APPENDIX I

Business and Technical Requirements

for development of a software solution to bolster the functionalities of the Audit Department of the Central Election Commission of Bosnia and Herzegovina

Table of Contents

Acronyms

API	Application programming interface
CEC	Central election commission of Bosnia and Herzegovina
COE	Council of Europe
HTTPS	Hypertext transfer protocol secure
JSON	JavaScript object notation
REST	Representational state transfer
SLA	Service level agreement
SOAP	Simple object access protocol

1. Introduction

1.1 Purpose of the document

This document presents the detailed business requirements for the development of the *software solution for Audit Department of the Central Election Commission (CEC) of Bosnia and Herzegovina.* The comprehensive technical specifications for the design and functionality of the software will increase the efficiency of the CEC BiH Audit Department in conducting audits of political parties' funding.

1.2 Reference Documents

DESCRIPTION	LINK TO THE DOCUMENT
Link for information on annual financial reports	https://www.izbori.ba/?Lang=3&CategoryId=1332&Tag=539
Link for information about budget revenues	https://www.izbori.ba/?Lang=3&CategoryId=1332&Tag=537
The link for information on submitted financial reports	https://www.izbori.ba/?Lang=3&CategoryId=1263&Tag=508
The previous method of publishing financial reports	https://www.izbori.ba/?Lang=3&CategoryId=1263&Tag=507 https://www.izbori.ba/?Lang=3&CategoryId=1263&Tag=507#BrA1

2. Executive summary

The activity aims to develop a robust software solution for the Audit Department of the Central Election Commission (CEC) of Bosnia and Herzegovina to enhance the oversight of political party funding. This software solution is designed to address several key problems faced by the department, including outdated IT systems, inefficient manual processes, and the need for enhanced data security and compliance with regulatory requirements.

The primary purpose of this endeavour is to modernize the CEC's audit capabilities by introducing a new system that automates data collection, improves data accuracy, and enhances reporting functionalities. This will lead to more efficient workflows, better compliance with legal standards, and improved transparency in political party funding oversight.

Problems Addressed

1. Outdated IT Systems: The current system relies on manual data entry and paper-based reports, leading to inefficiencies and a higher risk of human error.
2. Inefficient Workflows: Manual processes are time-consuming and prevent staff from focusing on more strategic tasks.
3. Data Security: There is a need for advanced security measures to protect sensitive financial data from unauthorized access and breaches.
4. Regulatory Compliance: Existing systems are insufficient to meet new regulatory requirements for financial reporting and political party funding oversight.

Causes of the Problems

1. Technological Obsolescence: The current IT infrastructure is outdated and lacks the capabilities needed for modern data handling and reporting.
2. Manual Processes: Reliance on manual data entry and verification processes increases the likelihood of errors and inefficiencies.
3. Limited Automation: The lack of automated tools for data verification and report generation hinders operational efficiency.
4. Inadequate Security Measures: The existing systems do not offer the level of security required to protect against data breaches and ensure compliance with data protection laws.

The new software solution will address these issues by:

1. Automating Data Collection: Political parties will submit financial reports through a secure online portal, which the system will automatically validate and import into the database.
2. Streamlining Workflows: The system will reduce manual data entry, automate data verification, and allow real-time report generation, freeing up staff for more strategic tasks.
3. Enhancing Security: Advanced security measures, including data encryption and strict access controls, will protect sensitive financial information.
4. Ensuring Compliance: The system will be designed to meet all relevant regulatory requirements, ensuring comprehensive oversight of political party funding.

Expected Benefits

1. Improved Efficiency: Automation of data collection and verification will significantly reduce the time and effort required for these tasks.
2. Enhanced Accuracy: Automated processes will minimize human error, leading to more accurate and reliable financial reports.
3. Increased Transparency: Real-time and interactive reporting tools will make it easier for stakeholders to access and understand financial data.
4. Strengthened Security: Robust security features will protect sensitive data and ensure compliance with data protection laws.

Urgency

- Immediate Need: Enhancing the audit functionalities is critical for maintaining the integrity of the electoral process and public trust.
- Technological Risks: The current system may soon become unsupported, posing risks to operational continuity and security.

Consequences of Delaying the Implementation

- Increased Costs: Delays could lead to higher costs due to emergency fixes and maintaining obsolete systems.
- Operational Inefficiencies: Continued reliance on outdated technology will perpetuate inefficiencies and potential errors.
- Reputational Risk: Any failure in the audit process could damage the Commission's reputation and undermine public trust in the electoral system.

Direct Beneficiaries

- CEC's Audit Department Staff: More efficient workflows, better tools, and reduced administrative burdens.
- Political Parties: Improved oversight ensures fair competition and transparency in funding.
- Public and Stakeholders: Increased transparency, timeliness and security in political funding reports will enhance public trust.

Indirect Beneficiaries

- Other Departments: Success in this activity can encourage similar improvements across the organization.
- International Observers: Enhanced audit capabilities will improve the country's standing in international assessments of electoral integrity.

Given the critical nature of maintaining electoral integrity and the significant improvements in efficiency, security, and transparency, the development of the adequate software solutions is of high priority for the stakeholders involved. The recommendations outlined in this document align well with the business objectives of improving the work of the Audit Department, simplifying workflows, enhancing security, and replacing obsolete technology.

3. Background Information

3.1. Project scope and objectives

Business Objectives of a software solution entail the following:

1. Enhancing Audit Department's capabilities

The development of the new software aims to enhance the functionalities of the Audit Department, which oversees political party funding. By developing a more robust software solution, the Audit Department can provide more accurate, timely, and transparent information to stakeholders, including political parties, the public, and international

observers. Improved data handling and reporting capabilities will lead to more efficient responses to inquiries and better service delivery.

2. Simplifying Workflows

Current processes involve manual data entry, paper-based reports, and outdated IT systems. The new software solution will automate many of these tasks, streamline workflows, and reduce the risk of human error. This will allow staff to focus on more strategic tasks rather than routine administrative work.

3. Enhancing Security

Given the sensitive nature of political funding data, the new system will incorporate advanced security measures to protect against data breaches and ensure the integrity of financial reports. This includes secure data storage, encrypted communication, and strict access controls.

4. Replacing Obsolete Technology

The existing IT infrastructure is outdated, lacking the capabilities needed to handle modern data requirements. The new technology will introduce up-to-date technology that can support current and future needs, improving overall efficiency and scalability.

5. Piloting a New Technology

Implementing this activity can serve as a pilot for adopting new technologies within the organization. Successful implementation could pave the way for further modernization initiatives across other departments.

Timing and Consequences:

- Urgency of Improved Oversight: Enhancing the audit functionalities is critical for maintaining the integrity of the electoral process and public trust.
- Technological Obsolescence: The current system may soon become unsupported, posing risks to operational continuity and security.
- Regulatory Compliance: There are recently imposed regulatory requirements that the current system cannot adequately address.
- Consequences of Delays:
- Increased Costs: Delaying the activity could lead to higher costs due to emergency fixes and maintaining obsolete systems.
- Operational Inefficiencies: Continued reliance on outdated technology will perpetuate inefficiencies and potential errors.
- Reputational Risk: Any failure in the audit process could damage the Commission's reputation and undermine public trust in the electoral system.
- Non-implementation:
- Compliance Issues: The Commission might fail to meet regulatory standards, resulting in the loss of credibility.
- Data Security Risks: Outdated systems are more vulnerable to cyberattacks, potentially compromising sensitive data.

- Missed Opportunities: The Commission will miss the opportunity to leverage new technologies for better performance and service delivery.
- Direct Beneficiaries:
- CEC's Audit Department Staff: They will benefit from more efficient workflows, better tools, and reduced administrative burdens.
- Political Parties: Improved oversight ensures fair competition and transparency in funding.
- Public and Stakeholders: Increased transparency and security in political funding reports will enhance public trust.
- Indirect Beneficiaries:
- Other Departments: Success in this project can encourage similar improvements across the organization.
- International Observers: Enhanced audit capabilities will improve the country's standing in international assessments of electoral integrity.

The stakeholders, especially those directly involved with the CEC's Audit Department, likely consider this project a high priority due to the critical nature of their work in maintaining electoral integrity and closing the gaps for corrupt activities. Given the potential for significant improvements in efficiency, security, transparency, and corruption prevention, it is expected that the development and later use of the new software solutions for more efficient oversight of political party funding will have a significant impact on the overall oversight regime of political funding in the country.

3.2 Out of Scope

Clearly defining the scope of this activity is essential for successful project management. This section identifies elements that are considered out of scope for the development and implementation of the new software system for the Audit Department of the CEC BiH. These exclusions help to set clear boundaries and manage expectations.

Out of Scope Elements

- Extensive Data Analytics and Advanced AI Features
- Integration with Non-Critical External Systems
- Development of Mobile Applications
- Legacy System Enhancements
- End-User Hardware Upgrades
- Multilingual Support Beyond Specified Languages
- Training Beyond Initial Implementation
- Third-Party Software or Tools Not Pre-Selected

By explicitly identifying and documenting the elements that are out of scope, this activity can maintain a clear focus and allocate resources effectively to achieve its defined objectives. These exclusions help to manage stakeholder expectations and ensure that the activity stays on track,

both in terms of budget and timeline. Future phases or separate activities can address the out-of-scope elements if deemed necessary.

3.3 Presentation of the relevant directorates/departments

The implementation of the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina will significantly impact several key teams within the organization. The Audit Department will transition from manual data entry to automated data collection and verification, enhancing their ability to generate detailed compliance reports. The Oversight Group will benefit from automated monitoring tools and advanced analytics, improving their ability to detect non-compliance and analyse financial data. The IT Department will be responsible for integrating the new system with existing infrastructure, ensuring data security, and providing ongoing user support and training. Political parties will also be affected, as they will need to adapt to a new secure online portal for submitting financial reports, benefiting from automated validation checks to ensure data accuracy.

Additionally, the Oversight Group Members, who will be tasked with overseeing business operations, will have access to comprehensive audit reports and strategic tools to make informed decisions and enforce compliance. Understanding the roles of these teams ensures that the project addresses their specific needs and facilitates a smooth transition. Effective communication, training, and support will be essential to help these teams adapt to the new system and leverage its capabilities to enhance their operations and achieve the project's objectives.

3.4 Business processes

Business processes are the structured activities or tasks that organizations perform to achieve specific goals and deliver value to their customers. These processes encompass a series of steps, involving various stakeholders and systems, to ensure the smooth operation and efficiency of the organization's functions. In the context of the Audit Department of the Central Election Commission of Bosnia and Herzegovina, business processes include collecting, verifying, analysing, and reporting financial data from political parties. Understanding and documenting these processes is crucial when developing new software solutions, as it provides a clear baseline (AS IS) for identifying improvements and streamlining workflows (TO BE). This section will detail the existing business processes, highlight inefficiencies, and describe how the new system will enhance these processes, providing a framework for the subsequent functional specifications and system development.

