SECURE IEC ONLINE VOTING SYSTEM

Information System Development

GROUP 13	
222868254	MOKOATLE N
219867387	MABANGA TST
219985614	MAILA TH
220197425	SHIVITI M
220420051	LESUDI TR

Final Project

Group 13

Table of Contents

Phase 1: Scope Management

1. Overview of the company

South Africa's Independent Electoral Commission (IEC) is a vital component of the country's democratic system. It was created as a constitutional body, and its main duty is to organize free and fair elections for every office in the government. The Independent Electoral Commission (IEC) ensures efficiency, openness, and correctness throughout the electoral process by carefully carrying out its tasks in compliance with the South African Constitution and electoral legislation.

In its pursuit of election integrity, the IEC covers all ground, from voter education to ballot preparation, and from voter registration to candidate nominations. Further demonstrating its dedication to democracy are its management of polling places, supervision of vote counting, and announcement of results.

Through adherence to these values and conscientious task execution, the IEC is essential to preserving democracy in South Africa. its efforts, it fosters an environment where citizens can exercise their right to vote freely, knowing that their voices will be heard and their choices respected. In essence, the IEC serves as a guardian of democracy, ensuring that the electoral process remains a cornerstone of South Africa's governance.

2. Objectives and Goals

The goals of the Independent Electoral Commission (IEC) in South Africa encompass diverse factors of its mandate to make sure free, fair, and transparent elections. Some of the key targets consist of:

2.1. Voter Registration: The IEC ambitions to check in eligible voters, ensuring that all residents who're eligible to vote are capable of accomplish that. This includes engaging in voter registration drives, updating voter rolls, and presenting accessible registration facilities.

2.2. Voter Education and Awareness: The IEC seeks to educate voters approximately their rights and responsibilities, in addition to the electoral process. This consists of supplying facts about voter registration, polling methods, and the importance of civic participation through voter education campaigns and materials.

2.3. Electoral Integrity: The EC is devoted to upholding the integrity of the electoral system with the aid of preventing fraud, irregularities, and malpractice. This entails implementing measures to protect the security and accuracy of voter rolls, ballots, and balloting techniques.

2.4. Electoral Administration: The IEC aims to efficiently administer all aspects of the electoral technique, together with candidate nominations, poll education, polling station control, vote counting, and the declaration of effects. This consists of making sure that electoral laws and guidelines are adhered to at some point of the manner.

2.5. Inclusivity and Accessibility: The IEC strives to promote inclusivity and accessibility within the electoral process, making sure that each one residents, such as people with disabilities and marginalized, have same opportunities to participate in elections. This includes offering handy polling stations, voter schooling materials, and assistance for voters with unique wishes.

2.6. Transparency and Accountability: The IEC is committed to engaging in elections in a obvious and accountable way, thereby enhancing public self belief inside the electoral procedure. This includes supplying access to facts, allowing for observation via domestic and global observers, and addressing any proceedings or disputes which could get up for the duration of the electoral procedure.

Overall, the objectives of the IEC in South Africa are aimed at promoting democratic principles, protecting the rights of voters, and ensuring the integrity of the electoral process.

3. The problems that the IEC faces

The Independent Electoral Commission (IEC) in South Africa faces numerous demanding situations in its efforts to ensure free, fair, and obvious elections. Some of the important thing troubles the IEC encounters include:

3.1. Voter Registration Issues: Despite efforts to check in all eligible voters, challenges inclusive of inadequate get entry to to registration facilities, lack of documentation, and low public recognition contribute to incomplete voter registration rolls.

3.2. Voter Education and Awareness: Ensuring that citizens are safely informed about their rights, the electoral manner, and the significance of participation stays a undertaking. Language barriers, low literacy costs in sure groups, and disinformation campaigns can hinder voter schooling efforts.

Three.

3.3. Electoral Integrity Concerns: Instances of voter fraud, irregularities in voter rolls, tampering with ballots, and allegations of political interference can undermine the integrity of elections and erode public trust in the electoral method.

3.4. Inclusivity and Accessibility: Despite efforts to promote inclusivity and accessibility, boundaries which include insufficient infrastructure, constrained transportation alternatives, and inaccessible polling stations can prevent sure companies, inclusive of human beings with disabilities and marginalized communities, from participating absolutely within the electoral procedure.

3.5. Electoral Violence and Intimidation: Incidents of violence, intimidation, and coercion, in particular in areas with a history of political anxiety or battle, pose a chance to the integrity of elections and can discourage voter turnout.

3.6. Election Administration Challenges: Managing logistical demanding situations along with the distribution of election materials, training of polling workforce, and making sure the safety of election infrastructure requires significant sources and coordination, especially in remote or underserved areas.

3.7. Legal and Regulatory Framework: Adapting electoral laws and regulations to address emerging issues such as online disinformation, campaign financing, and the use of technology in elections presents ongoing challenges for the IEC and policymakers. Addressing these challenges requires ongoing collaboration between the IEC, government authorities, civil society organizations, and other stakeholders to strengthen electoral processes, promote accountability, and safeguard democracy in South Africa.

4. Key Stakeholders

Identifying key stakeholders for an IEC (Independent Electoral Commission) undertaking in South Africa normally entails:

4.1. Sponsors/Key Stakeholders:

* South African government officials overseeing electoral tactics.
* Political parties and civil society companies advocating for honest and obvious elections.
* International groups presenting guide and investment for electoral approaches in South Africa.

4.2. Users:

* South African residents eligible to vote.
* Political events collaborating in elections.
* Electoral observers and monitors.
* Media agencies masking elections.

4.3. Project Team:

* Representatives from the Independent Electoral Commission (IEC) of South Africa.

* Technical specialists in election management systems, voter registration, and electoral logistics.
* Data analysts and statisticians for analyzing electoral information.
* Legal experts acquainted with electoral legal guidelines and guidelines.
* IT professionals for handling technology infrastructure.
* Administrative staff for logistical support.

5. Project need

Times are changing. The time for pen and paper is almost over. The IEC has been using the same old system of voting on a physical ballot and putting it in a box which will later be counted manually. This mode has caused many problems before where voters even thought some votes were fake. It also takes time to count all the votes, which is another issue for voters. There are also many political parties for the people to vote for including the newly introduced individual candidates, so it might be hard for people to find their candidate on paper. There is also the issue of long queues at the voting stations that causes many people not to vote. That is why we want to bring in a new online voting system which will allow all the voters to vote from the comfort of their own homes. The system can count the votes in a matter of seconds and in that way, voters can have confidence that the votes are legit. This will also help increase the number of voters especially young people.

6. Processes of the system

The system will first request the users' personal details. After the user enters the details, it will proceed to the next phase where the user is prompted to scan their fingerprint. The system will be connected with the home affairs system to tackle the issue of ghost voters and people stealing the identity of other people to vote on their behalf. It will then allow the user to vote. The screen will show 20 candidates per page in alphabetical order for the user to select. If the user cannot find their Ideal candidate, they can search for the name of the candidate through the search bar that will be on top. The user will then select the candidate and then will be prompted by the system to confirm their vote. After that the system will show a screen to thank the user for voting and then go back to the home screen. The system will then add this vote to the system immediately and start the count. At the end of the voting period, the system will add all the votes and display the winner on

the IEC website and social media pages, including all the votes they got. A voter will only be allowed to vote once and if the ID number has been used to vote once, you cannot use it again.

7. External Interfaces

The Independent Electoral Commission (IEC) interacts with a number of external interfaces like political parties, voters, government agencies, media organizations and international election observation missions. These external parties have different roles to the system, ranging from campaigning, voter registration, monitoring, reporting, and observing.

Here are the main external interfaces that interact with the IEC:

- Political Parties: Political parties take part in the electoral process by nominating candidates, campaigning, and by mobilizing voters. They participate with the IECC, nominating candidates, following the campaign rules, and reporting any anomalies during the voting.

- Voters: The second most important external entity. The constituency interacts with the IEC system by registering to vote, verifying their voter details, and voting on Election Day. The IEC has set up voter education, had registration facilities and polling stations to allow this connection.

- Government Agencies: Many government institutions work with IEC to maintain the proper functioning of elections. This involves not only the provision of services such as logistics, security and information sharing, but also encouragement to the electoral process.

- Media Organizations: Media have a great responsibility to inform the public about the electoral process, candidates, and election results. They cooperate with the IEC through providing events coverage, exit polls analysis, and publishing the official election results from the IEC.

- International Election Observation Missions: International election observation missions watch over the political process in order to keep it just, free, and in compliance with international norms. They participate with the IEC through a variety of ways such as observing polling stations, evaluating election procedures, and submitting reports with suggestions for improvement.

Feedback and corrections

1) **Clearly define the solution being proposed for the problem identified.**

An online voting system for the IEC would be a secure, web-based platform that enables eligible voters to cast their ballots electronically from any location. This system is designed to manage the entire voting process, from voter authentication and ballot distribution to vote casting, tabulation, and result reporting. In the past month we just had our national elections and there were several issues surrounding election rigging and the long lines that people had to standing in and the IECs system being down leading to even longer lines. A secure web-based voting system is the solution to these problems, voting on your personal devices anywhere eliminates the long unbearable lines for voters. AI counting and publishing the voting results eliminates human error or manipulation.

2) External interfaces should outline the other existing systems within IEC that which the proposed system will interact with or integrated with.

Interfaces that interact with the Online voting system

- Voters Registration: The purpose is to verify the identity and eligibility of voters. The online voting system should integrate with the voter registration database to ensure only registered voters can cast their ballots
- Authentication System: To authenticate voters before they can access the voting system. Integrating with the home affairs (national ID system) and biometric authentication system
- Ballot Design and Management System: To design, manage and distribute digital ballots. The online voting system should pull ballot designs from this system and ensure the correct ballot is presented to each voter.
- Election Management System: To manage the overall election process, including scheduling, monitoring, and reporting. The online voting system should communicate with this system to receive instructions and provide updates on voting status and results.
- Security and Monitoring Systems: To monitor and ensure the security of the voting process. Integration with security monitoring tools, intrusion detection systems, and possibly third-party security audits.

- Results Tabulation and Reporting System: To collect, tabulate, and report election results. The online voting system should securely transmit voting data to this system for accurate and transparent result tabulation.
- Help desk and Support System: To provide voter support and address any issues that arise during the voting process. The online voting system should interface with a support system to log issues and track resolutions.
- Communications System: To send notifications and updates to voters and election officials. The online voting system should integrate with email, SMS, or other notification systems to keep all stakeholders informed.
- Audit and Compliance Systems: To ensure the voting process complies with legal and regulatory requirements. The online voting system should generate audit trails and reports that can be reviewed by auditors and compliance officers.
- Third-Party Verification Systems: For independent verification of the election process. Allow third-party verifiers to access necessary data to perform their checks and validations.
- Data Backup and Recovery Systems: To ensure data integrity and availability in case of system failures. The online voting system should regularly back up data and be able to restore it quickly if needed

The collective contribution of these external interfaces toward the integrity and legitimacy of the electoral process in South Africa is achieved through their interaction with the IEC and fulfilling their different mandates.

8. Method for managing scope creep

- Verify the project scope with the stakeholders: To avoid scope creep we can meet stakeholders and share all the project requirements documentation with them, and show them the project schedule to ensure that we satisfy their expectations.

