.
7.	Post-implementation Monitoring Framework and support plans
8.	Final Report

LIST OF APPENDICES

1. Law on Political Parties - <http://kqz.gov.al/wp-content/uploads/2020/11/Ligji-8580-per-partite-politike-ndryshimet-e-fundit-2017.pdf>
2. Electoral Code - https://kqz.gov.al/wp-content/uploads/2020/12/Kodi-Zgjedhor-2020_perditesuar_qpz.pdf