3.4.1 Existing (AS IS) processes

The current system used by the Audit Department of the Central Election Commission of Bosnia and Herzegovina for overseeing political party funding involves a combination of manual processes and outdated IT systems. The process includes:

1. Data Collection: Financial reports from political parties are typically submitted electronically through current system.

2. Data Entry: Staff gets data from these reports which are in the existing IT system exports into Excel spreadsheets.
3. Data Verification: The entered data is cross-checked with physical documents from external sources to ensure accuracy. This verification process is time-consuming and prone to human error.
4. Report Generation: Financial reports and summaries are edited manually. This process involves extracting data from the system, organizing it, and formatting it into publishing reports.
5. Publication: Financial reports are published on the official website in static formats such as PDFs. This method limits the accessibility and usability of the data for stakeholders.

3.4.2 Future (TO BE) processes

The proposed software solution (TO BE) aims to modernize and streamline the existing processes, bringing several enhancements:

1. Automated Data Collection: Political parties will submit their financial reports through a secure online portal. The system will automatically validate and import these reports into the database, reducing manual data entry.
2. Integrated Data Management: The new system will provide a centralized database where all financial data is stored, managed, and accessed. This will ensure data consistency and integrity.
3. Automated Data Verification: The system will include automated tools for verifying the accuracy of submitted reports. These tools will cross-check the data against predefined criteria and flag any discrepancies for further review.
4. Real-time Reporting: The system will allow for real-time generation of financial reports. Users will be able to create customized reports on demand, with the data being pulled directly from the centralized database.
5. Interactive Publication: Financial reports will be published in an interactive format on the website. Stakeholders will be able to search, filter, and analyse the data directly through the online interface, enhancing transparency and usability.

Value Addition

The new system will provide significant value by:

- Reducing Manual Work: Automation of data collection and verification will free up staff to focus on more strategic tasks.
- Improving Accuracy: Automated processes reduce the risk of human error, leading to more accurate financial reports.
- Enhancing Transparency: Interactive and real-time reporting tools will make it easier for stakeholders to access and understand financial data.
- Strengthening Security: A modern IT system with advanced security features will protect sensitive financial data from unauthorized access and breaches.

Functional Specifications Basis

The detailed description of the current and future business processes will serve as a foundation for creating the functional specifications. These specifications will outline the requirements for the new software system, ensuring it meets the needs of the Audit Department and enhances its capabilities.

This summary of the business processes and the transition from the current system to the proposed system provides a clear reference for understanding the improvements and value that the new software solution will bring to the Audit Department of the Central Election Commission of Bosnia and Herzegovina.

For detailed information on the current system and additional context, please refer to the provided documents and links:

1. Annual Financial Reports Information
2. Budget Revenue Information
3. Submitted Financial Reports Information
4. Previous Method of Publishing Financial Reports

3.5 Identified stakeholders, users, roles & responsibilities

User Roles

1. External Users

- Political Parties and Independent Candidates: These users are responsible for entering financial data into the system. Each political party has designated representatives who handle this task.

2. Internal Users

- Audit Department Staff: These users are responsible for verifying and analysing the data submitted by political parties. They ensure compliance with regulations and prepare reports.
- Oversight Group Members (NB: to be defined internally by the CEC BiH): These users review the audit findings and provide oversight. They use the system to access detailed financial data and reports.

3. System Administrators

- IT Administrators: These users are responsible for maintaining the system, ensuring it operates smoothly, managing user access, and addressing technical issues.

Tasks and Relationships

Political Parties

- Task 1: Data Entry

- Enter financial data into the system through a secure portal.
- Validate the data before submission to ensure accuracy and completeness.

- Task 2: Submission

- Submit the data for review by the Audit Department.

- Task 3: Corrections and Updates

- Make necessary corrections and updates if the data is flagged for errors or discrepancies.

CEC's Audit Department Staff

- Task 1: Data Review

- Review submitted financial data for accuracy and compliance.
- Use automated tools to cross-check data and identify discrepancies.

- Task 2: Data Analysis

- Analyse the financial data to prepare audit reports.
- Generate insights and summaries for Oversight Group members.

- Task 3: Report Generation

- Create detailed financial reports for internal use and public dissemination.
- Ensure reports meet regulatory standards and are formatted correctly.

CEC's Oversight Group Members

- Task 1: Report Review

- Access and review detailed financial reports prepared by the Audit Department.
- Provide feedback and request additional information if needed.

- Task 2: Oversight

- Monitor the overall financial health and compliance of political parties.
- Use the system to make informed decisions and recommendations.

CEC's IT Administrators

- Task 1: System Maintenance

- Ensure the system is operational and secure.
- Perform regular updates and backups.
- Task 2: User Management
- Manage user accounts and access permissions.
- Provide technical support to users.

Workflow Diagrams

CEC Pre-Election, Post-Election, and Pre-Campaign Workflow

1. Political Parties

- Compile and submit financial reports.
- Ensure all transactions for the month are accounted for and validated.
- Automatic generation of confirmation after entering all mandatory documents into the system.

2. CEC's Audit Department Staff

- Conduct a thorough review of reports.
- Generate reports for internal review.
- Generate summary reports and prepare for Oversight Group review.

3. CEC's Oversight Group Members

- Review summary reports.
- Provide feedback and request additional data if necessary.

4. CEC's IT Administrators

- Perform system maintenance and backups.
- Review system logs for any security issues or anomalies.

Annual Workflow

1. Political Parties

- Prepare and submit annual financial statements.
- Ensure all yearly transactions are accurate and complete.
- Automatic generation of confirmation after entering all mandatory documents into the system.

2. CEC's Audit Department Staff

- Perform an in-depth review of annual statements.
- Generate reports for internal review.
- Generate comprehensive annual audit reports.

3. CEC's Oversight Group Members

- Review annual audit reports.
- Provide strategic oversight and recommendations.

4. CEC's IT Administrators

- Conduct annual system audits.
- Implement any necessary system upgrades or improvements.

Hand-offs and Task Relationships

1. Data Submission

- Political Parties submit data, which is then reviewed by CEC's Audit Department Staff.
- Any corrections requested by CEC Audit Department Staff are addressed by Political Parties.

2. Report Preparation

- CEC Audit Department Staff prepare reports based on reviewed data.
- Reports are handed off to CEC Oversight Group Members for oversight.

3. System Management

- CEC IT Administrators manage and support the entire workflow, ensuring system stability and security.

By clearly defining user roles, tasks, and workflows, we ensure that the system meets all business objectives and user requirements. This approach helps prevent missed requirements and facilitates a smoother implementation and operation of the new system.

3.6 Interaction with other systems

The new software system for the CEC Audit Department of the Central Election Commission of Bosnia and Herzegovina will interact with various existing systems both within and outside the Commission. This section details these interactions and provides a diagram to visualize the relationships between the systems and the information flow.

Internal Systems Interactions (Sub-systems)

- e-Izbori System

- Interaction: Direct integration with the e-Izbori system.
- Information Passed:
  - Financial data submitted by political parties.
  - Verification and validation status of financial reports.
  - Audit findings and reports.
- Responsibilities:
  - The new system will extract relevant financial data from e-Izbori for auditing purposes.
  - Ensure data consistency and integrity between both systems.

External Systems Interactions (direct connection with external systems and capability of importing data from External Systems via offline Excel form table)

- Porezna Uprava (Tax Administration)

  - Interaction: Integration with the Tax Administration's system.
  - Information Passed:
    - Financial transactions and tax-related data of political parties.
    - Compliance and discrepancy reports.
  - Responsibilities:
    - The new system will send and receive data to ensure compliance with tax regulations.
    - Facilitate cross-verification of financial data for accuracy.

- Izvršna Vlast (Executive Authority)

  - Interaction: Integration with the Executive Authority's system.
  - Information Passed:
    - Audit summaries and compliance reports.
    - Notifications regarding significant discrepancies or compliance issues.
  - Responsibilities:
    - Provide oversight authorities with timely and accurate audit information.
    - Ensure that the Executive Authority is informed of any potential issues affecting electoral integrity.

- Banks

  - Interaction: Integration with Central Bank of Bosnia and Herzegovina and commercial banks in Bosnia and Herzegovina.
  - Information Passed:
    - Verification of the transaction account numbers of political parties from Central Bank.
    - API and manual upload of data from commercial banks facilitating secure and efficient data retrieval, ensuring that all relevant financial information is available for audit and compliance purposes.
  - Responsibilities:
    - Ensuring that all financial transactions reported by political parties are linked to verified accounts, enhancing the accuracy and reliability of financial data.
    - This integration and data access approach will streamline financial data management and enhance the effectiveness of the Audit Department's oversight functions.

Verbal Description of Interactions

- Internal System (e-Izbori)

The new audit system will directly integrate with the e-Izbori system, which is the main electoral database. This integration will allow the new system to access detailed financial submissions made by political parties. The audit system will validate this data, cross-check it against other sources, and flag any inconsistencies. This integration ensures that all financial data used for auditing is current and accurate.

- External Systems (Porezna Uprava and Izvršna Vlast)

The new system will also interface with external systems such as the Tax Administration (Porezna Uprava) and the Executive Authority (Izvršna Vlast). Through its connection with the Tax Administration, the audit system will facilitate the exchange of tax-related information, ensuring that political parties comply with tax regulations. This exchange is crucial for verifying the legitimacy of financial transactions reported by political parties.

Moreover, the integration with the Executive Authority's system will ensure that audit findings and compliance reports are communicated to oversight bodies. This connection is essential for maintaining transparency and ensuring that any issues related to political party funding are promptly addressed.

By integrating with both internal and external systems, the new software solution will enhance the CEC's Audit Department's ability to oversee political party funding effectively. The interactions with the e-Izbori system ensure that all financial data is accurately collected and verified, while the connections with the Tax Administration and Executive Authority facilitate compliance and oversight. This comprehensive integration supports the overall goal of maintaining the integrity and transparency of the electoral process in Bosnia and Herzegovina.

These detailed interactions and responsibilities will be essential for the functional specification phase, ensuring that all necessary requirements are captured and addressed.

3.7 Replacement of existing / older systems

Replacing the existing system with the new software solution for the CEC Audit Department involves several critical steps to ensure a smooth transition. This section outlines the special actions required for switching from the old system to the new one, focusing particularly on the migration of the database.

Summary of Actions

1. Assessment and Planning

- Conduct a thorough assessment of the existing system to understand its structure, data formats, and dependencies.
- Develop a detailed migration plan, including timelines, resource allocation, and risk management strategies.

2. Data Preparation

- Clean and validate the existing data to ensure accuracy and consistency before migration.
- Identify and resolve any data quality issues, such as duplicates, incomplete records, and inconsistencies.

3. System Setup and Configuration

- Install and configure the new software system on the designated servers or cloud infrastructure.
- Set up necessary integrations with e-Izbori, Porezna Uprava, and Izvršna Vlast.