- Communicating clearly and often: If there's a change in scope we will take a lead and meet with stakeholders to discuss how the change will impact the overall project. We will work together to make a decision and carry out action.

- Have a written contract: Documenting the details of our project before we start the project, it will make it easier for us to identify and manage scope creep. We can ensure that we do not overlook any stakeholders expectations by gathering a list of requirements and communicating with all stakeholders.

- Create a back up plan: We discuss who will be responsible for reviewing and approving requested changes, the cost associated with extra work, and how long timelines can be extended.

9. Project communication

- Email
- Microsoft teams
- Voice calls

Strategic Communications Plan

Developing a strategic communication plan is essential. This plan outlines how to achieve positive media coverage. It involves reaching voters through various channels, including traditional (television, radio, newspapers) and new media (internet, blogs, social media).

Media outreach plays a significant role in informing, inspiring and motivating supporters. These channels allow direct communication with voters and provide real time updates.

1.Secure Communication Tool

The IEC must establish secure communication channels to address voter queries and concerns.

Tools include:

- End-to-End Encrypted tools: This ensures privacy and security during information exchange.
- Chatbots: Implement AI-driven chatbots on the IEC website to answer common questions
- Mobile App:Develop a user-friendly mobile app for voters Features include:

- Verified Voter Indentification: Implement secure methods to verify voters identities during online interactions.
- Election Reminder: Send notifications about upcoming elections
- How to vote guides: Provide visual instructions on casting votes online

1.1 .Internal Communication Tools

- Collaboration Platform: Use tools like Microsoft Team, Google Workspace for internal communication among IEC staff. These platform allow real-time messaging, file sharing and collaboration
- Intranet: Set up an internal website or intranet where staff can access official documents, announcements, and updates
- Email: Use secure email services for official communication within the organization

1.2 External Communication Tools

- Social Media: Establish official IEC profiles on platforms like Twitter, Facebook, and Instagram. Regularly share updates, election information, educational content , infographics and engage with voters
- Webinars and Online Workshops: Host virtual sessions explaining how to navigate the online system
- Website: Maintain an informative and user-friendly website with details about the elections, candidates, or updates related to online voting
- SMS Alerts: Send text messages to registered voters with important updates or reminders

2. Feedback mechanisms:

- Online Survey and Feedback Forms: Collect feedback from voters about their online voting experience.
- Social Listening: Monitor social media conversations to understand public sentiment and address any issues promptly

3. Transparency and Disclosure:

To build trust, the IEC should transparency throughout the process Techniques include:

- Real-Time Updates: Display live results on the IEC website during the election
- Publicly Disclose System Components: Provide information about the e-voting system's components for verification and clarification purposes
- Regular Updates: Keep voter informed about system security, privacy measures and any changes.
- Audit Trail: Maintain details logs of all online voting activities

- Public Announcements: Regularly update citizens on the progress of online votings

4. Multilingual Support

South Africa is linguistically diverse, so the IEC should offer information in multiple languages

Tools include:

- Language Selection: Allow users to choose their preferred language on the website
- Translation Services: Collaborate with professional translators to ensure accurate translations

5.Accessibility features

Consider citizens with disabilities

10. Techniques include:

- Screen Reader: Ensure the online platform is compatible with screen readers
- Accessible Design: Create an intuitive interface with clear fonts, colour contrast, and keyboard navigation
- Google Forms: To create the voting ballot.

In summary, the IEC leverages a combination of technology, communication channels and innovative devices to ensure accurate results and smooth operations during election. These efforts contribute to the maintaining the integrity of democratic process in South Africa

Phase 2: Project Plan

Introduction

In this document we are going to explain our project plan. This includes all the work that must be done, who is supposed to do the work and how long they have to complete the work. It will also include all the project milestones and all the difficulties we came across while completing our project. We will also write all the resources needed including the funds that should be allocated to the project.

Reiterated Project Scope

Project deliverables:

Times are changing. The time for pen and paper is almost over. The IEC has been using the same old system of voting on a physical ballot and putting it in a box which will later be counted manually. This mode has caused many problems before where voters even thought some votes were fake. It also takes time to count all the votes, which is another issue for voters. There are also many political parties for the people to vote for including the newly introduced individual candidates, so it might be hard for people to find their candidate on paper. There is also the issue of long queues at the voting stations that causes many people not to vote.

Our project aims to fix these problems with the following deliverables:

An Online/ Internet-based National electoral system:

- Capable of autonomously tabulating votes.
- Generating graphical representations illustrating the outcome of the electoral process.
- A secure internet-based voting system that prompts users to authenticate their identity by scanning their fingerprints subsequent to entering their personal details.
- The system will be connected with the home affairs system to tackle the issue of ghost voters and people stealing the identity of other people to vote on their behalf.
- The screen will show 20 candidates per page in alphabetical order for the user to select.
- A search functionality enabling users to search the database to locate their preferred candidate, through the search bar provided on each page.
- The user will then select the candidate and then will be prompted by the system to confirm their vote.
- At the end of the voting period, the system will add all the votes and display the winner on the IEC website and social media pages, including the number of votes each candidate received.

Customer Acceptance Criteria

The Acceptance Criteria for an internet-based voting system include:

Security:
The system must ensure the confidentiality, integrity, and authenticity of each vote.

Accessibility:
The platform should be accessible to all eligible voters, including those with disabilities, and be available across various devices and internet browsers.

User-friendliness:
The interface should be easy to navigate, catering to users with varying levels of technological proficiency.

Accuracy:
The system should accurately record and tally votes, ensuring the integrity of the voting process.

Reliability:
The platform must be stable and available throughout the duration of the voting period, with minimal downtime or technical issues.

Scalability:
The system should be capable of handling a large volume of concurrent users without experiencing performance degradation.

Transparency:
The voting process should be transparent, allowing voters to verify their choices and providing visibility into the overall electoral process.

Compliance:
The system must adhere to relevant legal and regulatory requirements governing elections and data privacy.

Auditability:
There should be mechanisms in place to audit the voting process and verify the accuracy of the results. ✓ Support:

Adequate support channels should be available to assist voters with any issues or inquiries they may encounter during the voting process.

Organizational Chart for Online Voting Implementation

1. Project Management Team

In order to successfully design, carry out, and deliver the online voting implementation project, the project management team is essential. They give the project team guidance, leadership, and support to guarantee that goals are reached and needs of stakeholders are properly met.

- Project Manager
  - Oversees the entire online voting implementation project.
  - Manages project scope, schedule, and budget.
  - Coordinates activities between different teams and stakeholders.

PERSON RESPONSIBLE: Neo Mokoatle

- Deputy Project Manager

➢ The Deputy Project Manager plays a vital role in supporting the Project Manager and ensuring the successful planning, execution, and completion of the online voting

implementation project. Their involvement helps to enhance project efficiency, effectiveness, and overall project management capabilities.

PERSON RESPONSIBLE: Neo Mokoatle

2. Technical Development Team

Responsible for the development, deployment, and maintenance of the online voting platform.

• Team Lead
➢ Oversees technical aspects of the project.

PERSON RESPONSIBLE: Thembelihle Mabanga

• Software Engineers
➢ Manage servers, databases, and network infrastructure.

PERSON RESPONSIBLE: Thembelihle Mabanga

3. Security and Compliance Team

Monitors and ensures the security and integrity of the online voting system.

- Team Lead: Thato Lesudi

• Security Analysts
➢ Conduct security assessments and monitor for threats.

PERSON RESPONSIBLE: Thato Lesudi, Masungu Shiviti

4. Infrastructure Team

- Team Lead: Tisetso Maila

- System Administrators
- System administrators are responsible for the day-to-day management and maintenance of servers, databases, and other critical infrastructure components. They ensure that servers are properly configured, perform routine maintenance tasks such as updates and patches, and troubleshoot any issues that arise.

PERSON RESPONSIBLE: Tisetso Maila, Thembelihle Mabanga, Thato Lesudi, Neo Mokoatle, Masungu Shiviti

Milestones:

1. Feasibility Study and Planning

- Make a thorough examination of the viability of putting in place an online voting system, taking into account things like the necessary technology, legal and regulatory issues, the money, and the time frame.
- Determine the project's objectives, success criteria, and goals.
- Create a project plan that details the resources needed, the timetable, the scope, and the risk management strategy.
- Set up procedures and routes of contact for project participants.

- Responsible: Project Management Team

- Output: Feasibility report and project plan

- Completion: 17 days

- Reporting Type: Written Report

2. Technical Development

- When designing the online voting system's architecture, keep usability, scalability, and security requirements in mind.
- Provide software components for a range of features, such as the production of ballots, voter registration, and result tabulation.
- Put in place security mechanisms including access restriction, authentication, and encryption.
- For more functionality, integrate third-party services or APIs as required.

- Responsible: Technical Development Team

- Output: Online voting platform prototype
- Completion: 25 days

- Reporting Type: Demo/Presentation

3. Security and Compliance Review

- Examine the security measures of the online voting system in detail to find any weaknesses or dangers.
- Conduct code reviews and penetration tests to evaluate the system's resistance to online attacks.
- Make sure that online voting systems adhere to all applicable laws, rules, and best practices, including GDPR, HIPAA, and election legislation.

- Responsible: Security and Compliance Team
- Output: Security audit report and compliance assessment
- Completion: 16 days
- Reporting Type: Formal Report

4. Infrastructure Setup

- Procure and configure hardware, software, and networking equipment required to support the online voting system.
- Set up servers, databases, and other infrastructure components in secure and resilient environments.
- Implement disaster recovery and backup solutions to ensure data integrity and availability.
- Establish monitoring and logging mechanisms to track system performance and security incidents.

- Responsible: Infrastructure Team
- Output: Scalable and secure server infrastructure
- Completion: 20 days
- Reporting Type: Progress Meetings/Updates

5. Testing and Piloting

- Develop test cases and scenarios to validate the functionality, usability, and performance of the online voting system.
- Conduct unit testing to verify individual software components.
- Perform integration testing to ensure seamless interaction between system modules.
- Conduct user acceptance testing (UAT) with representative users to gather feedback and identify any issues or concerns.
- Pilot the system in a controlled environment to simulate real-world usage and assess its readiness for deployment.

- Responsible: Technical Development Team
- Output: Testing reports and piloting results
- Completion: 10 days
- Reporting Type: Testing Reports, User Feedback Analysis

6. Rollout and Deployment

- Prepare deployment plans and schedules, including rollback procedures in case of deployment issues.
- Deploy the online voting system to production environments in a phased approach or all at once, depending on project requirements.
- Monitor deployment activities and address any issues or setbacks promptly.
- Conduct post-deployment testing to validate system functionality and performance in the production environment.

- Responsible: Project Management Team with support from all teams
- Output: Online voting system deployed and operational
- Completion: 30 days
- Reporting Type: Deployment Plan, Operational Reports

7. Training

- Develop training materials and documentation for election officials, administrators, and voters.
- Conduct training sessions to educate stakeholders on how to use the online voting system effectively and securely.
- Provide ongoing support and guidance to stakeholders as they familiarize themselves with the system.
- Update documentation based on user feedback and system enhancements.