4. Data Migration

- Export data from the old system in a format compatible with the new system.
- Import the data into the new system, ensuring it is correctly mapped to the new database schema.
- Conduct a thorough data validation to confirm that the migration was successful, and all data is accurate and complete.

5. Testing and Validation

- Perform comprehensive testing of the new system to ensure it meets all functional and performance requirements.
- Validate the data integrity and system functionality through user acceptance testing (UAT) involving key stakeholders.

6. User Training and Support

- Provide training sessions for all users, including Audit Department Staff, Oversight Group Members, and IT Administrators. Training for Political Parties will be explored as well.
- Develop user manuals and provide ongoing support to address any issues during the transition period.

7. Switch-over and Monitoring

- Schedule the switch-over to minimize disruption to ongoing operations.
- Monitor the system closely during the initial period after the switch-over to quickly address any issues that arise.

Detailed Actions for Database Migration

1. Step 1: Assessment and Planning

- Assess Current Database: Analyse the existing database to understand its structure, data types, relationships, and dependencies. Document this information thoroughly.
- Develop Migration Plan: Create a detailed plan outlining each step of the migration process, including timelines, resource allocation, risk assessment, and mitigation strategies.

2. Step 2: Data Preparation

- Data Cleaning: Clean the existing data by removing duplicates, correcting errors, and standardizing formats.

- Data Validation: Validate the data to ensure it is complete and accurate. This may involve cross-referencing with other sources or manually verifying critical data points.

3. Step 3: System Setup and Configuration

- Install New System: Set up the new software system on the designated infrastructure, ensuring all necessary components and dependencies are installed.
- Configure Integrations: Establish connections with e-Izbori, Porezna Uprava, and Izvršna Vlast to enable seamless data exchange.

4. Step 4: Data Migration

- Data Export: Export data from the existing system in a format that can be imported into the new system (e.g., CSV, XML, JSON).
- Data Mapping: Map the exported data to the new database schema, ensuring all fields are correctly aligned.
- Data Import: Import the data into the new system, using automated tools where possible to streamline the process.
- Data Validation: Conduct a thorough validation to ensure all data has been accurately migrated and is complete.

5. Step 5: Testing and Validation

- System Testing: Perform functional, performance, and security testing to ensure the new system meets all requirements.
- User Acceptance Testing (UAT): Involve end-users in testing to validate that the system meets their needs and expectations.

6. Step 6: User Training and Support

- Training Sessions: Conduct training sessions for all user roles, covering system functionality, new workflows, and best practices.
- User Manuals: Develop comprehensive user manuals and reference guides to assist users in navigating the new system.
- Ongoing Support: Provide support during the transition period to address any issues and ensure a smooth adoption.

7. Step 7: Switch-over and Monitoring

- Schedule Switch-over: Plan the switch-over to occur during a low-activity period to minimize disruption.
- Monitor System: Closely monitor the system during the initial days following the switch-over to quickly identify and resolve any issues.

The migration to the new system involves detailed planning and execution to ensure a smooth transition. By following these steps, we can minimize disruption, ensure data integrity, and provide a seamless experience for all users and stakeholders. This plan serves as the foundation for the successful implementation of the new software solution, enhancing the capabilities and efficiency of the Audit Department.

3.8 Production rollout considerations

The production rollout strategy outlines the steps necessary to deploy the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina. This includes detailed plans for populating the system data, managing data and transaction volumes, and ensuring a smooth transition to the new system.

Rollout Phases

1. Preparation Phase

- Finalize the migration plan and ensure all stakeholders are informed of the rollout schedule.
- Conduct a final review of the new system to confirm it meets all functional and performance requirements.
- Prepare the initial dataset for migration, ensuring it is cleaned, validated, and ready for import.

2. Pilot Phase

- Deploy the new system in a controlled environment with a limited number of users (e.g., a subset of the CEC Audit Department staff).
- Monitor system performance and user feedback closely to identify any issues.
- Address any problems identified during the pilot phase and make necessary adjustments.

3. Staggered Rollout Phase

- Gradually expand the deployment to include all users in the CEC Audit Department, followed by other internal users (Oversight Group Members).
- Continue monitoring system performance and user feedback, providing support as needed.
- Ensure that each group of users is fully trained and comfortable with the new system before moving to the next group.

4. Full Deployment Phase

- Once the staggered rollout is successful, proceed with full deployment to all external users (Political Parties) and finalize the integration with external systems (Porezna Uprava and Izvršna Vlast).
- Conduct a final validation to ensure all data and functionalities are working as expected.

Initial Data Population

1. Data Extraction

- Extract existing data from the current system, ensuring it is in a compatible format for the new system.

- Perform data cleaning to remove any duplicates, errors, and inconsistencies.

2. Data Transformation

- Transform the data to fit the new database schema, mapping old fields to new ones.
- Validate the transformed data to ensure accuracy and completeness.

3. Data Loading

- Import the transformed data into the new system using automated tools to streamline the process.
- Conduct a thorough validation of the imported data to confirm it is accurate and complete.

4. Post-Load Verification

- Perform a comprehensive check to verify that all data has been correctly imported and is accessible in the new system.
- Resolve any discrepancies identified during the verification process.

Expected Data Volume

- Historical Data: The initial data load will include all historical financial data submitted by political parties. This data will be significant in volume but manageable with the new system's capabilities.
- Current Data: Ongoing financial data submissions will continue, adding to the database regularly.

Expected Transaction Volume

- Daily Transactions: The system will handle daily data submissions from political parties, averaging a few hundred transactions per day.
- Annual Transactions: Annual financial statements will represent the highest volume of transactions, requiring robust system performance during peak periods.

Monitoring and Support

- Performance Monitoring: Implement real-time monitoring tools to track system performance, identifying and addressing any issues promptly.
- User Support: Provide a dedicated support team to assist users during the rollout, offering training, troubleshooting, and guidance as needed. The software solution will need to include an automatic help dictionary feature that provides context-sensitive assistance for up to 8 key input forms for end customers.
- Feedback Mechanism: Establish a feedback mechanism for users to report any issues or suggest improvements, ensuring continuous system enhancement.

The production rollout strategy is designed to ensure a smooth and successful transition to the new software system. By following a phased rollout approach, carefully populating the system with initial data, and managing data and transaction volumes, we can minimize disruption

and maximize the benefits of the new system for all users and stakeholders. This comprehensive plan will facilitate a seamless adoption of the new technology, enhancing the Audit Department's capabilities and efficiency.

3.9 Method of requirements capture used

To complete the Business Requirements Document (BRD), a combination of stakeholder interviews, document analysis, and workflow observations were conducted. Key stakeholders, including CEC Audit Department staff and IT administrators, were interviewed to gather insights into current processes, challenges, and needs. Existing documentation and systems were analysed to understand the current state (AS IS) and identify areas for improvement. Workflow observations were conducted to capture detailed process flows and user interactions with the existing system. This multi-method approach ensured a comprehensive understanding of the business requirements, leading to the development of a robust and relevant BRD for the new software solution.

4. Business Requirements

Business requirements are the critical foundation for any successful project, outlining the essential needs and expectations of the stakeholders. These requirements define what the system must achieve to support the organization's goals and improve its processes. In the context of the Audit Department of the Central Election Commission of Bosnia and Herzegovina, business requirements encompass the functionalities, capabilities, and constraints necessary for developing a software solution that enhances audit operations and political party funding oversight. Clear and well-defined business requirements ensure that the new system addresses current challenges, meets user needs, and supports strategic objectives, providing a roadmap for effective development and implementation.

Copyright and rights of exploitation of developed solution

In accordance with the provisions detailed in the contract, CEC acquires ownership rights over all delivered documentation in all forms, over the source code, over the executable versions of the software, over design models, and over all materials generated through engagement on the requested activities (Copyright).

CEC is the holder of copyright property rights and other intellectual property rights on works and other products, i.e., creations protected by intellectual property rights, that are produced using the services subject to this procurement, unless it has already, by virtue of the law, become the holder of the said rights.

In terms of the aforementioned, upon delivery of the procurement items from the Contractor, CEC acquires exclusive, substantively, temporally, and spatially unlimited rights to exploit copyright and other intellectual property rights on creations that are subject to the System, all in accordance with regulations governing the protection of intellectual property.

CEC is authorized to freely transfer the aforementioned rights without any restrictions. The Contractor, author, or third party is excluded from any exploitation of these rights.

All documentation created as part of the project, including user manuals, technical specifications, installation and operation guides, training materials, known errors and workarounds, and any other relevant documents, will be fully owned by the beneficiary, the Central Election Commission of Bosnia and Herzegovina. This ensures that CEC retains complete control and access over all instructional and operational materials related to the new software system. The ownership allows CEC to update, distribute, and utilize the documentation as needed to support ongoing operations, training, and system maintenance. By having ownership of these documents, CEC can ensure continuity, accuracy, and relevance of information, adapting the materials to evolving requirements and facilitating a seamless transition to any future system enhancements or changes.

3.3 Detailed Business Requirements

- Territorial Codebook (Šifrarnik)

  - Requirement: Maintain a comprehensive and updated territorial codebook for managing regions and associated data.
  - Details: The system must allow for easy updates and historical data preservation to track changes over time.

- Data Modification

  - Requirement: Implement a system that preserves historical data when changes are made.
  - Details: Ensure that any updates to current data do not overwrite historical records but rather create a new version of the data.

- Form and Report Publication

  - Requirement: Link forms and reports directly to the website for publication.
  - Details: Enable automatic generation of reports from submitted data and ensure they are formatted correctly for web publication.

- Password Management

  - Requirement: Provide a secure and user-friendly password change functionality.
  - Details: Ensure users can easily change their passwords and implement strong security measures to protect user accounts.

- Automated Statistics Creation

  - Requirement: Automate the creation of statistical reports.
  - Details: Include tools for generating various statistics from the data, allowing users to customize and generate reports as needed.

- Auditor Reports

  - Requirement: Facilitate the generation and management of auditor reports.

- Details: Ensure that the system can generate detailed auditor reports and allow users to upload and manage these reports efficiently.

- Uploading Auditor Reports

- Requirement: Provide functionality for uploading auditor reports.
- Details: Ensure users can easily upload auditor reports, with validation to ensure data integrity.

- Spending Plans for Parties

- Requirement: Compare spending plans for political parties against actual spending.
- Details: Allow automatically comparing plans of expenditure with actual spending data, highlighting discrepancies.

- User Roles

- Requirement: Support three levels of users with different permissions:
  - External User: General data entry and basic access.
  - CEC Internal User: Management and review of data.
  - CEC Oversight Group Member: Full system access and management.
  - CEC IT Administrator: Full access maintaining the system.
- Details: Ensure role-based access control to secure data and functionalities appropriately.

- Compliance for Political Parties

- Requirement: Ensure political parties publish their financial data on their websites.
- Details: Provide tools and reminders to help political parties comply with this requirement.

- Automatic Letter Generation

- Requirement: Automatically generate and send letters from the system.
- Details: Define triggers for creating and sending letters, ensuring customization and timely dispatch.

- Multilingual Support

- Requirement: Support Bosnian, Croatian, and Serbian (Cyrillic) languages.
- Details: Ensure that the application is fully functional in all three languages, including data entry and interface.

- Data Entry and Translation

- Requirement: Translate data entries as needed.
- Details: Implement translation functionalities to ensure data entered in one language is accurately translated into the other supported languages.

Workflow Diagram

- Political Parties -> Data Entry -> Automated Data Validation -> Historical Data Preservation -> Enhanced Report Generation -> Seamless Report Publication
- Political Parties -> Create Spending Plans
- Administrator users -> Compare spending plans with actual spending -> Analysis of differences
- Internal Users -> Review Data -> Generate Auditor Reports -> Upload Auditor Reports
- System -> Automated Statistics Creation -> Multilingual Support -> Automatic Letter Generation

For each automation implemented in the new system, it is essential to include the capability for CEC internal users to modify any necessary parameters or data. This flexibility ensures that internal users can make adjustments to accommodate changes in regulations, correct errors, or update information without requiring extensive technical intervention. By providing this functionality, the system will remain adaptable and responsive to the evolving needs of the CEC Audit Department, enhancing overall efficiency and accuracy.

By transitioning from the current system to the proposed system, the Audit Department of the Central Election Commission of Bosnia and Herzegovina will experience significant improvements in efficiency, accuracy, and transparency. The new system will streamline workflows, enhance data management, and provide robust tools to support the Department's critical functions. The detailed description of the existing and future business processes will serve as a foundation for developing the functional specifications and ensuring the successful implementation of the new software solution.

Software solution requirements to bolster the functionalities of the Audit Department of the Central Election Commission of Bosnia and Herzegovina and the oversight of political party funding in the country have been grouped into the following two tables. The first table shows the general requirements for the software solution (hereinafter SOLUTION), while the second table shows the specific or special system requirements.

The Bidder shall commit to every function/requirement in the given tables of this document and enclose the completed tables in their Bid.

The required functions/requirements marked with the letter “R” must be met. The requirements/functions that are optional, but desirable, are marked with the letter “O”. In the column “Bidder response”, the Bidder must state how the function/requirement will be met, by using the following marking system:

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 Bidder must enclose a functional specification in their Bid, i.e. a description of the bid software solution, and other relevant accompanying documentation that describes the bid SOLUTION.

The total number of General and Functional requirements is 74, majority of which are required.

4.1.1 General requirements

The requirements for the software solution to enhance the functionalities of the Audit Department of the Central Election Commission (CEC) of Bosnia and Herzegovina have been grouped into two categories: Required (R) and Optional (O). These requirements are based on the analysis of the current system and the needed enhancements for the new system, focusing on semi-automatic and automatic processes and reports.

Table 1

Reference number	Functional requirements	Required / optional	Bidder response (A-D)
GR01	Automate data collection from political parties through a secure online portal.	R	
GR02	Validate submitted data automatically to ensure accuracy and completeness.	R	
GR03	Give users the advantage of processing information from more than one user at the same time and to access the information wherever it is possible over the internet.	R	
GR04	Integrate with the Central Bank of Bosnia and Herzegovina for transaction account verification. Integration with additional non-critical external systems. Integration with external systems (Tax Administration).	O	

	Integration with external systems (Executive Authority).		
GR05	No direct cooperation with commercial banks; use API for data access when necessary.	O	
GR06	Retrieve transaction account statements via Central Bank's API.	O	
GR07	External users, or groups of users, will submit to an authenticating process depending on their level of authorization or clearance; the process will grant access to the SOLUTION and specify which information may be viewed, created or edited, and which services may be used, with read only, read & write, or administrator rights.	R	
GR08	Centralized database for storing, managing, and accessing all financial data.	R	
GR09	Automated tools for data verification, flagging discrepancies for review.	R	
GR10	Real-time generation of financial reports, customizable on demand. Interactive publication of financial reports on the website, enabling search and filter functionalities. Automatic generation of reports from submitted data and ensuring correctly formatted reports for web publication. Ensure that the system can generate detailed auditor reports and allow users to upload and manage these reports efficiently and also upload auditor reports.	R	
GR11	Advanced security measures, including encryption and strict access controls.	R	
GR12	Compliance with all relevant regulatory requirements.	R	
GR13	Role-based access control for different user types (external users, internal users, administrators).	R	
GR14	Training and support for all user roles, including "Train the Trainer" programs.	R	

GR15	Regular backups and disaster recovery plan to ensure data availability and integrity.	R	
GR16	Possibility to index and make available in search results all content that is requested by beneficiary.	R	
GR17	Support automation of processes and should structure workflows based on organizational structure. Search results must be able to be further filtered, so that users can manipulate a search result set to find items of high value. Provide content indexing and Searching capabilities, fast and easy to use.	R	
GR18	Facilitate work management for the whole organization unit and it must provide user management, security, role management, audit and identification functionalities, as well as communication tools management functionalities.	R	
GR19	Detailed audit logs of all data entries, modifications, and accesses.	R	
GR20	Secure data import from CSV files provided by the Central Bank BiH.	R	
GR21	Advanced data analytics and AI-driven insights for deeper financial analysis.	O	
GR22	Extensive data cleansing to address all historical data issues.	O	
GR23	Custom reporting for non-standard requirements.	O	
GR24	Integration with internal resources, e-Izbori system.	R	
GR25	All content in the SOLUTION must be able to be searchable.	R	
GR26	Offer document versioning management.	O	
GR27	Provide an improved mobile user experience, easily to navigate and view in touch enabled devices (responsive design or dedicated app).	R	

GR28	Data migration from old system to new SOLUTION.	R	
GR29	Support drag and drop functionality for documents, photos and other types of files that are uploaded into the system. (virus sanitization of uploaded document is mandatory).	R	
GR30	Support functionalities for organizing content and routing of documents based on metadata.	O	
GR31	It should support application of content retention policies in order classify and preserve information according to institution policies and document characteristics (as per latest General data protection regulation (GDPR) policies.	R	
GR32	Maintain a comprehensive and updated territorial codebook for managing regions and associated data.	R	
GR33	Offer the possibility to monitor user traffic on public and internal site.	R	
GR34	Offer the possibility to recover content that may be accidentally deleted by the users.	R	
GR35	Offer a mechanism for alerting users on different events (such as document modification, etc.) on which the users may subscribe.	R	
GR36	Enable users to upload, store, manage, share, and ultimately dispose of large documents.	R	
GR37	Ensure multi-language support (Bosnian/Croatian/Serbian).	R	
GR38	Ensure multi-language support (English).	O	
GR39	Ensure that any updates to current data do not overwrite historical records but rather create a new version of the data.	R	
GR40	Ensure users can easily change their passwords, and implement strong security measures to protect user accounts	R	
GR41	Allow administrative access to create spending plans and automatically compare them with actual spending data, highlighting discrepancies.	R	

GR42	The software solution will need to include an automatic help dictionary feature that provides context-sensitive assistance for up to 8 key input forms for end customers. This feature ensures that users can quickly access relevant information and guidance directly within the forms, enhancing their ease of use and reducing the need for external support.	R	
GR43	Provide tools and reminders to help political parties comply with publishing their financial data on their websites.	R	
GR44	Implement translation functionalities to ensure data entered in one language is accurately translated into the other supported languages.	R	
GR45	The SOLUTION must allow for easy updates and historical data preservation to track changes over time.	R	

4.1.2 Specific requirements

Table 2

Reference number	Functional requirements	Required/ optional	Bidder response (A-D)
FR01	The proposed SOLUTION can be developed for the project needs. SOLUTION shall be open for integration with future systems.	R	
FR02	Communication with the SOLUTION should be secured via SSL.	R	
FR03	The proposed SOLUTION should be able to support additional external identity providers through SAML for future development.	R	
FR04	In order to prevent loss of data, the SOLUTION should offer data protection services.	R	
FR05	Virus sanitization of uploaded document is mandatory.	R	
FR06	The SOLUTION must provide the ability to backup and restore information.	R	

FR07	The SOLUTION must provide ability to have backup versioning with several key differences.	R	
FR08	The SOLUTION should control user access to the SOLUTION through security groups, level of rights and the hierarchy of rights.	R	
FR09	The SOLUTION Users must be able to assign permissions at a variety of levels within the SOLUTION, e.g. at the folder, or item levels within the boundaries of their personal workspace. SOLUTION Administrators shall be able to configure general set of permission policies on SOLUTION Level.	R	
FR10	The SOLUTION must enable IT to delegate the ability to assign authorization policy to trusted non-IT users.	R	
FR11	The SOLUTION must provide an audit trail for changes to authorization policy.	R	
FR12	The SOLUTION must provide auditing functions to track which user has performed what action on the libraries, documents, lists, etc.	R	
FR13	The SOLUTION must provide a professional and appealing look and feel for all sites. The final design will be validated by CEC in collaboration with COE.	R	
FR14	User interface should be web based, intuitive and simple to use.	R	
FR15	The SOLUTION must enable users to see and navigate an overall map of a site's content and structure.	R	
FR16	The SOLUTION should be accessible though all major browser (Edge, Internet Explorer, Firefox, Chrome, etc).	R	
FR17	It should support at least the following file types: .doc, .docx, .pdf, .ppt, .txt, .xls, .xml.	R	
FR18	The SOLUTION must be compatible with Microsoft Office package that beneficiaries are using (2013 and new versions).	R	
FR19	The database should support installation in high availability/cluster mode.	R	

FR20	The database should offer functionalities for data encryption.	R	
FR21	The database should support auditing functionalities.	R	
FR22	The SOLUTION must be compatible with a virtualized operation.	R	
FR23	The SOLUTION must support HTTPS access.	R	
FR24	The SOLUTION must support SSO (single sign-on).	R	
FR25	The SOLUTION should have the possibility of logging, traceability.	R	
FR26	The SOLUTION should have the ability to encrypt the information transmitted (thick client communicates with a server and a web browser with the server).	R	
FR27	The basic access should not require the installation of specific plug-ins or extensions to the web browser.	R	
FR28	Every Source code developed in the scope of the project must be delivered in electronic format as well as the content. The Source Code ownership will be passed to the COE free from copyright and later given to the beneficiary, CEC.	R	
FR29	Load distribution between servers will be managed using a Load Balancer component. The contractor is required to implement redundant software load balancing using open-source components, distributed across separate CEC servers. This solution should not require additional licenses or costs and should utilize existing CEC resources where possible.	R	

These requirements ensure that the new software solution will provide comprehensive support for the Audit Department's needs, enhancing efficiency, accuracy, security, and compliance. By automating data collection, validation, and reporting processes, the system will streamline workflows and reduce the risk of human error. Advanced security measures and regulatory compliance features will protect sensitive financial data, while interactive reporting and real-time data access will improve transparency and usability for all stakeholders. Optional features such as advanced analytics and mobile access may be considered for future phases to further enhance the system's capabilities.