Organisational chart for the IEC:

Phase 1: Election-related Preparedness

Milestone 1: Organizing the Election

- ACTIVITIES:
  Examining the rules and legislation pertaining to elections .
  Planning for resources and budget allocation .
  Electoral officers' appointment .
  Temporary Output: Election preparation paperwork.

PERSON RESPONSIBLE: Head of Planning Department
Time frame: 30 days

Milestone 2: Voter Registration Drive

- ACTIVITIES:
  Creating materials for voter registration
  Educating registration officials
  Establishing registration hubs
  Data collecting on voter registration as an interim output

PERSON RESPONSIBLE: Head of the Voter Registration Department Time frame: 60 days.

Phase 2: Conduct of Elections

Milestone 3: Printing of Ballot Papers

- ACTIVITIES:
  Creating and editing voting paper .
  Choosing and hiring printing businesses.
  Printed and sealed ballot papers are the interim output.

PERSON RESPONSIBLE: The head of the operations department is accountable. Time frame: 45 days

Milestone 4: Establishing Polling Places

- ACTIVITIES
  locating and guarding polling places
  Assembling voting booths and other necessary supplies educating poll workers
  Providing an interim output of prepared polling places.

PERSON RESPONSIBLE: Regional Operations Managers Duration: 30 days

Phase 3: Election Day

Milestone 5: Voting Activities

- ACTIVITIES
  Supervising the voting process
  Ensuring polling place security and order
  Helping voters with disabilities
  Providing interim output (the voting process completed)

PERSON RESPONSIBLE: Chief Electoral Officer
Duration: 1 DAY

Milestone 6: Results of the Vote Count

- ACTIVITIES

  Moving ballot boxes to counting centers

  Counting and confirming votes

  Announcing preliminary results

  Providing an interim output of preliminary election results.

PERSON RESONSIBLE: The Chief Electoral Officer

- Time frame: 5days

Phase 4: Activities Following Election

Milestone 7 : Post-election analysis • ACTIVITIES

Assessing the election process

Handling complaints and irregularities

Drafting a post-election report

Producing an interim post-election analysis report

PERSON RESPONSIBLE: Commission Chairperson

Duration: 45 days.

Milestone 8: Results Certification

- ACTIVITIES
  Final election results certification
  Candidate declaration
  Official results submission to appropriate authorities
  Interim output of certified election results

PERSON RESPONSIBLE: Election commission chairperson Duration: 15-day

Work Breakdown Structure:

WORK DESCRIPTION	DURATION	RESPONSIBLE PERSON
Scope statement	19 march – 24 march = 5 days	Maila TH and Mabanga TST

Project plan	25 march – 12 April = 18 days	Lesudi TR and Mokoatle N
Alternative solution analysis	13 April – 21 April = 8 days	Shiviti M & Maila TH
User requirements	21 April – 5 may = 14 days	Mabanga TST & Lesudi TR
System specifications	5 may – 19 may = 14 days	Mokoatle N & Maila TH
Test plan	19 may – 2 June = 14 days	Shiviti M & Mabanga TST
Final project documentation	3 June – 9 June = 6 days	Lesudi TR & Shitivi M

Planning dependencies

1. In order to start the planning of the project we have to identify the problems that the IEC is facing.
2. To implementation the project depend on project manager identifying the required project resources.
3. The project development can begin when there is availability of resources and the planning of the project is completed.
4. The completion of the project depend on project manager communicating with stakeholders about the expected results of the project.
5. In order for the project to be completed the project manager has to oversee the performance of the creation system.

Assumptions

- The user will assume that the new IEC online voting system is ready for use during the time of the election.
- The project team assuming that they are going to complete the project using the provided resources.
- The planned budget is going to complete the project.

Constraints

- Cost constraints- The money that we are going to spend in order to complete the project. The funds that are provided for this project are not enough to complete it, we are going to run out of funds in the middle of the project.
- Time constraints- The schedule time for us to complete the project. During the period of writing tests and holidays we have to put the project on hold, which may unable us to complete the project at the scheduled time.
- Scope constraints- The amount of the team's resources that we are going to use to complete the project. During the process of the project a stakeholder adding what the want the system to do will cause us to encounter scope creep.

- Quality constraints- how the project results are going to meet stakeholders satisfaction, expectations and needs. We are unable to communicate with all key stakeholders during the project, which may lead us to not meeting their satisfaction, expectation, and needs.

Identified Risks

Identifying the risks, countermeasures, and the person accountable for each countermeasure.

Developing software for elections presents several risks, below we address both the risks and ways to mitigate them:

RISKS	COUNTERMEASURES	CANDIDATE RESPONSIABLE
Security Risks Vulnerabilities in the software could be exploited to manipulate votes or compromise voter data.	Implement robust security measures, including encryption, authentication, and regular security audits. Employing end-toend verifiable systems can enhance transparency and trust in the election process.	MASUNGULO SHIVITI
Accuracy and Reliability Risks: Errors or bugs in the software may lead to inaccurate vote counting or result reporting.	Conduct thorough testing, including stress testing and simulation of real-world scenarios. Implement redundancy and failover mechanisms to minimize the impact of software failures.	NEO MOKOATLE
Accessibility Risks: The software may not be accessible to all voters, including those with disabilities.	Ensure that the software complies with accessibility standards such as WCAG (Web Content Accessibility Guidelines). Provide alternative voting methods for voters who cannot use the software.	THATO LESUDI
Privacy Risks: Personal information of voters may be compromised or misused.	Implement strong data protection measures, including encryption of voter data and adherence to privacy regulations such as GDPR (General Data Protection Regulation). Limit access to voter information to authorized personnel only.	THEMBELIHLE MABANGA
Legal and Regulatory Risks: Non-compliance with election laws and regulations could lead to legal challenges or sanctions.	Ensure that the software adheres to all relevant election laws and regulations. Consult legal experts to assess compliance and address any potential issues.	TISETSO MAILA
Trust and Transparency Risks: Lack of transparency in the election process may undermine public trust.	Implement measures to increase transparency, such as providing audit trails and allowing independent verification of election results. Engage with stakeholders to build trust and confidence in the software.	NEO, MASUNGULO

Infrastructure and Technical Risks: Inadequate infrastructure or technical support may lead to disruptions during the election.	Ensure that the software is hosted on reliable and scalable infrastructure. Have contingency plans in place to address technical issues and ensure continuity of the election process.	THEMBELIHLE, THATO, TISETSO

This budget provides a comprehensive estimate for developing and maintaining an election software program over a period of one year, with allowances for planning, development, testing, infrastructure setup, training, and ongoing maintenance. Costs may vary based on factors such as project scope, team size, technology stack, and infrastructure requirements. Additionally, it's important to budget for contingency and unforeseen expenses.

Project Budget

PHASE OF THE PROJECT	PERSONNEL	DAYS	COST	EXPENSE VALUE
1. Feasibility Study and Planning				
– Detailed project plan	Project Manager, Business Analyst	10 Days	R50,000/month	R300,000
– Project Objectives			R50,000 Once-off	R50,000
			Total for Planning Phase:	R350 000
2. Technical Development				
– Systems Design	Technical Team	25 days	R40,000/month	R2,840,000
– Software components			R200,000	R2,916 000
● Third-Party Services			R	R644,003
			Total for Development Phase:	R4,040,0003
3. Security and Compliance Review				
– Conduct code Review and	Security And compliance Team	16 DAYS	R45,000/month	R720,000
Penetration Test				
			Total for Security and Compliance Review	R720,00

4. Infrastructure Setup

– Servers, Networking Equipment And Purchase and setup:	Infrastructure Team	20 DAYS	R500,000	R500,000
– Cloud Services Hosting, data storage:		10 DAYS	R300,000	R300,000
● Disaster recovery and backup:		10 DAYS		
● Monitoring and Logging mechanisms		25 DAYS		
			Total for Infrastructure Setup:	R800,0005

5.Testing and Piloting

– Testing Tools and Resources	QA Engineers (4)	4 months	R45,000/month	R720,000
– Testing environments and tools			R100,000	R100 000
			Total for Testing Phase:	R820,0004

6.Rollout and Deployment

● Deployment plans and schedules	Project management team with support from all teams	30 DAYS	R500,000	R500,000
● Deploy the online voting system		14 DAYS	R800,000	R800,000
● Conduct postdeployment testing		1 MONTH	R120,000	R120,000
			Total for Rollout and Deployment	R1,420,00

7.Training

– Training Materials and Workshops			R150,000	R150,000
– Training sessions, documentation:	Trainer	2 months	R80,000	R80,006
			Total for Training	R230,006.

9. Maintenance and Support (ongoing)

– Software Updates and Patches		ongoing	R400,000	R400,000
– Technical Support	Helpdesk	ongoing	R300,000	R300,000
			Total for Maintenance (per year):	R700,000

Overall Budget Summary

Total Development Cost:	R6,240,000
Total Ongoing Maintenance Cost (per year):	R700,000
Total unforeseen circumstances:	R500,000

Reports

When developing an online voting system for the Independent Electoral Commission (IEC), it's crucial to have comprehensive reports to ensure transparency, efficiency, and accountability. Here are some essential weekly and monthly reports:

Weekly Reports:

System Performance Metrics: Monitor system uptime, response times, and any incidents or outages. Report on server load, database performance, and user access patterns.

Security Audit: Review security logs, intrusion attempts, and any vulnerabilities discovered. Highlight any suspicious activities or breaches.

Help Desk Statistics: Compile data on user inquiries, technical support requests, and resolution times. Identify common issues and areas for improvement.

Election Preparation Progress: Track progress on election-related tasks, such as candidate nominations, ballot design, and training sessions for election officials.

Monthly Reports:

Election Results: Present election results, including the number of votes cast for each candidate or party. Show the distribution of votes by region or constituency.

Complaints and Disputes: Document any complaints received during the month, investigations conducted, and resolutions. Address any legal challenges or disputes related to the electoral process.

Financial Expenditure: Report on budget utilization, expenses incurred, and funding sources. Ensure transparency in financial management.

User Feedback and Suggestions: Gather feedback from voters, election officials, and system administrators. Use this input to enhance the voting system's usability and functionality.

Feedback and corrections

Overall Feedback

1) **You missed out on problem escalation and change management process.**
2) **Reiterate the project scope - What the project will not do was not covered. The criteria that the customer will use to determine if they are happy with the final deliverables was not covered.**

Customer Acceptance Criteria

The Acceptance Criteria for an internet-based voting system include:

- ✓ Security:
  The system must ensure the confidentiality, integrity, and authenticity of each vote.
- ✓ Accessibility:
  The platform should be accessible to all eligible voters, including those with disabilities, and be available across various devices and internet browsers.
- ✓ User-friendliness:
  The interface should be easy to navigate, catering to users with varying levels of technological proficiency.
- ✓ Accuracy:
  The system should accurately record and tally votes, ensuring the integrity of the voting process.
- ✓ Reliability:
  The platform must be stable and available throughout the duration of the voting period, with minimal downtime or technical issues.
- ✓ Scalability:
  The system should be capable of handling a large volume of concurrent users without experiencing performance degradation.
- ✓ Transparency:
  The voting process should be transparent, allowing voters to verify their choices and providing visibility into the overall electoral process.
- ✓ Compliance:
  The system must adhere to relevant legal and regulatory requirements governing elections and data privacy.
- ✓ Auditability:
  There should be mechanisms in place to audit the voting process and verify the accuracy of the results. ✓ Support:
  Adequate support channels should be available to assist voters with any issues or inquiries they may encounter during the voting process.

3) **Organizational chart/WBS - A drawing would have been better.**

4) **Planning dependencies The dependencies have little if any to do with the project manager. Dependencies could include financial availability, infrastructure, training, etc.**

Problem Escalation Process

1. Identification and Reporting
    - Users: Issues can be reported by voters, administrators, or any system users.
    - Channels: Issues are reported through designated channels like a helpdesk, email, or online support form.
2. Initial Assessment
    - Support Team: The first line of support performs an initial assessment to understand the issue's nature and severity.
    - Categorization: Issues are categorized (e.g., critical, major, minor) based on their impact and urgency.
3. Immediate Response
    - Tier 1 Support: Simple issues are resolved by the initial support team.
    - Documentation: All steps taken are documented for transparency and future reference.
4. Escalation to Tier 2
    - Unresolved Issues: Complex or unresolved issues are escalated to the second-tier support team.
    - Specialist Involvement: Involves technical specialists with deeper expertise in the system's components.
5. Escalation to Tier 3
    - Critical Issues: Issues that threaten system integrity, security, or cause significant downtime are escalated to the highest support tier, involving senior engineers and system architects.
    - Emergency Response Team: An emergency response team is activated for critical issues to minimize impact.
6. Resolution and Recovery
    - Solution Implementation: The issue is resolved, and normal operations are restored.
    - Testing: Thorough testing is conducted to ensure the issue is completely resolved and no new issues have been introduced.
7. Post-Incident Review
    - Root Cause Analysis: A detailed analysis to identify the root cause and prevent recurrence.
    - Reporting: A comprehensive report is created, documenting the issue, resolution steps, and preventive measures.

8. Communication
    - Stakeholder Updates: Regular updates are provided to stakeholders throughout the escalation process.
    - User Communication: Affected users are informed about the issue and resolution status.

Change Management Process

1. Change Request Initiation
    - Submission: Change requests can be submitted by any stakeholder (e.g., users, developers, administrators).
    - Documentation: Each request includes a description, justification, impact analysis, and proposed implementation plan.
2. Review and Approval
    - Change Advisory Board (CAB): A CAB reviews all change requests to assess feasibility, risk, and impact.
    - Prioritization: Changes are prioritized based on urgency, benefit, and resource availability.
3. Planning
    - Detailed Plan: A detailed implementation plan is created, including timelines, resource allocation, and rollback procedures.
    - Risk Assessment: Potential risks are identified and mitigation strategies are developed.
4. Testing
    - Development Environment: Changes are initially implemented and tested in a controlled development environment.
    - User Acceptance Testing (UAT): Key users test the changes to ensure they meet requirements and do not introduce new issues.
5. Implementation
    - Scheduling: Changes are scheduled for implementation during low-usage periods to minimize disruption.
    - Execution: The change is implemented as per the plan, with continuous monitoring.
6. Post-Implementation Review
    - Verification: The change is verified to ensure it has been correctly implemented and is functioning as expected.
    - Documentation: All changes and findings are documented for future reference.
7. Continuous Monitoring and Feedback

- Monitoring: The system is continuously monitored for any issues arising from the change.
- Feedback Loop: User feedback is collected to evaluate the change's impact and effectiveness.

8. Audit and Compliance
    - Compliance Check: Ensuring all changes comply with regulatory and organizational standards.
    - Audit Trail: Maintaining an audit trail for all changes for accountability and future audits.

What the Online Voting System Will Not Do

1. Offline Voting
    - The system will not facilitate or process votes cast offline. Traditional voting methods (e.g., paper ballots) will not be integrated into this system.
2. Voter Registration
    - The system will not handle the voter registration process. It assumes that voters are already registered through existing IEC processes.
3. Campaign Management
    - It will not provide features for candidates or parties to manage their campaigns, communicate with voters, or advertise.
4. Political Analysis and Reporting
    - The system will not offer tools for political analysis, predictive analytics, or detailed reporting on voter behavior beyond basic election results.
5. Third-Party Integrations
    - The system will not integrate with third-party applications or services unless explicitly required by IEC South Africa.
6. User Management for Non-Election Purposes
    - It will not manage user accounts for purposes other than voting, such as social networking or general communication.
7. Content Moderation
    - The system will not include features for moderating user-generated content, as it focuses strictly on the voting process.
8. Post-Election Services

- It will not provide post-election services such as archiving of votes or detailed statistical analysis beyond immediate election results.

9. Non-Secure Environments
    - The system will not function in non-secure environments or without proper authentication and authorization mechanisms in place.
10. Legal Compliance
    - The system will not be responsible for ensuring compliance with all local, national, and international laws beyond those directly related to the voting process.

Criteria for Customer Satisfaction with Final Deliverables

1. Functionality
    - Completeness: All agreed-upon features and functionalities are fully implemented and operational.
    - Usability: The system is user-friendly and accessible to all voters, including those with disabilities.
2. Performance
    - Scalability: The system can handle the expected number of voters without performance degradation.
    - Reliability: The system operates reliably without crashes or significant downtime during the voting period.
3. Security
    - Data Integrity: Votes are accurately recorded and counted, with no tampering or data loss.
    - Confidentiality: Voter information and votes are kept confidential and secure from unauthorized access.
    - Authentication: Strong authentication measures are in place to verify voter identities.
4. Compliance
    - Legal and Regulatory: The system complies with all relevant electoral laws and regulations in South Africa.
    - Standards Adherence: The system adheres to industry standards and best practices for online voting systems.
5. User Experience
    - Ease of Use: Voters find the system easy to navigate and use without extensive instructions.
    - Support: Adequate support is available for voters encountering issues during the voting process.
6. Accuracy and Transparency

- Result Accuracy: Election results are accurate and verifiable.
- Auditability: The system provides a clear audit trail for all voting activities.

7. Technical Support and Maintenance
   - Documentation: Comprehensive documentation is provided, covering system use, administration, and troubleshooting.
   - Training: Sufficient training is provided to IEC staff and stakeholders on how to use and manage the system.
   - Ongoing Support: Post-implementation support is available to address any issues or updates required.
8. Stakeholder Feedback
   - Voter Satisfaction: Positive feedback from voters regarding the ease and reliability of the voting process.
   - Stakeholder Approval: Approval from key stakeholders, including IEC officials, government bodies, and election observers.

5) Project budge - The project budget should be futuristic. For instance, 2024/25. You want to present the total budget of R6M and then break it down into the various appropriations (allocations).

Project Budget

This is the budget for 2024/25

The total cost for the budget is R10 000 000

PHASE OF THE PROJECT	PERSONNEL	DAYS	COST	EXPENSE VALUE
1. Feasibility Study and Planning				
– Detailed project plan	Project Manager,	10 Days	R50,000/month	R300,000

	Business Analyst			
– Project Objectives			R50,000 Once-off	R50,000
			Total for Planning Phase:	R350 000

2. Technical Development

– Systems Design	Technical Team	25 days	R40,000/month	R2,840,000
– Software components			R200,000	R2,916 000
- Third-Party Services			R100,00	R644,003
			Total for Development Phase:	R6,400,003

3. Security and Compliance Review

– Conduct code Review and	Security And compliance Team	16 DAYS	R45,000/month	R320,000

Penetration Test				R175,000
			Total for Security and Compliance Review	R495,000

4. Infrastructure Setup

– Servers, Networking Equipment And Purchase and setup:	Infrastructure Team	20 DAYS	R500,000	R500,000
– Cloud Services Hosting, data storage:		10 DAYS	R300,000	R300,000
● Disaster recovery and backup:		10 DAYS	R100,000	R100,000
● Monitoring and Logging mechanisms		25 DAYS	R80,000	R80,000
			Total for Infrastructure Setup:	R980,000

5. Testing and Piloting

– Testing Tools and Resources	QA Engineers (4)	4 months	R45,000/month	R720,000

– Testing environments and tools			R100,000	R100 000
			Total for Testing Phase:	R820,000

6. Rollout and Deployment

● Deployment plans and schedules	Project management team with support from all teams	30 DAYS	R500,000	R500,000
● Deploy the online voting system		14 DAYS	R800,000	R800,000
● Conduct post-deployment testing		1 MONTH	R120,000	R120,000
			Total for Rollout and Deployment	R1,420,000

7. Training

– Training Materials and Workshops			R150,000	R150,000
– Training sessions, documentation:	Trainer	2 months	R80,000	R80,006
			Total for Training	R230,006.

8. Maintenance and Support (ongoing)

– Software Updates and Patches		ongoing	R400,000	R400,000
– Technical Support	Helpdesk	ongoing	R300,000	R300,000

			Total for Maintenance (per year):	R700,000

Overall Budget Summary

Total Development Cost:	R9 875 009
Total Ongoing Maintenance Cost (per year):	R100,000
Total unforeseen circumstances:	R100,000

6) Reporting - You might wanna include ad hoc reporting as well.

Phase 3: Alternative Solutions Analysis

Overview of the business problem or opportunity

In order to ensure that elections in South Africa are free and fair, the Independent Electoral Commission (IEC) is essential. The main duty of the IEC is to oversee the election process and make sure that it is carried out legally, effectively, and transparently. The South African IEC, like every electoral system, must contend with a number of obstacles and opportunities.

1. Accessibility: Ensuring that the electoral process is available to all eligible voters, particularly those living in remote or rural areas, is one of the major difficulties facing the IEC. Some voters may find it impossible to go to physical polling places, which could result in their disenfranchisement.
2. Efficiency: Manual election administration can be resource- and time intensive. Election results announcements may be delayed, thus eroding public confidence in the process, as counting paper votes and verifying the accuracy of results can take a long time.
3. Security: It is crucial to guarantee the honesty and safety of the voting process. Voter fraud can take several forms in traditional paper-based voting systems, such as ballot stuffing and tampering. Preserving public trust in election results requires safeguarding the democratic process from these dangers.
4. Inclusivity: With several official languages and a rich cultural heritage, South Africa is a diverse nation. Upholding democratic norms requires that the electoral process be inclusive of all citizens and allow for this variety.
5. Engagement: The IEC is constantly working to increase voter participation and engagement. Many people might not completely comprehend the

significance of their vote or feel disillusioned with the political system. It is essential to figure out how to successfully inform and involve voters.

In this context, the South African IEC has a chance to improve the election process and address these issues by utilizing technology. Through the creation of a website or online voting system, the IEC can:

- Increase Accessibility: Voters who might find it difficult to participate in person, such as those who live in distant locations or have mobility challenges, may find the election process easier to access with the help of an online voting system.
- Boost Efficiency: By streamlining the electoral process, digital voting can cut down on the time and resources needed for chores like tabulating results and counting ballots. Election results may become more accurate and timely as a result of this.
- Strengthen Security: Although electronic voting brings with it additional security concerns, it also presents chances to put strong authentication and encryption systems in place to protect the fairness of the voting process.