4.2 Interface Requirements

To ensure that the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina meets the highest standards of usability and accessibility, it is essential to adhere to established guidelines and best practices. This section defines the standards to be achieved, ensuring that the system is easy to use, learn, and accessible to all users, including those with disabilities or special needs.

Usability Standards refers to the ease of use and learnability of the system. It encompasses the following key principles:

1. Effectiveness: The system must enable users to achieve their goals accurately and completely. This includes intuitive navigation, clear instructions, and helpful feedback.
2. Efficiency: Users should be able to perform tasks with minimal effort and time. The system should streamline workflows and reduce unnecessary steps.
3. Satisfaction: The overall user experience should be positive, making users feel confident and satisfied with their interactions. This involves user-friendly design, aesthetically pleasing interfaces, and responsive performance.

To achieve these usability standards, the system will adhere to the ISO 9241-11:2018 standard, which provides guidance on usability definitions and concepts, focusing on user performance and satisfaction.

Accessibility Standards ensures that the system is usable by as many people as possible, including those with disabilities. Key principles of accessibility include:

1. Perceivable: Information and user interface components must be presented in ways that users can perceive, regardless of their sensory abilities. This includes providing text alternatives for non-text content and ensuring sufficient contrast between text and background.
2. Operable: Users must be able to operate the interface and navigate the system effectively. This includes making all functionalities accessible via keyboard and ensuring that the interface does not require interaction that users cannot perform.
3. Understandable: The information and operation of the system must be understandable. This involves using clear and simple language, consistent navigation, and providing instructions or help as needed.
4. Robust: The system must be robust enough to work with various assistive technologies. This includes ensuring compatibility with screen readers, magnifiers, and other accessibility tools.

The system will comply with the Web Content Accessibility Guidelines (WCAG) 2.1, at a minimum conformance level of AA. These guidelines provide a comprehensive framework for making web content more accessible to people with disabilities, including vision, auditory, physical, speech, cognitive, language, learning, and neurological disabilities.

By adhering to these established usability and accessibility standards, the new software system will be designed to be effective, efficient, and satisfying for all users, while also being accessible to those with disabilities. These standards will ensure that the system meets the

needs of the Audit Department and supports its mission of overseeing political party funding with the highest level of integrity and inclusivity.

4.3 User profiles

This section specifies who has authorized access to the new software system, the circumstances under which access is granted, and the specific parts of the system each user profile can access. The system will support four primary user profiles: External User, CEC Internal User, CEC Oversight Group Member, and CEC IT Administrator. Each profile will have distinct access rights and permissions tailored to their roles and responsibilities.

User Profiles and Access Specifications

1. External User

Description: External Users primarily consist of representatives from political parties or independent candidates responsible for submitting financial data.

- Access Rights:

  - Functionality:
    - Submit financial reports.
    - Edit and update submitted reports until they are finalized.
    - View their own submission history and statuses.
  - Data Access:
    - Access to their own financial data submissions.
    - Read-only access to public data and reports published by CEC.

- Circumstances for Access:

  - Authorized by their respective political party.
  - Authorized by the CEC Internal User.
  - Access is granted upon successful login with a secure username and password.

- Parts of the Product:

  - Submission portal for financial reports.
  - Dashboard showing submission history and statuses.
  - Public reports section.

2. CEC Internal User

Description: CEC Internal Users are staff members responsible for reviewing, validating, and analysing financial data submitted by political parties.

- Access Rights:

  - Functionality:
    - Review and validate submitted financial reports.
    - Generate and analyse statistical reports.

        - Upload auditor reports.
    - Data Access:
        - Access to all financial data submitted by political parties.
        - Access to historical data and audit logs.
        - Read and write access to statistical and audit reports.

- Circumstances for Access:

    - Authorized by the CEC Oversight Group Member.
    - Access is granted upon successful login with multi-factor authentication.

- Parts of the Product:

    - Review and validation interface.
    - Statistical report generation tools.
    - Auditor report management.
    - Comparison of political parties' spending plans with actual spending and analysis of differences.

3. CEC Oversight Group Member

Description: Oversight Group Members are responsible for oversight and governance, reviewing the findings and reports generated by the Audit Department.

- Access Rights:

    - Functionality:
        - View and review detailed financial and audit reports.
        - Provide feedback and request additional information.
    - Data Access:
        - Access to all financial and audit reports.
        - Read-only access to statistical data and spending plans.

- Circumstances for Access:

    - Authorized by the CEC Oversight Group.
    - Access is granted upon successful login with multi-factor authentication.

- Parts of the Product:

    - Report review interface.
    - Feedback and request submission tools.
    - Dashboard for oversight and governance.

4. CEC IT Administrator

Description: IT Administrators are responsible for maintaining the system, managing user accounts, and ensuring data security and system integrity.

- Access Rights:

  - Functionality:
    - Manage user accounts and access permissions.
    - Perform system maintenance and updates.
    - Monitor system performance and security.
    - Backup and restore data.
  - Data Access:
    - Full access to all system data and functionalities.
    - Access to system logs and audit trails.

- Circumstances for Access:

  - Authorized by the CEC IT Oversight Group Member.
  - Access is granted upon successful login with multi-factor authentication and elevated permissions.

- Parts of the Product:

  - User management interface.
  - System maintenance and monitoring tools.
  - Security and performance dashboards.
  - Data backup and restoration tools.

By clearly defining the access rights and circumstances for each user profile, the system ensures secure and appropriate use of functionalities and data. This structured access control helps maintain data integrity, security, and compliance with regulatory requirements, while supporting the operational needs of the Audit Department and its stakeholders.

5. Technical Requirements

5.1 Operational environment standards

The system must be implemented as a web application installed on servers according to the available infrastructure, which users access via an Internet browser. Supported browsers are listed below in the description of requirements for user workstations.

The system also provides an Application Programming Interface (API) implemented using web service technology to enable integration with other information systems both within and outside CEC.

5.2 Hardware and Infrastructure requirements

The system must meet the technological prerequisites for implementation on the infrastructure of the CEC. Infrastructure is based on the Microsoft technologies (IIS, MS SQL server, Microsoft Server) with current usage of VMWare technology for virtualisation, where there will be migration to Hyper-V. It is needed to use .NET technology for building new system.

The contractor is required to establish a development and testing environment on the software and hardware infrastructure provided by CEC. The development environment will be used for the development of the entire information system, as well as for internal functional and integration testing by development teams. The system testing environment will be used for system testing and any subsequent modifications in the system by users, for testing data migration procedures, and for user training. CEC will timely provide access to its own infrastructure through which the initial system setup is enabled.

The contractor is required to establish a production environment in accordance with the detailed Project Plan, which will be agreed upon with CEC. The production environment will be used for the official operation of CEC.

For the installation of its server component, the System must be compatible with Windows Enterprise version 10 or higher. The licenses for the operating system are provided by CEC.

The system must use the existing Microsoft SQL Server database for data storage purposes. Hardware, licenses, and database administration will be provided by CEC.

The system must ensure scalability and high availability through the use of redundant distribution across multiple servers, with the option to use a virtualized server environment.

Load distribution between servers will be managed using a Load Balancer component. Contractor is required to implement redundant software load balancing based on open-source components and distributed across separate CEC servers, without the need for additional licenses and other costs, or by using existing CEC resources.

5.3 Access modes and security requirements

Internal users of CEC access the system using workstations connected to CEC's internal network. The system must be compatible with Internet browsers:

i. Microsoft Edge

ii. Google Chrome

in their latest versions according to the maintenance and upgrade policy of their providers.

External users, who are obligated to fill in the system information for the analysis of money laundering and terrorist financing risks among political parties, also access the system. It must be compatible with modern and most commonly used Internet browsers

5.4 Operational security

The Contractor is expected to carry out standard testing procedures for both the test and production systems, and to ensure the quality and stability of the system. Records of the testing will be kept and must be presented to CEC upon request.

The Contractor is obligated to deliver detailed system acceptance testing procedures as part of the system implementation, which include acceptance criteria based on the expected results from using the system.

Successful completion of the acceptance testing is a prerequisite for CEC's acceptance of the system delivery. The Contractor is expected to provide necessary on-site support during the acceptance testing and the system deployment.

Hardware Access

- CEC IT Administrators: Authorized to access all hardware components of the system, including servers, network devices, and storage devices.
- Contractor's Technical Team: Granted temporary access to hardware components for installation, configuration, and maintenance purposes. Access is limited to the duration of specific tasks and requires approval from CEC IT Administrators.
- Exceptions: No other personnel are permitted to access the hardware unless explicitly authorized by CEC IT management for emergency or special situations.

Media Access

- CEC IT Administrators: Authorized to handle all media related to the system, including backup tapes, external drives, and other storage media.
- Contractor's Technical Team: May access media temporarily for data migration, backup, and recovery tasks under the supervision of CEC IT Administrators.
- Exceptions: Media access is restricted to prevent unauthorized handling or data breaches.

Administration Controls

- CEC IT Administrators: Have full administrative control over the system, including user management, system configuration, and security settings.
- Contractor's Technical Team: Provided with administrative access during the implementation phase to set up the system, perform configurations, and address any issues. This access is revoked upon completion of the implementation and acceptance testing.
- Exceptions: Administrative controls are not granted to any other users except for authorized CEC personnel for specific administrative tasks.

Testing Procedures - Standard Testing Procedures

- Contractor's Responsibility: The Contractor is expected to carry out comprehensive testing procedures for both the test and production systems. This includes:
  - Functional Testing: Ensuring all system functionalities work as intended.
  - Performance Testing: Evaluating system performance under various conditions.
  - Security Testing: Assessing the system's security measures and identifying potential vulnerabilities.
  - Usability Testing: Verifying the ease of use and user satisfaction.

- Record Keeping: The Contractor must keep detailed records of all testing procedures and results. These records must be presented to CEC upon request.

System Acceptance Testing

Detailed Procedures

- Acceptance Testing Plan: The Contractor is obligated to deliver detailed system acceptance testing procedures as part of the system implementation. This includes:
  - Test Scenarios: Comprehensive scenarios that cover all aspects of the system's functionality.
  - Test Cases: Specific test cases with expected outcomes to validate the system's performance.
  - Acceptance Criteria: Clearly defined criteria based on the expected results from using the system, ensuring it meets CEC's requirements.

Prerequisites for Acceptance

- Completion of Testing: Successful completion of the acceptance testing is a prerequisite for CEC's acceptance of the system delivery. The criteria include:
  - Functionality: All functionalities must operate as specified.
  - Performance: The system must meet performance benchmarks.
  - Security: The system must pass all security tests without significant vulnerabilities.
  - Usability: The system must be user-friendly and meet usability standards.