Alternative IT Solutions

Creating an online voting system involves various options and considerations. Here are some key options we explored:

1. **Develop Custom Software**: Building a custom online voting system gives you full control over features, security, and user experience. You can tailor it to your specific requirements and integrate advanced security measures. However, this option requires significant time, resources, and expertise in software development and cybersecurity.

2. **Use Open-Source Solutions**: There are several open-source online voting platforms available, such as Helios Voting and Belenios. These platforms provide a foundation for building a secure and transparent voting system while allowing customization to suit your needs. Open-source solutions offer transparency and community support but may require technical expertise for deployment and maintenance.

3. **Adopt Commercial Voting Software**: Many companies offer commercial online voting software and services tailored for various election scenarios, including government elections, corporate governance, and organizational polls. These solutions often provide user-friendly interfaces, security features, and support services. However, they may come with licensing fees and limited customization options.

4. **Utilize Third-Party Services**: Some companies specialize in providing online voting services as a third-party solution. These services handle all aspects of the voting process, including voter registration, ballot creation, and result tabulation. While convenient, relying on third-party services raises concerns about data privacy, security, and vendor lock-in.

5. **Integrate with Established Platforms**: You can integrate online voting functionality into existing platforms, such as social media networks, collaboration tools, or government portals. Leveraging established platforms can simplify voter outreach and registration, but it requires careful consideration of security and privacy implications.

6. **Explore Blockchain-Based Solutions**: Blockchain technology offers decentralized and tamper-resistant voting systems that enhance transparency and security. Several blockchain-based voting platforms, such as Voatz and Democracy Earth, leverage distributed ledger technology to ensure the integrity of the voting process. However, implementing blockchain solutions requires expertise in blockchain development and may face regulatory challenges.

When choosing an option to create an online voting system, consider factors such as security, scalability, usability, regulatory compliance, and budget constraints. Additionally, engage stakeholders, including election officials, voters, and cybersecurity experts, to ensure the system meets their needs and addresses potential concerns.

Bearing in mind these options and the Customer satisfaction criteria, we chose to utilize Third party services, and here are our alternative solutions:

1. **SurveyMonkey**:
    - SurveyMonkey offers an easy-to-use online survey platform that can be adapted for voting purposes. It provides various question types, customization options, and analytics features. Additionally, SurveyMonkey offers security features such as SSL encryption and GDPR compliance.

2. **Typeform**:
    - Typeform provides a modern and interactive form builder with features like conditional logic, customization, and multimedia integration. It offers a user-friendly interface for both creators and respondents. Typeform also supports data encryption and compliance with data protection regulations.

3. **ElectionBuddy**:

- ElectionBuddy specializes in online voting and election management. It offers customizable ballot design, secure voting processes, and result tabulation. ElectionBuddy provides features like voter authentication, multiple voting methods, and audit trails to ensure the integrity of the voting process.

4. **ElectionRunner**:
    - ElectionRunner is a web-based voting platform designed for conducting online elections, polls, and surveys. It offers features such as customizable ballot templates, voter authentication, and result tracking. ElectionRunner supports various voting methods, including ranked choice voting and weighted voting.
5. **Simply Voting**:
    - Simply Voting is a secure online voting platform used by organizations, associations, and governments worldwide. It provides features like customizable ballots, voter authentication, and real-time result reporting. Simply Voting employs encryption and other security measures to protect voter data and ensure confidentiality.
6. **Crowdsignal (formerly Polldaddy)**:
    - Crowdsignal is a versatile polling and survey platform that can be used for online voting. It offers features such as customizable forms, multiple question types, and result visualization. Crowdsignal provides integration with WordPress and other content management systems for seamless deployment.
7. **ElectionRunner**:
    - ElectionRunner is a web-based voting platform designed for conducting online elections, polls, and surveys. It offers features such as customizable ballot templates, voter authentication, and result tracking. ElectionRunner supports various voting methods, including ranked choice voting and weighted voting.
8. **Google Forms:**
    - Google Forms is a versatile tool for creating surveys and forms. You can use it to design and distribute ballots, collect votes, and gather feedback from voters. It offers customizable templates, multiple question types, and built-in analytics for tracking responses.
9. **Democracy Live:**

- Democracy Live offers secure online voting solutions for government elections, corporate governance, and organizational polls. It provides end-to-end encryption, multi-factor authentication, and accessibility features to ensure the integrity and inclusivity of the voting process.

Assessment, Comparison, and conclusion of Alternative solutions:

To assess and compare the alternative solutions for creating an online voting system, we analyzed each option based on key criteria such as security, usability, scalability, regulatory compliance, and budget constraints:

Developing custom software:

One of the safest and most advanced method we considered. It gives you full control of the security features and user experience. However, we had a few concerns that made us think otherwise. It requires large amounts of time and resources to be able to get the final product. It requires expertise in the software development industry. Therefore, we concluded that this method would not be the best for our project.

Use open-source solutions:

There are various open-source solutions available that offer voting functionality. However, they require technical expertise for deployment and maintenance. Since the software is open source, no one is responsible for the software. So if it crashes during the voting period you cannot hold anyone accountable.

Adopt commercial voting software:

Many companies offer online voting platform that are safe and easy to use. These services are offered for a certain fee. They also offer little to no customization flexibility.

Integrate with established platforms:

We can integrate our voting system into our existing online platform, but it would require high level expertise in web development. It also would require a large number of resources and funds. It also needs careful consideration of security and privacy implications.

Explore blockchain based solutions:

It is one of the safest options available but it requires expertise in blockchain development and may have regulatory challenges. It also requires lot of resources and money

1. **SurveyMonkey:**

Security: It offers SSL encryption and GDPR compliance, ensuring data protection during the voting process.

Usability: It provides a platform that is easy to use with various question types and customization options.

Scalability: it can handle a high number of respondents, making it good for scalable voting processes.

Regulatory Compliance: GDPR compliance ensures compliance to data protection regulations.

Budget: it is cost-effective, but pricing may be different based on usage and additional features.

2. **Typeform:**

Security: it supports data encryption and adherence to data protection regulations.

Usability: supplies a modern and interactive interface, advancing the user experience.

Scalability: can handle scalable voting processes very well.

Regulatory Compliance: makes sure the is adherence to data protection regulations.

Budget: Prices may be different depending on usage and additional features but generally offers competitive prices.

3. **ElectionBuddy:**

Security: Specializes in online voting and offers secure voting processes.

Usability: Provides customizable ballot design and user-friendly features.

Scalability: Suitable for scalable voting processes.

Regulatory Compliance: Ensures compliance with election regulations and security standards.

Budget: Pricing may be higher due to specialized features but can be cost-effective for large-scale elections.

4. **ElectionRunner:**

Security: provides safe voting processes and authentication features.

Usability: offers customizable ballot templates and supports different voting methods.

Scalability: it is perfect for scalable voting processes and supports a variety of voting methods.

Regulatory Compliance: makes sure there is compliance with election regulations and security standards.

Budget: Pricing will vary but it generally offers competitive prices for its features.

5. **Simply Voting:**

Security: Uses encryption and other security methods to protect voter data.

Usability: Provides customizable ballots and user-friendly features.

Scalability: perfect for large-scale elections and supports same time result reporting.

Regulatory Compliance: ensure compliance with election regulations and security standards.
Budget: Prices might vary based on usage and additional features but it offers competitive rates.

6. **Crowd signal (formerly Polldaddy):**

Security: Offers secure polling and survey features.

Usability: it offers customizable forms and result visualization.

Scalability: it is perfect for scalable voting processes.

Regulatory Compliance: makes sure there is compliance to data protection regulations.

Budget: it is cost-effective, but prices may be different based on usage and additional features.

7. **Google Forms:**

Security: Uses Google's security measures and data protection standards.

Usability: it offers customizable templates and built-in analytics.

Scalability: its desirable for scalable voting processes.

Regulatory Compliance: makes sure there is compliance to data protection regulations.

Budget: Free to use, making it the most cost-effective option.

8. **Democracy Live:**

Security: provides end-to-end encryption and multi-factor authentication.

Usability: offers secure online voting solutions with access to various features.

Scalability: satisfactory for scalable voting processes.

Regulatory Compliance: makes sure there is compliance to election regulations and security standards.

Budget: Prices may be different based on usage and additional features but generally offers competitive rates.

Based on the assessment, each solution offers varying degrees of security, usability, scalability, regulatory compliance, and budget considerations. Utilizing third-party services of google forms is the perfect solution as it offers sufficient security features but also is the most cost-effective method from the rest.

Risk Analysis of each Alternative Solution:

As we create an online voting system for the IEC, let's examine the risk analysis of each of the components. The following summarizes the dangers connected to each factor:

1. **Developing Custom Software**:
    - **Software Quality:** There are hazards associated with code quality when developing custom software. While community engagement is advantageous for open-source projects, the skill and resources of the development team determine the quality of bespoke code. It is essential to guarantee thorough testing, code reviews, and adherence to best practices.

    - **Long-Term Sustainability**: The success of custom software depends on committed developers. Should the team experience burnout or resource limitations, the project's viability could be jeopardized.

    - **Budget Estimation**: It is crucial to estimate the budget accurately. Inadequate financial resources may result in inadequate or unsatisfactory solutions.

2. **Use Open-Source Solutions**:
    - **Software quality**: The quality of open-source projects differs. Some might not have the necessary documentation or maintenance. Consider security and maintenance metrics when selecting reliable packages.

    - **Security:** Although visible, open-source code is not immune to flaws. To reduce security concerns, evaluate and update dependencies on a regular basis.

3. **Adopting Commercial Voting Software**:
    - **Vendor Dependency**: Using outside vendors puts you in a dependent position. Make sure that contractual agreements, governance, and backup plans are all clear.

    - **Security and Transparency**: Check the commercial providers' security policies. It's critical that their codebase and processes be transparent.

- **Cost**: Commercial solutions can be expensive.

4. **Using Third-Party Services**:
   - **Supplier Risk:** The dependability of your system is impacted by third-party services. Failures of suppliers may cause operations to stall and damage reputation. Put in place reliable procedures for managing third-party risk.

   - **Security:** Check for security flaws in third-party services. Transparency and routine audits are crucial.

5. **Integrating with Established Platforms**
   - **Compatibility:** There may be problems with compatibility when integrating with current platforms. Ensure thorough testing and take backward compatibility into account.

   - **Data Consistency**: It can be difficult to synchronize data between systems. Address issues with data integrity and consistency.

6.**Exploring Blockchain-Based Solutions**:
   - **Complexity**: Consensus procedures, smart contracts, and scalability issues all contribute to the complexity of blockchain. Make sure you understand blockchain technology well.

   - **Security and Privacy**: Blockchain technology offers transparency, but it is not immune to attacks. Consider privacy issues and weigh the pros and cons.

A comprehensive approach to risk management is essential. Think about things like vendor relationships, software quality, security, and sustainability. Consistent risk evaluations, transparency, and compliance to best methodologies will contribute to maintaining the authenticity of the virtual voting platform for the IEC

Since we chose to use third party, let's examine the risk analysis for every alternative solution
1. **SurveyMonkey:**

- Some users feel that its reports, integrations, and design features are less user-friendly than those of Typeform or other options.
- Fewer Customization Options: Provides a reduced number of customization choices for the completed survey.

2. **Typeform:** • Cost: May be more expensive than other alternatives.
   - Only a select few file formats are supported for uploads.
   - Live communication functions are absent.