On-site Support

- Contractor's Obligation: The Contractor is expected to provide necessary on-site support during the acceptance testing and system deployment. This support includes:
  - Technical Assistance: Addressing any issues or bugs identified during testing.
  - Training: Providing training to CEC staff on system usage and administration.
  - Documentation: Supplying comprehensive documentation covering system operations, maintenance, and troubleshooting.

Clear definition of the access controls and testing procedures will ensure that the new system is secure, reliable, and meets the required standards. The involvement of both CEC and the Contractor in these processes guarantees a thorough and effective implementation, leading to a successful deployment and operation of the system.

5.5 Development and implementation of the CEC system

The development and implementation of the CEC System must encompass the following activities:

1. Preparation and execution of the implementation project with detailed and clear implementation procedures,
2. Analysis of business requirements and creation of a detailed functional specification of the System,

3. Development and testing of the System's application modules,
4. Creation of a system acceptance testing plan,
5. Creation of technical documentation for the maintenance of the System,
6. Installation and configuration of the development, testing, and production environments of the System,
7. Training of key users to operate the System,
8. Installation and configuration of the production environment of the System according to specifications and final tuning of the System,
9. Launching the production environment of the System into operation,
10. Support during the production use of the System throughout the warranty period.

Importantly, CEC and the Contractor will each appoint a Project Manager from their side. The Project Manager will be the single point of contact between the contracting parties and will ensure the creation of plans, monitoring, and reporting on the execution of project tasks, communication, and coordination between the project teams on both sides.

5.6 Backup and archiving

To ensure the continuity and security of the system data for the Audit Department of the Central Election Commission of Bosnia and Herzegovina, it is critical to establish robust backup and archiving practices. This section outlines the necessary requirements and changes to existing practices to maintain effective data backup and archiving.

Requirements for Backup and Archiving

1. Backup Schedule

- Daily Backups: Perform daily incremental backups of all critical system data to capture changes made throughout the day.
- Weekly Full Backups: Conduct full system backups every week to ensure a complete copy of all data is available.
- Monthly Archival Backups: Create monthly archival backups that are stored for long-term retention, ensuring historical data preservation.

2. Backup Storage

- On-Site Storage: Maintain a secure on-site storage solution for immediate backup availability.
- Off-Site Storage: Implement off-site storage to protect against physical disasters. This could include cloud storage solutions or secure external locations.
- Redundancy: Ensure backups are stored in multiple locations to prevent data loss in case of a single point of failure.

3. Archiving Strategy

- Data Retention Policy: Define a data retention policy specifying the duration for which different types of data should be archived. For example, critical financial data might be archived for 10 years.
- Regular Archiving: Schedule regular archiving processes, ensuring that outdated data is moved to archival storage while remaining accessible if needed.
- Compliance and Regulatory Requirements: Ensure that the archiving strategy complies with all relevant legal and regulatory requirements, including data protection and privacy laws.

Changes to Existing Practices

1. Automated Backup Systems

- Implementation of Automated Tools: Introduce automated backup tools to handle the scheduling, execution, and monitoring of backups, reducing the risk of human error.
- Notification and Reporting: Set up notifications and reporting systems to alert administrators of backup successes, failures, and any issues requiring attention.

2. Data Verification and Integrity Checks

- Regular Verification: Implement processes to regularly verify the integrity of backups, ensuring that data can be restored successfully.
- Checksum Validation: Use checksum validation techniques to detect and correct any corruption in backup files.

3. Disaster Recovery Plan

- Development of a Comprehensive Plan: Develop a disaster recovery plan that includes detailed procedures for restoring data from backups in case of data loss or system failure.
- Regular Testing: Conduct regular disaster recovery drills to ensure that the plan is effective, and that staff are familiar with the procedures.

4. Staff Training and Awareness

- Training Programs: Provide training for IT staff on the new backup and archiving procedures, ensuring they are capable of managing and maintaining the system effectively.
- Awareness Campaigns: Conduct awareness campaigns to educate all users about the importance of data backup and the role they play in maintaining data integrity.

Implementing these requirements and changes to existing practices will ensure that the system data for the Audit Department is securely backed up and archived. This will provide a robust framework for data continuity, enabling the Commission to recover quickly from any data loss incidents and maintain the integrity and availability of critical financial information.

5.7 Service level: Availability, performance, and support

This section documents the key availability, performance, and support requirements necessary for the successful operation and maintenance of the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina. These requirements ensure that the system meets the high standards needed for handling sensitive financial data and supporting the Commission's critical functions.

Performance Requirements

- Speed and Latency
  - Requirement: The system should provide response times of less than 2 seconds for standard queries and operations under normal load conditions.
  - Detail: Ensure that all user interactions, including data entry, report generation, and data retrieval, are executed promptly to maintain efficiency.
- Accuracy
  - Requirement: Data entered into the system must be processed and stored with 100% accuracy.
  - Detail: Implement validation checks and error-handling mechanisms to ensure data integrity and correctness.

Availability and Reliability

- Reliability and Availability
  - Requirement: The system must maintain an uptime of 99.9%, excluding scheduled maintenance windows.
  - Detail: Utilize redundant hardware and failover systems to minimize downtime and ensure continuous availability.
- Robustness and Fault Tolerance
  - Requirement: The system should be robust and fault-tolerant, capable of handling unexpected errors and failures without significant disruption.
  - Detail: Implement fault-tolerant design principles, including redundancy, error detection, and automatic recovery processes.
- Capacity - Users and Data
  - Requirement: The system must support at least 500 concurrent users and handle large volumes of financial data.
  - Detail: Design the system architecture to scale efficiently, accommodating increasing numbers of users and data as needed.

Scalability and Length of Expected Use

- Scalability
  - Requirement: The system should be scalable to meet future growth in user numbers, data volume, and functional requirements.
  - Detail: Utilize modular and flexible architecture to allow for easy scaling and integration of additional features over time.

- Length of Expected Use
  - Requirement: The system should be designed for a minimum operational lifespan of 7 years.
  - Detail: Ensure that the technology stack and design principles support long-term use and maintenance.

Security Requirements

- Security
  - Requirement: Implement comprehensive security measures to protect the system against unauthorized access, data breaches, and other security threats.
  - Detail: Use encryption, multi-factor authentication, regular security audits, and compliance with relevant security standards.

Governance Issues

- Confidentiality
  - Requirement: Ensure that sensitive data is accessible only to authorized users.
  - Detail: Implement role-based access controls and encryption to protect data confidentiality.
- Integrity
  - Requirement: Protect data from unauthorized modification to ensure its integrity.
  - Detail: Use checksums, audit logs, and validation processes to detect and prevent data tampering.
- Availability
  - Requirement: Ensure that data and system functionalities are available to authorized users whenever needed.
  - Detail: Use redundant systems, regular backups, and robust disaster recovery plans to maintain availability.

Support Requirements

- Support and Maintenance
  - Requirement: Provide ongoing technical support and maintenance services to ensure the system's continuous operation.
  - Detail: Establish a support team available during weekly working hours to handle technical issues, perform regular system updates, and ensure system stability.
- Documentation and Training
  - Requirement: Provide comprehensive documentation and training materials for users and administrators.
  - Detail: Develop user manuals, training programs, and support resources to help users understand and effectively use the system.

These availability, performance, and support requirements ensure that the new software system for the CEC Audit Department is reliable, secure, and capable of supporting the Commission's needs. By adhering to these standards, the system will provide a robust

platform for managing financial data and enhancing the overall efficiency and transparency of the CEC Audit Department's operations.

The warranty period starts from the date of signing the Handover Protocol of the software solution. The minimum warranty period that the Contractor must provide is 24 months after the handover of the solution.

5.8 System documentation

To ensure the successful implementation, operation, and maintenance of the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina, comprehensive and thorough documentation is required. This section outlines the various types of documentation needed, detailing their scope and contents.

Documentation Types

1. Specifications

- Functional Specifications
  - Content: Detailed description of system functionalities, user roles, and business processes.
  - Purpose: To provide a clear understanding of what the system is designed to do and how it will support the business requirements.
- Technical Specifications
- Content: Detailed technical information about the system architecture, database design, APIs, data flow diagrams, and integration points.
- Purpose: To guide developers and IT personnel in understanding the technical aspects of the system.

2. Installation and Operation Files

- Installation Guide
  - Content: Step-by-step instructions for installing the system, including software prerequisites, configuration settings, and deployment procedures.
  - Purpose: To ensure the system is correctly installed and configured on all required environments.
- Operation Manual
  - Content: Detailed instructions on system operations, including startup and shutdown procedures, routine maintenance tasks, and system monitoring.
  - Purpose: To provide IT administrators with the knowledge to operate and maintain the system effectively.

3. User Manual

- User Documentation
  - Content: Instructions for CEC end-users on how to use the system, including navigation, data entry, report generation, and troubleshooting common issues.
  - Purpose: To help users understand and effectively utilize the system.

- Training Materials
  - Content: Training guides, tutorials, and exercises for educating users on system functionalities and best practices.
  - Purpose: To ensure users are well-trained and confident in using the system.

4. User Manual for Political Parties

- Content: Instructions for end-users (political parties and independent candidates) on how to use the system, including navigation, data entry, report generation, and troubleshooting common issues.
- Purpose: To help users understand and effectively utilize the system.

5. Policies and Guidelines

- Security Policies
  - Content: Guidelines and best practices for ensuring system security, including access controls, data protection, and incident response.
  - Purpose: To protect the system and its data from unauthorized access and breaches.
- Operational Guidelines
  - Content: Procedures for routine operations, including data backup, system updates, and performance monitoring.
  - Purpose: To ensure the system operates smoothly and efficiently.

Comprehensive documentation covering all aspects of the system is crucial for its successful implementation, operation, and maintenance. By providing detailed specifications, installation and operation guides, user manuals, policies, and guidelines, we ensure that all stakeholders have the information they need to understand, use, and support the system effectively. This thorough documentation will facilitate smooth transitions, efficient training, and prompt issue resolution, ultimately contributing to the system's long-term success and reliability.

6. Critical considerations

6.1 Assumptions

This section outlines the key assumptions made during the development and implementation of the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina. Documenting these assumptions is crucial to ensure all stakeholders have a clear understanding of the context and constraints within which the project operates.

Key Assumptions

- Legal and Political Assumptions

- New Laws or Political Decisions: It is assumed that no new laws or political decisions will be introduced that significantly alter the requirements or scope of the project during its development and initial implementation phases.

- Regulatory Compliance: The system is assumed to comply with all current regulations and legal requirements related to political party funding and financial reporting.

- Technological Environment

- Operating Environment: The system will operate within the existing technological infrastructure of the CEC, including compatibility with current operating systems, network configurations, and hardware.
- Internet Access: Reliable internet access is assumed for both internal and external users to ensure smooth operation of the system's web-based functionalities.