3. **ElectionBuddy:**
   - Email communication is the main method of contact.
   - Only a select few file formats are supported.
   - No major disadvantages were mentioned.

4. **Google Forms:**
   - Design: Some people may find the structure repetitive.
   - File Format Limitations: Only a select few file types are supported.

In conclusion, when selecting the best equipment for your online IEC voting system, take into account your unique needs and risk tolerance.

Analyses of the Cost and Benefits of the Alternative Solution:

1. **SurveyMonkey**

Cost: Using a surveymonkey is less costly because it allows users to use basic tools free of charge.

Benefit: It is user-friendly interface, secure to use, cost saving and has advanced analytics.

2. **Typeform**

Cost: Typeform is a free use form builder, however it offers us some paid plan basics.

Benefit: It is user-friendly interface, secure and cost saving.

3. **ElectionBuddy**

Cost: Using electionbuddy is expensive, because it offers free service for up to 20 voters only and start charging from there going up.

Benefit: Increase voters, user-friendly, secure and time saving.

4. **ElectionRunner**

Cost: Using ElectionRunner is expensive, because it offers free service for up to 20 voters only and start charging from there going up.

Benefit: Increases voters, user-friendly, secure and time saving.

5. **Simply Voting**

Cost: Simply Voting costs are fair and less costly.

Benefit: Increase voters, user-friendly, time saving and potential cost saving.

6. **CrowdSignal**

Cost: CrowdSignal is less costly to use and monitor.

Benefit: Time saving, secure, user-friendly, cost saving .

7. **Google forms**

Cost: Google forms are free to create and maintain.

Benefit: Cost saving, easy and effective use, getting feedback from voters and tome saving.

8. **Democracy Live**

Cost: Democracy live offers free of charge online voting solutions.

Benefit: User-friendly, secure, cost saving and time saving.

Phase 4: System Speficifations

Introduction

Overview of the product:

Times are changing. The time for pen and paper is almost over. The IEC has been using the same old system of voting on a physical ballot and putting it in a box which will later be counted manually. This mode has caused many problems before where voters even thought some votes were fake. It also takes time to count all the votes, which is another issue for voters. There are also many political parties for the people to vote for including the newly introduced individual candidates, so it might be hard for people to find their candidate on paper. There is also the issue of long queues at the voting stations that causes many people not to vote.

Our project aims to fix these problems with the following deliverables:

An Online/ Internet-based National electoral system:

- Capable of autonomously tabulating votes.
- Generating graphical representations illustrating the outcome of the electoral process.
- A secure internet-based voting system that prompts users to authenticate their identity by scanning their fingerprints subsequent to entering their personal details.
- The system will be connected with the home affairs system to tackle the issue of ghost voters and people stealing the identity of other people to vote on their behalf.
- The screen will show 20 candidates per page in alphabetical order for the user to select.
- A search functionality enabling users to search the database to locate their preferred candidate, through the search bar provided on each page.
- The user will then select the candidate and then will be prompted by the system to confirm their vote.

- At the end of the voting period, the system will add all the votes and display the winner on the IEC website and social media pages, including the number of votes each candidate received.

Project Team

1. Project Management Team

In order to successfully design, carry out, and deliver the online voting implementation project, the project management team is essential. They give the project team guidance, leadership, and support to guarantee that goals are reached and needs of stakeholders are properly met.

- Project Manager
  - Oversees the entire online voting implementation project.
  - Manages project scope, schedule, and budget.
  - Coordinates activities between different teams and stakeholders. PERSON RESPONSIBLE: Neo Mokoatle

- Deputy Project Manager

➢ The Deputy Project Manager plays a vital role in supporting the Project Manager and ensuring the successful planning, execution, and completion of the online voting implementation project. Their involvement helps to enhance project efficiency, effectiveness, and overall project management capabilities.

PERSON RESPONSIBLE: Neo Mokoatle

2. Technical Development Team

Responsible for the development, deployment, and maintenance of the online voting platform.

- Team Lead

➢ Oversees technical aspects of the project.

PERSON RESPONSIBLE: Thembelihle Mabanga

• Software Engineers
➢ Manage servers, databases, and network infrastructure.

PERSON RESPONSIBLE: Thembelihle Mabanga

3. Security and Compliance Team

Monitors and ensures the security and integrity of the online voting system.

- Team Lead: Thato Lesudi

• Security Analysts
➢ Conduct security assessments and monitor for threats.

PERSON RESPONSIBLE: Thato Lesudi, Masungu Shiviti

4. Infrastructure Team

- Team Lead: Tisetso Maila

- System Administrators
- System administrators are responsible for the day-to-day management and maintenance of servers, databases, and other critical infrastructure components. They ensure that servers are properly configured, perform routine maintenance tasks such as updates and patches, and troubleshoot any issues that arise.

PERSON RESPONSIBLE: Tisetso Maila, Thembelihle Mabanga, Thato Lesudi, Neo Mokoatle, Masungu Shiviti

SYSTEM REQUIREMENTS

Lists and prioritizes requests received regarding capabilities and features, such as from management, end users, or user groups. Requests from management will take priority. Requests from users and end-users take second priority. All requests have to be vetted by the management and support team before being taken to the developers.

DATABASE REQUIREMENTS

Database-related requests will be sent to the support group. Since the database is a crucial part of the system, the request has to be vetted thoroughly. They will be vetted first by the support group. Then the requests will be sent to top management where they will be vetted again. These requests can only come from the people inside the organization, and they will be prioritized according to their level of importance. For example, requests related to the functionality of the database will take priority over requests related to additional features.

Prioritization:

For Managerial Reports:

- Security Audit Report
- Voter Turnout Analysis
- Voting Patterns Analysis
- System Performance Report
- Compliance Report

For Operational Reports:

- Incident Report
- Voter Registration Report
- Vote Counting Report
- Ballot Generation Report
- Voting Process Report

MANAGERIAL REPORT MANAGEMENT:

Voter Turnout Analysis: An analysis of historical trends in voter turnout broken down by age, gender, and geography.

Voting Patterns Analysis: A study of voting trends, including inclinational trends, well-liked parties or candidates, and any anomalies found.

System Performance Report: Continual reports on the online voting system's uptime, response speeds, and any technical problems that may arise.

Security Audit Report: A thorough report on the security mechanisms put in place within the system, including recommendations for improvement and any breaches or attempted breaches.

Compliance Report: Verifying that all applicable laws and rules, such as those pertaining to data protection and elections, are met by the online voting system.

OPERATIONAL REPORT MANAGEMENT:

Voter Registration Report: Contains comprehensive data on the number of people who have registered to vote, together with demographics and any updated or modified voter records.

Ballot Generation Report: Monitoring the production and dissemination of ballots, guaranteeing precision and fairness all along the way.

Voting Process Report: Keeping an eye on the actual voting process, including voter turnout and any technological difficulties users may be having.
Vote Counting Report: Offering updates on the counting of votes, along with preliminary findings and methods for verification.

Incident Report: A record of any problems or disturbances that arise during the voting process, such as technical difficulties, cyberattacks, or other crises, together with the actions that were done to resolve them.

Creating a secure online voting system requires a comprehensive approach to address various potential threats and vulnerabilities. Here are some essential security requirements:

Security requirements

1. **Authentication and Authorization**:
    - Robust authentication mechanisms should be in place to ensure that only eligible voters can access the system.
    - Authorization mechanisms should be implemented to grant appropriate permissions to users based on their roles and privileges.
2. **End-to-End Encryption**:
    - All communication between the voter's device and the voting server should be encrypted to prevent eavesdropping and tampering.
    - End-to-end encryption ensures that votes remain confidential throughout the entire process.
3. **Tamper-Resistance**:

- Measures should be taken to prevent tampering with the voting system, including protections against unauthorized access to the server infrastructure and the integrity of the voting software.

- Utilize techniques such as digital signatures and cryptographic hashing to ensure the integrity of ballots and voting results.

4. **Voter Anonymity**:

   - The system should guarantee the anonymity of voters, preventing anyone, including the administrators, from tracing individual votes back to specific voters.

5. **Auditability and Transparency**:

   - The system should provide a transparent audit trail that allows for independent verification of the voting process and results.

   - This may include cryptographic proofs, paper trails, or other mechanisms to ensure the integrity of the election.

6. **Resilience to Denial-of-Service (DoS) Attacks**:

   - Implement measures to mitigate the risk of DoS attacks that could disrupt the voting process by overwhelming the system with traffic.

   - This may involve redundancy, load balancing, and rate limiting.

7. **Secure Infrastructure**:

   - Ensure that the servers hosting the voting system are securely configured and regularly patched to protect against known vulnerabilities.

- Implement strict access controls and monitoring to prevent unauthorized access to sensitive data.

8. **Backup and Disaster Recovery**:

   - Implement robust backup and disaster recovery procedures to ensure that voting data is not lost in the event of hardware failure, natural disasters, or other unforeseen events.

9. **Independent Security Audits**:

   - Regular independent security audits should be conducted to identify and address potential vulnerabilities in the voting system.

   - Vulnerability disclosure programs can encourage responsible reporting of security issues by external researchers.

10. **Legal and Regulatory Compliance**:

- Ensure that the online voting system complies with relevant laws, regulations, and industry standards related to data privacy, election integrity, and cybersecurity.

Look and feel requirements

- Colour- The system is supposed to have a colour that will attract the attention of voters and it should be a colour that is not harmful to users eyes. The colour used must be the same throughout the system. Colours: Blue and White background with black font

- Font size - The System is supposed to have a font size that is easy to read and understand. Important details are supposed to be typed in a visible font size and Bold.

Font size: Arial 12pt

- Navigation – The navigation of the system is supposed be easy to access and use. It must be place on a place where users can easily see it and must be able to direct users throughout the system.
- Help section – The help section of the system must be easy to use and provide users with answers of the Frequently asked question.
- Tooltips – The system must have tooltip that will display some additional information when the user's pointer hover is on a specific element.
- Hotkeys-The system must have hotkeys to help users to perform their tasks more quickly and efficiently. It must be able to help users to do multiple tasks at once.

Operational requirements.

Business rules – The system should have a business rule that will help users to perform their tasks. The business rules should support the policies and requirements of the system.

User workflow - The System must have a clear workflow so that users can easily complete their tasks and it must be able to reduce errors on the system.

Usability attributes – The system must be designed in a manner that users can easily use it, learnable, and enjoyable, users are supposed to feel satisfied when using it.

Required training – the system should be easy to learn and use, it should also provide guide on how to use and understand it.

Installation requirements – the system should be easy to install, setup and maintain on different devices.

Important actions for handling new requirement modifications when putting into place an online voting system for the Independent Electoral Commission (IEC) of South Africa are as follows:

Managing new requirements

1. Identifying Stakeholders:

Consult with important parties, electoral specialists, and relevant organizations to secure support for the recommended requirements.

2. Assessing Socio-Economic and Political Implications:

Take into account aspects such as the system's legality, transparency, and rural/urban split while assessing the socio-economic and political implications of the new requirements.

3. Ensuring Compliance:

Verify that the new specifications meet the independence, truthfulness, sustainability, integrity, transparency, and credibility—the IEC's core competencies.