- Software and Development

- Available Software Components: It is assumed that all necessary software components and development tools will be available and compatible with the new system.
- Integration with e-Izbori: The system will successfully integrate with the e-Izbori system, allowing for seamless data exchange and functionality.

- Concurrent Projects

- Other Products in Development: No other major software systems are being developed concurrently that would conflict with or duplicate the functionalities of the new audit system.

- Resources and Staffing

- Availability of Staff: It is assumed that all necessary staff, including CEC internal users, IT administrators, and contractor personnel, will be available and have the required skills to support the project.
- Capability of Bought-in Components: Any third-party components or services procured for the project will meet the required specifications and quality standards.

- External Dependencies

- Dependencies on External Systems: The system will depend on certain external systems, such as the Porezna Uprava (Tax Administration) and Izvršna Vlast (Executive Authority). It is assumed these systems will be available and compatible for integration.
- Data from External Parties: Political parties and other stakeholders will provide accurate and timely data as required by the system.

- Scope and Exclusions

- Non-carried Requirements: Certain requirements, such as extensive data analytics or advanced AI functionalities, are not within the scope of this project and will not be carried out by the product.
- Security and Governance: It is assumed that the existing security and governance frameworks within the CEC are robust and will support the new system. Any

additional security measures specific to the new system will be implemented as part of the project.

These assumptions provide a framework within which the project will be developed and implemented. By clearly documenting these assumptions, we ensure that all stakeholders have a shared understanding of the project's context and constraints. This clarity helps in managing expectations, identifying potential risks, and ensuring the successful delivery of the new software system.

6.2 Constraints

This section identifies and documents the constraints within which the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina will be developed and implemented. Understanding these constraints is essential for effective project planning and execution.

Key Constraints

- Solution Design Constraints

  - Legacy System Integration: The new system must integrate seamlessly with the existing e-Izbori system and other legacy systems currently in use.
  - Modular Architecture: The system must be designed with a modular architecture to allow for future scalability and flexibility in adding new features or modules.
  - User Interface Design: The design of the user interface must be intuitive and user-friendly, supporting trilingual capabilities (Bosnian, Croatian, Serbian) including Cyrillic script.

- Implementation Environment

  - Existing Infrastructure: The new system must operate within the existing IT infrastructure of the CEC, including servers, network configurations, and hardware.
  - Data Migration: The project must include a robust plan for migrating existing data from the current system to the new one without data loss or corruption.

- Application Compatibility

  - Integration with External Systems: The new system must work with external systems such as Porezna Uprava (Tax Administration) and Izvršna Vlast (Executive Authority) to ensure data exchange and compliance.
  - Existing Applications: The system must be compatible with existing applications used by the CEC to ensure a seamless transition and avoid disruptions in current workflows.

- Pre-chosen Software

  - Packaged Solutions: Any pre-chosen software or third-party components must be integrated into the new system. This includes ensuring compatibility and addressing any limitations posed by these pre-selected solutions.

- Workplace Environment

  - Remote Access: The system must support remote access for external users (political parties) and internal users who may need to work from different locations.
  - User Training and Support: Adequate training and support must be provided to ensure all users are comfortable with the new system and can utilize its features effectively.

- Time

  - Project Timeline: The project must be completed within the specified timeline to meet critical deadlines, such as electoral cycles and reporting periods.
  - Phased Rollout: The system must be deployed in phases to minimize disruption and ensure smooth transition.

- Budget

  - Budget Constraints: The project must be completed within the allocated budget, covering all aspects including development, testing, deployment, and training.
  - Cost Management: Effective cost management practices must be in place to ensure that the project stays within financial constraints.

- Security and Governance

  - Data Security: The system must comply with stringent data security standards to protect sensitive financial information and personal data.
  - Regulatory Compliance: The system must adhere to all relevant legal and regulatory requirements, ensuring governance issues such as confidentiality, integrity, and availability are addressed.
  - Access Control: Robust access control mechanisms must be implemented to ensure that only authorized personnel can access sensitive data and system functionalities.

Documenting these constraints provides a clear understanding of the boundaries within which the project will operate. Acknowledging these constraints helps in effective planning, risk management, and ensures that the project objectives are met without compromising on quality or functionality.

6.3 Risks

The purpose of this section is to identify potential risks associated with the development and implementation of the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina. Each risk is assessed based on its probability of occurrence and its potential impact on the project. Mitigation measures are proposed to manage these risks effectively.

Identified Risks:

- Integration with Existing Systems
- Data Migration Issues
- Budget Overrun

- Timeline Delays
- User Adoption and Training
- Security Breaches
- Regulatory Changes
- Vendor Dependence

It is important to highlight that the integration of the new system with existing systems will pose a significant challenge. This has been identified as one of the primary risks in the project. It is strongly recommended that the CEC staff involved in the project be fully aware of this issue and be prepared to actively cooperate with the Contractor. Close collaboration will be essential in ensuring a smooth and effective integration, minimizing potential disruptions, and addressing any challenges that may arise during the process.

By identifying and assessing these risks early in the project, we can develop effective mitigation strategies to manage them proactively. Continual risk evaluation and management throughout the project lifecycle will help ensure the successful implementation of the new software system, meeting the needs of the Audit Department and supporting its critical functions.

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

Technical	INTEGRATION WITH EXISTING SYSTEMS Difficulty integrating the new system with existing systems like e-Izbori and external systems such as Porezna Uprava and Izvršna Vlast.	4	3	High	Months 2-6 (during system integration and testing phases)	Conduct thorough system analysis and compatibility testing during the initial phase. Engage experienced integration specialists. Allocate additional time for integration testing in the project timeline.	
Data	DATA MIGRATION ISSUES Potential data loss or corruption during the migration from the current system to the new system.	4	3	High	Months 3-5 (during data migration and initial testing phases)	Develop a comprehensive data migration plan, including multiple testing phases. Implement robust data validation and verification processes. Maintain backups of all data before starting the migration.	

Project Management	TIMELINE DELAYS Project not being completed within the specified timeline.	3	3	Medium	Throughout the project, with heightened risk in months 4-10 (as project milestones approach and dependencies may cause delays).	Develop a detailed project schedule with clear milestones. Monitor progress closely and adjust resources as needed. Ensure timely decision-making and problem resolution.	
Human Resources	USER ADOPTION AND TRAINING Users may struggle to adopt the new system, affecting productivity.	3	3	Medium	Months 7-10 (during user training and initial system rollout)	Provide comprehensive training programs for all user roles. Develop user-friendly documentation and support resources. Offer continuous support and refresher training post-implementation.	
Security	SECURITY BREACHES Unauthorized access or	4	1	Medium	Throughout the project, with heightened risk during	Implement robust security measures, including	

	data breaches compromising sensitive information.				months 5-12 (as system deployment approaches and begins operation).	encryption, multi-factor authentication, and regular security audits. Conduct thorough security testing before deployment. Establish a response plan for potential security incidents.	
Legal	REGULATORY CHANGES Changes in laws or regulations impacting system requirements.	3	1	Low	Unpredictable, but preparation should be ongoing (continuous monitoring required).	Stay informed about potential regulatory changes. Design the system to be flexible and adaptable to changes. Engage legal experts to ensure compliance throughout the project.	
Vendor Management	VENDOR DEPENDENCE Dependence on third-party	3	3	Medium	Months 1-12 (throughout the project, particularly during procurement and critical	Carefully evaluate and select reliable vendors. Develop contingency	

	vendors for critical components or support.				dependency phases)	plans for vendor-related issues. Establish clear contracts with service level agreements (SLAs).	

7. Data Requirements

7.1 Data inputs

The new software system will record a variety of data types critical to the operations of the Audit Department of the Central Election Commission of Bosnia and Herzegovina. Key data to be recorded includes financial reports and transactions submitted by political parties, auditor reports, compliance and discrepancy analyses, user activity logs, and statistical data on political party funding. Business areas involved in recording this data include the financial audit team, responsible for inputting and validating financial data; the Oversight Group, which records and analyses compliance-related information; IT administrators, who manage user activity logs and system performance data; and political party representatives, who submit financial reports. Further detailed analysis will be conducted to ensure all data requirements are comprehensively understood and met.

7.2 Data outputs and reporting requirements

Defining reporting requirements early in the project is crucial to ensure the system captures and processes all necessary data. This section outlines the key reports that need to be generated by the new software system, along with the business areas that will receive them. Further detailed analysis will be conducted to refine these requirements.

Key Reports and Recipients

1. Financial Compliance Reports

- Content: Detailed summaries of financial transactions and compliance status of political parties.
- Recipients:
  - CEC Audit Department Staff: To verify compliance and identify discrepancies.
  - CEC Oversight Group Members: To review overall financial compliance and make informed decisions.

2. Auditor Reports

- Content: Comprehensive reports generated by auditors, including findings, recommendations, and compliance issues.
- Recipients:
  - Audit Department Staff: To address identified issues and follow up on recommendations.
  - Oversight Group Members: To oversee audit outcomes and ensure corrective actions are taken.

3. Statistical Analysis Reports

- Content: Aggregated statistical data on political party funding, spending patterns, and compliance rates.
- Recipients:
  - Oversight Group Members: To analyse trends and prepare for regulatory reporting.
  - Political Parties: To provide insights into their financial performance and compliance status.

4. Discrepancy Reports

- Content: Reports highlighting discrepancies between reported and actual financial data, including potential reasons and impacts.
- Recipients:
  - Oversight Group Members: To investigate and resolve discrepancies.
  - Political Parties: To correct any discrepancies in their financial reports.

5. User Activity Reports

- Content: Logs of user activities within the system, including data submissions, updates, and access logs.
- Recipients:
  - IT Administrators: To monitor system usage, detect unauthorized access, and ensure data security.
  - Oversight Group Members (Audit Department): To review and manage user activities related to financial data.

6. Annual Financial Reports

- Content: Yearly summaries of financial activities, including income, expenditures, and compliance status of all political parties.
- Recipients:
  - Oversight Group Members: To assess the financial health and compliance of political parties.
  - External Stakeholders: To ensure transparency and public accountability.

7. Automated Letter Generation Reports

- Content: Notifications and letters generated automatically by the system for compliance reminders, audit findings, and regulatory updates.
- Recipients:
  - Political Parties: To ensure timely compliance with financial reporting requirements.
  - Oversight Group Members (Audit Department): To track communication and follow-ups with political parties.

By defining these reporting requirements, the system will be able to capture and process all necessary data to support comprehensive and timely reporting. This ensures that all business areas have the information they need to perform their roles effectively, maintain compliance, and uphold the integrity of the electoral process. Further analysis will refine these requirements to ensure all necessary details are captured and addressed.

7.3 Data migration

Data migration involves transferring data between different storage types, formats, or computer systems, and is critical when upgrading to the new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina. This process must be automated to ensure efficiency and accuracy, minimizing the need for manual intervention. Given the sensitive nature of financial and compliance data handled by the Audit Department, significant analysis is required to ensure all data is accurately and securely migrated without loss or corruption. This migration is essential to maintain continuity of operations, support historical data access, and leverage the enhanced functionalities of the new system. Identifying and addressing data migration needs early in the project will allow for a comprehensive plan to be developed, ensuring a smooth transition and uninterrupted service. Further detailed analysis will be conducted to define the specific data sets involved, the mapping requirements, and the technical processes needed to achieve a successful migration.

8. User Documentation and Training Requirements

Level of Documentation

The documentation provided will be comprehensive and detailed, covering all aspects of system usage, configuration, and maintenance. It will be designed to cater to different user roles, including end-users, administrators, and IT support staff.

User Involvement

Users will be involved in the production of documentation through feedback sessions and user testing phases to ensure the documentation meets their needs and is user-friendly.

Responsibility for Maintenance

The IT administrators at CEC will be responsible for keeping the documentation up to date, with support from the Contractor for major updates and revisions.

Form of Documentation

The documentation will be provided in various forms, including:

- Digital Documents: PDF files and other digital formats accessible via the system.
- Online Help: Integrated help features within the system.

Types of Documentation

1. User Manual

- Purpose: To guide all end-users on how to operate the system, including data entry, report generation, and troubleshooting.
- Users: All end-users, including political party representatives and CEC staff.
- Maintenance: IT administrators, with updates from the Contractor.
- Access Control: Available to all users with system access.
- Protection: Regular updates and version control to ensure accuracy.

2. Technical Documentation

- Purpose: To provide detailed instructions on system configuration, maintenance, and troubleshooting.
- Users: IT administrators and technical support staff.
- Maintenance: IT administrators, with support from the Contractor.
- Access Control: Restricted to authorized IT personnel.
- Protection: Secure storage and controlled access to sensitive information.

3. Configuration and Maintenance Guide

- Purpose: To outline procedures for configuring and maintaining the system.
- Users: Key IT staff and administrators.
- Maintenance: IT administrators - updated as needed by the Contractor.
- Access Control: Restricted to IT staff and administrators.
- Protection: Secure documentation with access logs.

Training Requirements

1. Necessary Training

- End-User Training: Comprehensive training on system functionalities, including data entry, report generation, and general use.
- IT Administrator Training: In-depth training on system configuration, maintenance, and troubleshooting.
- "Train the Trainer" Program: Training for up to 15 key trainers who will then educate other end-users.

2. Training Design

- Who Designs the Training: The Contractor, in collaboration with CEC, to ensure it meets the specific needs of the users.
- Who Provides the Training: The Contractor will conduct initial training sessions. Trained key users will then conduct further training sessions for all end-users.

Training Methods

- Classroom Workshops: Hands-on training sessions where users can test and practice implemented processes.

- Virtual Meetings: Using multimedia communication tools for remote training sessions.

Document and Data Protection

- Access Control Requirements

- User Manual: Accessible to all users.
- Technical Documentation and Maintenance Guide: Restricted to IT administrators and key technical staff.

- Protection Procedures

- Sensitive Data: Ensured by secure storage, regular updates, access logs, and encryption where necessary.
- Procedure Compliance: Adherence to data protection and confidentiality policies to safeguard sensitive information.

Comprehensive user documentation and training are critical to the successful implementation and operation of the new system. By providing detailed manuals, guides, and training programs, the project ensures that all users are equipped with the knowledge and resources they need to use the system effectively. Continuous updates and user involvement in documentation production will help maintain the relevance and accuracy of the information provided.

9. Regulatory Requirements

9.1 Privacy requirements

The new software system for the Audit Department of the Central Election Commission of Bosnia and Herzegovina must ensure the privacy of individuals' data, adhering to confidentiality, integrity, and availability requirements. The system must also comply with all relevant laws and regulations regarding data protection.

Privacy Requirements

- Confidentiality

- Data Encryption: All personal and sensitive data must be encrypted both in transit and at rest using industry-standard encryption protocols.

- Access Control: Implement strict role-based access controls to ensure that only authorized personnel can access personal data.
- Anonymization: Where possible, anonymize personal data to protect individual identities, especially in statistical and audit reports.
- Data Minimization: Collect only the minimum amount of personal data necessary for the system's operations, reducing the risk of exposure.

- Integrity

- Data Validation: Implement data validation checks to ensure the accuracy and completeness of personal data at the point of entry.
- Audit Logs: Maintain detailed audit logs of all data access and modifications to track and prevent unauthorized changes.
- Regular Integrity Checks: Conduct regular integrity checks to ensure that personal data has not been tampered with or altered improperly.

- Availability

- Redundant Systems: Utilize redundant systems and backups to ensure that personal data remains available even in the event of a system failure.
- Disaster Recovery Plan: Develop and maintain a comprehensive disaster recovery plan to quickly restore access to personal data in case of an emergency.
- Regular Backups: Perform regular backups of all personal data to prevent data loss and ensure timely restoration when needed.

Legal and Regulatory Compliance

- Data Protection Laws

- General Data Protection Regulation (GDPR): Ensure compliance with GDPR or other relevant regional data protection laws, which include provisions for data subject rights, data protection impact assessments (DPIAs), and data breach notifications.
- Local Data Protection Laws: Adhere to Bosnia and Herzegovina's specific data protection regulations, ensuring that all local legal requirements are met.

- Data Subject Rights

- Right to Access: Provide individuals with the ability to access their personal data upon request.
- Right to Rectification: Allow individuals to correct inaccurate or incomplete personal data.
- Right to Erasure: Implement procedures to delete personal data upon request, in accordance with legal requirements.
- Right to Restriction of Processing: Enable individuals to restrict the processing of their personal data under certain conditions.
- Right to Data Portability: Ensure that individuals can receive their personal data in a structured, commonly used, and machine-readable format.

Security Measures

- Physical Security

  - Secure Facilities: Ensure that data centres and storage facilities are physically secure, with controlled access to authorized personnel only.
  - Surveillance and Monitoring: Implement surveillance and monitoring systems to detect and respond to unauthorized physical access attempts.

- Technical Security

  - Firewalls and Intrusion Detection Systems: Deploy firewalls and intrusion detection systems (IDS) to protect against unauthorized access and cyber-attacks.
  - Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential security weaknesses.
  - Patch Management: Implement a robust patch management process to keep all systems up-to-date with the latest security patches and updates.

Data Handling Policies

- Data Retention Policy

  - Retention Periods: Define clear data retention periods for personal data, ensuring that data is retained only as long as necessary for the specified purposes.
  - Secure Deletion: Implement secure data deletion methods to ensure that personal data is irretrievably deleted when no longer needed.

- Incident Response

  - Breach Notification: Establish procedures for promptly notifying affected individuals and relevant authorities in the event of a data breach.
  - Incident Management: Develop an incident management plan to effectively respond to and mitigate the impact of data breaches or other security incidents.

To ensure the privacy of individuals' data, the new software system must implement robust measures addressing confidentiality, integrity, and availability. Compliance with all relevant data protection laws and regulations is mandatory, along with adopting best practices for data security and privacy. By doing so, the system will protect sensitive personal information and uphold the trust of all stakeholders involved.

9.2 Audit requirements

The new software system must retain comprehensive records to facilitate the required audit checks, ensuring transparency and accountability. This includes maintaining detailed logs of all data entries, modifications, and accesses, along with timestamps and user identifications. The system should store audit trails for a specified period, as mandated by regulatory requirements, ensuring that historical data is available for review. Additionally, the system must support the generation of audit reports that detail financial transactions, user activities, and compliance status. These records must be securely stored and protected against

unauthorized access or tampering, ensuring their integrity and availability for both internal and external audits. By retaining these records, the system will enable thorough and accurate audit checks, supporting the Audit Department's oversight and regulatory compliance functions.

9.3 Legislation

Financial Services Legislation

The system must comply with the Law on Financing Political Parties in Bosnia and Herzegovina, which regulates the manner and conditions under which political parties and their members secure funds for their operations. This includes strict adherence to the sources of funding, limitations on contributions, and obligations for financial reporting as outlined in the Election Law of Bosnia and Herzegovina.

Data Protection Rules

Compliance with data protection laws, such as the General Data Protection Regulation (GDPR) and local data protection regulations, is mandatory. The system must ensure that personal data of individuals is processed lawfully, transparently, and securely, with appropriate measures to protect against data breaches and unauthorized access. This includes implementing data subject rights, such as access, rectification, and erasure of personal data.

Freedom of Information

The system must be designed to facilitate compliance with freedom of information requirements. This includes providing public access to financial reports and other relevant data, while ensuring that sensitive personal information is adequately protected. The Central Election Commission of Bosnia and Herzegovina must ensure that transparency is maintained in the financial dealings of political parties without compromising individual privacy.

Governance Issues

1. Confidentiality

The system must implement strict access controls and encryption protocols to ensure that only authorized users can access sensitive data. This includes protecting the confidentiality of financial records, personal data, and internal communications of the Audit Department and political parties.

2. Integrity

Data integrity must be maintained through robust validation checks, audit logs, and regular integrity monitoring to ensure that information is accurate, complete, and unaltered. Any changes to data must be tracked and documented to provide a clear audit trail.

3. Availability

The system must ensure high availability and reliability to support continuous access to critical data and functionalities. This includes implementing redundant systems, regular backups, and a comprehensive disaster recovery plan to minimize downtime and data loss.

Failure to comply with these legal, compliance, and governance requirements could result in severe penalties, legal actions, and loss of public trust. It is crucial that the project team remains vigilant and proactive in addressing these issues throughout the development and implementation phases.

10. ANNEX I: Table of Fees

Below list specifies the expected deliverables and their corresponding deadlines. Prices are indicated in Euros **without VAT**, payable in local currency. ***Tenders proposing a total fee equivalent or above the exclusion level will be entirely and automatically excluded from the tender procedure.***

Deliverables ▼	**Deadline for delivery ▼**	**Fees ▼**	**Exclusion level ▼**
1. Clarify and refine with the Recipient the functional requirements of the application based on the Business and Technical Requirements, including the General requirements for the software solution stated in paragraph 4.1.1 and Specific Requirements defined in paragraph 4.1.2.	27 December 2024		55,000.00
2. Develop the software solution, including the testing of the software solution.	17 June 2025		
3. Finalize the development of the new software solution, following the feedback received from CEC and the findings of the testing phase.	22 July 2025		
4. Establish the production environment, integration, testing and production to the CEC.	26 August 2025		
5. Deliver trainings for the responsible CEC staff and key users of the platform and revise accordingly the system documentation defined in paragraph 5.8 of the Business requirements for the online platform.	9 September 2025		
6. Putting the software solution into production use.	7 October 2025		
TOTAL ►			**55,000.00**