4. Facilitating Conversations:

Start conversations and consultations to resolve issues and carefully consider the consequences of the new requirements

5. Learning from Comparative Experiences:

Draw insights from other countries' experiences with e-voting systems, both successful and unsuccessful, to inform decision-making and implementation strategies.

6. Addressing Transparency Concerns:

Focus on enhancing transparency in the voting process using technology while considering the critical role transparency plays in the credibility of electoral outcomes.

7. Continuous Evaluation and Improvement:

Acknowledge that voting systems may not produce straightforward outcomes and commit to ongoing evaluation and improvement based on feedback and experiences from other countries.

These steps are crucial for the successful implementation of new requirements in an online voting system for the IEC of South Africa, ensuring transparency, credibility, and efficiency in the electoral process

Feedback and corrections

The project team is on point. The system and database requirements need to be recaptured as these do not conform to system/database requirements.

System requirements

High priority

1. Security and authentication-Ensuring that login is secure and authentication processes to protect voter privacy and prevent fraud

2. Scalability and performance – Designing the system that can handle large volume of users and voter

3. Reliability and uptime – Ensuring that the system is always available and can handle high traffic during peak voting periods.

4. Logging and audit – Developing a comprehensive audit trail and logging system to track all system activities.

Medium priority

1. User-friendly interface-Designing an accessible interface for voters with varying levels of technical expertise

2. Voter registration integration- Streamline the voting process by integrating with existing voter registration systems.

3. Voting result analytics – Providing real-time analytics and insights on voting results

4. Accessibility features-features like text to speech, font size adjustment and screen reader compatibility must be included.

5. Candidate management – It must be easy to manage candidates and voting options.

Low priority

1. Voter reminders and notifications – sending reminders and notifications to voters about the upcoming election and voting deadlines.

Database requirements

High level

1. Scalability and performance – Designing the database that can handle high traffic and large volumes of data

2. Data security and encryption – Ensuring that data is stored, encrypted and secure, and it has access to control.

3. Voter registration data storage – Storing Voter registration information including personal details and voting history

4. Data backup and recovery – ensuring that there is data availability by doing backups and disaster recovery processes.

Medium Priority

1. Candidate data storage – Storing candidate information, descriptions and voting options

2. Voting System Configuration data- storing system configuration data such as settings and preferences

3. Voting results data storage – Storing voting results including vote counts and percentages.

Low Priority

1. System logs and debugging data – Storing the system logs and debugging data for the purpose of troubleshooting and development

2. Voting history data storage – Storing detailed voting history which includes past votes and election participation.

3. Voting system analytics data – storing data for analytics and insights such as voter engagement and election trends.

Phase 5: System Specifications

PURPOSE OF THE SYSTEM

The purpose of the online voting system for IEC South Africa is to modernize and streamline the voting process, making it more convenient, accessible, and efficient for all eligible voters. By allowing voters to cast their ballots from the comfort of their own homes or any location with internet access, the system aims to:

- **Increase Voter Participation:** The online voting system enables more people to participate in the political process, hence strengthening democracy and representation. It does this by removing obstacles like long lines and a restricted number of polling stations.
- **Accessibility:** The system makes sure that everyone has an equal chance to exercise their right to vote, even those who are physically unable to reach polling places due to mobility impairments, disabilities, or other obstacles.
- **Convenience:** Voters do not need to take time off work or reschedule their schedules in order to vote in person because they can cast their ballots at any moment throughout the allotted voting period.
- **Efficiency:** By digitizing the voting process, the system decreases the possibility of errors, speeds up the total counting and reporting of election results, and lessens the administrative burden on election authorities.
- **Security and Integrity:** To protect the confidentiality and anonymity of voters' selections as well as the integrity of the voting process, strong security measures are put in place, including audit trails, authentication procedures, and encryption.
- **Cost-effectiveness:** Eventually, switching to online voting may result in lower expenses for conventional paper-based elections, such as those related to hiring election staff, setting up polling places, and printing ballots.

BACKGRUND OF THE COMPANY

The Independent Electoral Commission (IEC) of South Africa is a constitutional body responsible for overseeing elections at all levels of government within the country. Established in terms of Chapter Nine of the Constitution of South Africa, the IEC operates independently and impartially to ensure free and fair elections that reflect the will of the people.

Here's a background on the IEC:

- **Formation:** The IEC was founded in 1993 to get ready for the 1994 first democratic elections in South Africa. It took the position of the Independent Electoral Commission, which was established to supervise the nation's initial non-racial elections.
- **Constitutional Mandate:** The South African Constitution outlines the mission and responsibilities of the IEC. All facets of the electoral process, such as voter registration, candidate nomination, poll worker supervision, ballot counting, and results announcement, are to be overseen and supported by it.
- **Independence:** The IEC functions without intervention or influence from politics. This independence guarantees a fair and transparent electoral process, as well as election results that fairly represent the electorate's wishes.
- **Accountability and Transparency**: The IEC is dedicated to maintaining accountability and transparency standards in all aspects of its operations. It makes comprehensive information about election rules, methods, and results available to the public so they can examine and confirm the fairness of the electoral process.
- **Inclusivity:** Promoting inclusive participation in the election process is a top priority for the IEC. To make sure that all eligible citizens, including those from underrepresented populations, are aware of their rights and obligations as voters, it conducts comprehensive voter education and outreach programs.
- **Technological Developments**: To increase the effectiveness and accessibility of the election process, the IEC has embraced technological developments over the years. To improve voting and lessen administrative hassles, this includes the deployment of electronic voting machines, online voter registration systems, and other digital technologies.

Customer Acceptance Criteria

The Acceptance Criteria for an internet-based voting system include:

- ✓ Security:
  The system must ensure the confidentiality, integrity, and authenticity of each vote.
- ✓ Accessibility:
  The platform should be accessible to all eligible voters, including those with disabilities, and be available across various devices and internet browsers.
- ✓ User-friendliness:
  The interface should be easy to navigate, catering to users with varying levels of technological proficiency.
- ✓ Accuracy:
  The system should accurately record and tally votes, ensuring the integrity of the voting process.
- ✓ Reliability:
  The platform must be stable and available throughout the duration of the voting period, with minimal downtime or technical issues.
- ✓ Scalability:
  The system should be capable of handling a large volume of concurrent users without experiencing performance degradation.
- ✓ Transparency:
  The voting process should be transparent, allowing voters to verify their choices and providing visibility into the overall electoral process.
- ✓ Compliance:
  The system must adhere to relevant legal and regulatory requirements governing elections and data privacy.
- ✓ Auditability:
  There should be mechanisms in place to audit the voting process and verify the accuracy of the results. ✓ Support:
  Adequate support channels should be available to assist voters with any issues or inquiries they may encounter during the voting process.

Security requirements

1. **Authentication and Authorization**:
   - Robust authentication mechanisms should be in place to ensure that only eligible voters can access the system.
   - Authorization mechanisms should be implemented to grant appropriate permissions to users based on their roles and privileges.
2. **End-to-End Encryption**:
   - All communication between the voter's device and the voting server should be encrypted to prevent eavesdropping and tampering.
   - End-to-end encryption ensures that votes remain confidential throughout the entire process.
3. **Tamper-Resistance**:
   - Measures should be taken to prevent tampering with the voting system, including protections against unauthorized access to the server infrastructure and the integrity of the voting software.
   - Utilize techniques such as digital signatures and cryptographic hashing to ensure the integrity of ballots and voting results.
4. **Voter Anonymity**:
   - The system should guarantee the anonymity of voters, preventing anyone, including the administrators, from tracing individual votes back to specific voters.
5. **Auditability and Transparency**:
   - The system should provide a transparent audit trail that allows for independent verification of the voting process and results.

- This may include cryptographic proofs, paper trails, or other mechanisms to ensure the integrity of the election.

6. **Resilience to Denial-of-Service (DoS) Attacks**:

- Implement measures to mitigate the risk of DoS attacks that could disrupt the voting process by overwhelming the system with traffic.
- This may involve redundancy, load balancing, and rate limiting.

7. **Secure Infrastructure**:

- Ensure that the servers hosting the voting system are securely configured and regularly patched to protect against known vulnerabilities.
- Implement strict access controls and monitoring to prevent unauthorized access to sensitive data.

8. **Backup and Disaster Recovery**:

- Implement robust backup and disaster recovery procedures to ensure that voting data is not lost in the event of hardware failure, natural disasters, or other unforeseen events.

9. **Independent Security Audits**:

- Regular independent security audits should be conducted to identify and address potential vulnerabilities in the voting system.
- Vulnerability disclosure programs can encourage responsible reporting of security issues by external researchers.

10. **Legal and Regulatory Compliance**:

- Ensure that the online voting system complies with relevant laws, regulations, and industry standards related to data privacy, election integrity, and cybersecurity.

Performance and response time requirements

1. **System availability:** the voting system should be available and accessible to voters throughout the period of voting without any significant downtime.
2. **Scalability:** the voting system should handle a larger number of concurrent users during peak voting period, and it shout be more responsive and be able to perform well under heavy loads.
3. **Response time:** the system should respond quickly to voters at times like when they are logging in, selecting candidates and submitting votes.
4. **Security performance:** robust security measures like authentication, encryption and protection against DDoS attacks to safeguard voting data and security integrity being implemented without compromising performance.
5. **Redundancy and failover:** implementing redundancy and failover mechanisms to ensure continuous operation in case there is hardware failure. It will maintain system availability and minimise downtimes.
6. **Monitoring and optimization:** the system should implement a continuous monitor system performance metrics and optimise system components as needed in order to maintain optimal performance levels.
7. **Transaction throughput:** the system should be able to support high transaction throughput to process votes efficiently, such as backend processing of votes, updating database and generating real-time reports

Data backup

1. **Regular backup:** implementing a schedule automatic backups of the voting system data. It can be a schedule of daily, hourly or it can be based on frequency of data updates.
2. **Off-site storage:** storing backups in separate location like cloud storage or any secure off-site facilities. It will help to protect the voting data from any physical damage or loss.
3. **Encryption:** the backup data can be encrypted in order to ensure confidentiality and to prevent unauthorized access, this is more important for sensitive voting data.

4. **Backup verification:** regularly verifying the integrity and completeness of backup in order to ensure that data can be restored accurately. It can be verified by conducting a mock disaster recovery drills which will help in identifying any issues with the backup process.
5. **Versioning:** maintaining multiple versions of backups to restore data from different point in time, it will protect in case of data corruption or errors.
6. **Test restores:** backups being regularly test restored to ensure that data can be successfully recovered and the system can be restored to it functionality state.
7. **Disaster recovery plan:** developing a plan of quickly restoring the system and data in case of disaster or failure.
8. **Compliance:** ensuring that data backup practices comply with relevant laws and regulations of the voting system, especially regarding data protection and privacy.

Report:

When creating the IEC online voting system, several managerial and operational reports are essential for monitoring and ensuring the system's effectiveness. These reports play a crucial role in overseeing the electoral process and maintaining transparency. Based on the provided sources:

1.Financial Management Reports: These reports are essential for monitoring the funds allocated for the development and execution of the online voting system. In addition to ensuring legal compliance, they offer information on financial accountability, procurement procedures, and budget use.

2. Operational Performance Reports: These reports concentrate on the online voting system's operational features, such as performance metrics, system uptime, and the effectiveness of IT operations. They support the assessment of the electoral system's overall performance, security, and reliability.

3. **Reports on System Maintenance:** These provide information on the routine maintenance procedures carried out to guarantee the seamless operation of the online voting system. To properly support corporate processes, they address tasks including system updates, security improvements, and system optimization.

4. **Information and Communication Technology (ICT) Operations Reports**: These reports are essential for keeping an eye on the system's security and stability. They contain details on risk management techniques, disaster recovery procedures, and network infrastructure.

5. **User Engagement and Feedback Reports**: The subject of these reports is citizen input on the online voting platform. They support the process of evaluating user happiness, identifying areas in need of development, and making sure the system satisfies stakeholders' requirements.

6. **Reports on Election Staff Training and Performance Evaluation**: To guarantee staff proficiency with the online voting system, reports on Election Staff Training and Performance Evaluation are crucial. They support the process of determining what training is needed, assessing employee performance, and improving comprehension of electoral rules and regulations.

The IEC can effectively monitor the design, implementation, and functionality of the online voting system and guarantee transparency, effectiveness, and credibility in the electoral process by producing and evaluating these managerial and operational reports.

Hardware Requirements:

The system needs to be compliant with hardware specifications for the machines and gadgets used in the voting process. To guarantee system accuracy, it should offer the best levels of protection against mechanical, thermal, and electromagnetic stresses. Furthermore, in order to maintain the integrity of the voting process, protection should be given top priority in equipment design.

- A backup power supply to keep the system operational in the event of a power loss;
- Tamper-evident hardware seals to detect any illegal physical access to voting equipment;

- Secure servers with high availability and redundancy to manage huge amounts of traffic and voting data

Software requirements:

According to election officials' specifications, the system must accurately record candidates, issues, and contests. It should also guarantee that the right options are recorded exactly as they are. To ensure the security and accuracy of the voting process, the voting system's software has to comply to certain requirements.

Software Conditions

- Strong access controls to restrict and keep an eye on who has access to important system components.
- Enforcing preconditions and ensuring the safe execution of system operations in the required sequence.
- Protections against system failures, fixes, or interventions to maintain system integrity.
- Complete accuracy in the tabulation, reporting, and recording of votes, with no room for error
- Restoring functionality and retrieving voting data following breaks down .
- Additional accuracy measures for DRE systems, such as redundant copies of the original ballot images.
- Data integrity is ensured via parity checks, checksums, and error detection/correction techniques.
- Data read/write quality and error rate monitoring.

In summary, when creating an IEC voting system, it is crucial to adhere to the Voluntary Voting System Guidelines, ensuring that the hardware and software components meet the specified requirements to maintain the integrity and security of the voting process.

Installation

The system is very easy to implement, and it does not require any installation as it will be an online system which can be accessed by any browser. Users will only have to ensure that they have internet access then they can access it.

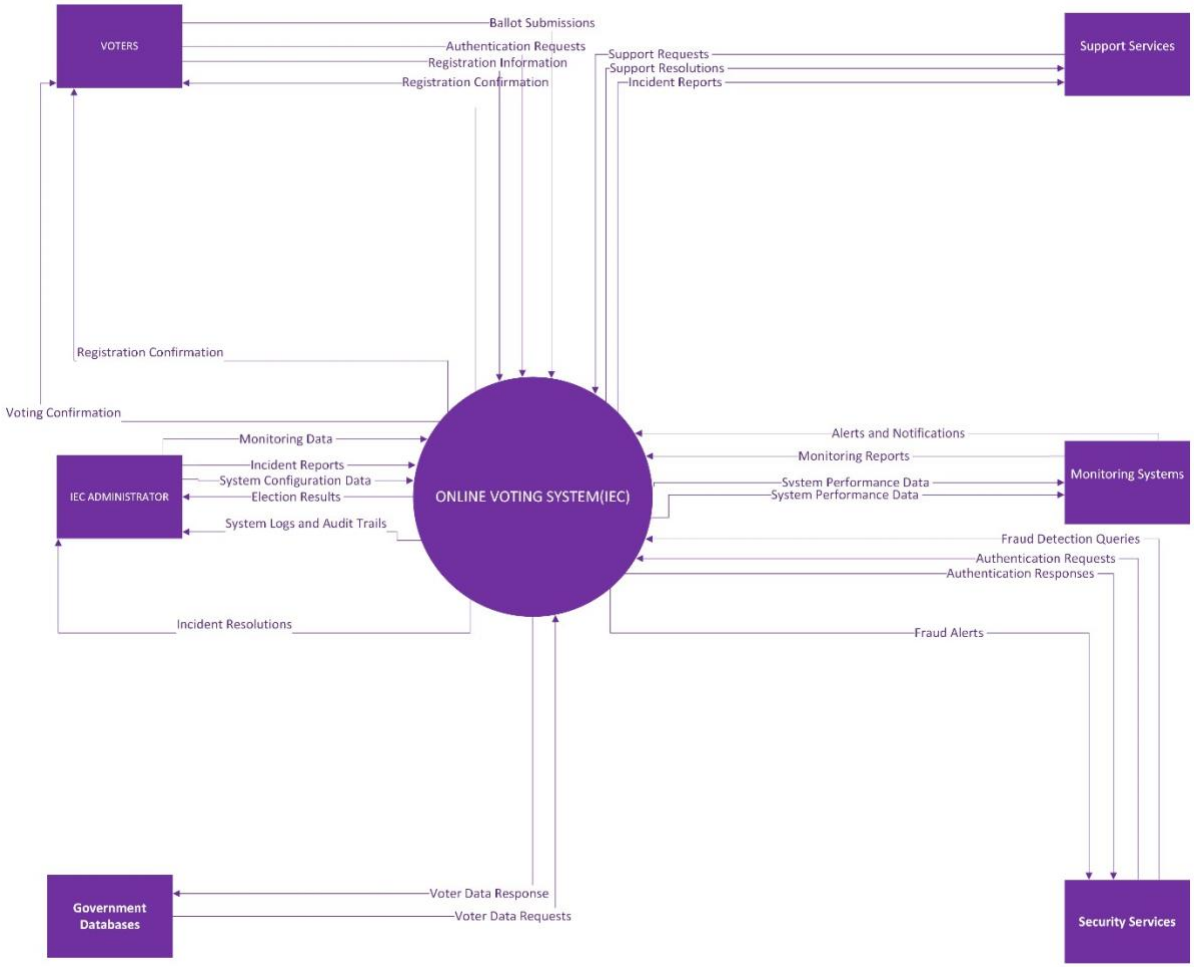
TESTING

The system will go through a series of tests before it can be deployed. First it will be tested by the developers immediately after development. Then it will be tested by a few stakeholders using sample data. Then the system will be tested for scalability to see if it can withstand large amounts of people using sample data as well. Then lastly before it is deployed it will be taken to an independent testing company to ensure that it reaches all the requirements. The system will also be tested continuously to ensure it functions correctly, especially after enhancements have been made.

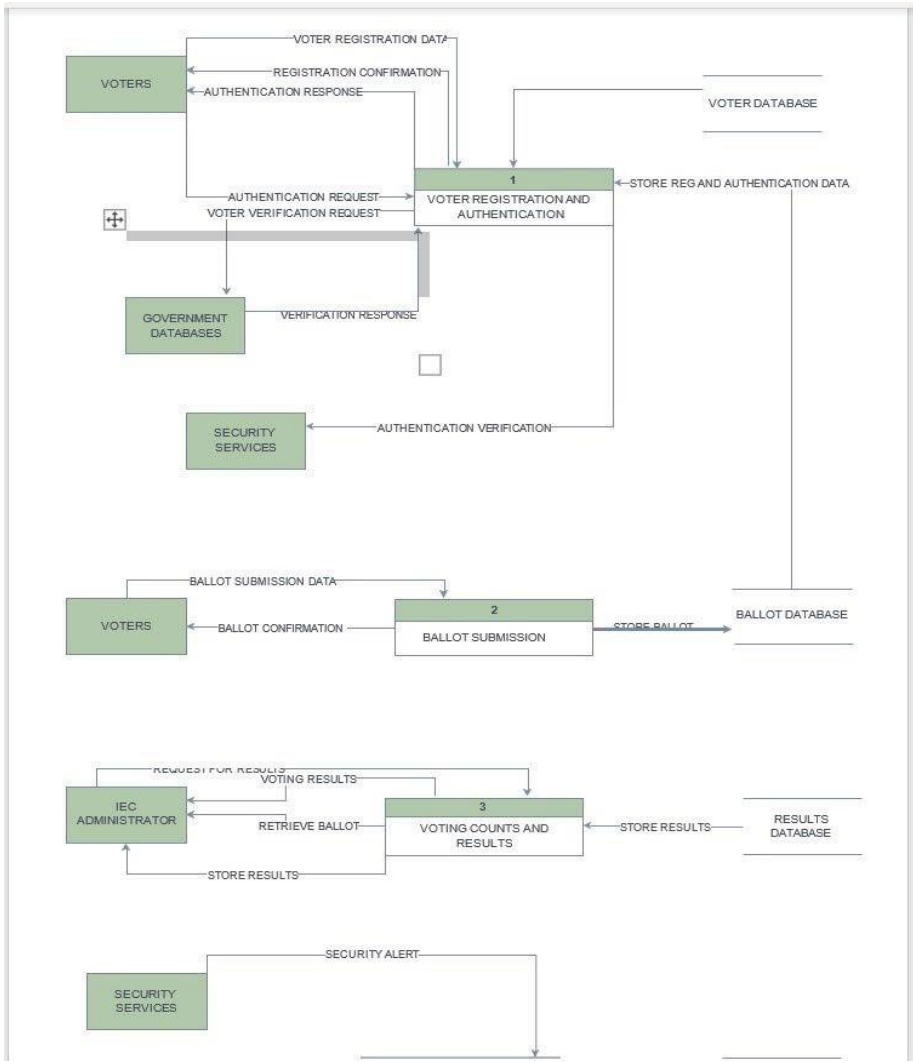
METHODOLOGY

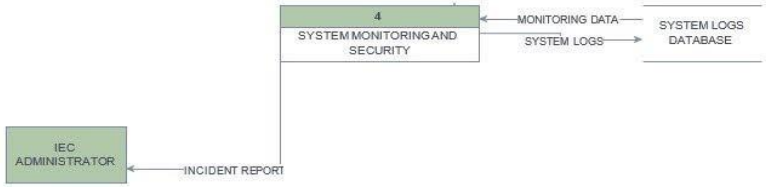
We are going to use the agile methodology as it is the most efficient way to develop high level systems. It will allow us to develop the system and then keep enhancing it as time goes. The methodology is used by all in the software development industry and it is recommended by industry leaders all over the world.

Context Diagram:



DFD(Data Flow Diagam:


VOTERS
VOTER REGISTRATION DATA
REGISTRATION CONFIRMATION
AUTHENTICATION RESPONSE
VOTER DATABASE
1
VOTER REGISTRATION AND AUTHENTICATION
STORE REG AND AUTHENTICATION DATA
AUTHENTICATION REQUEST
VOTER VERIFICATION REQUEST
GOVERNMENT DATABASES
VERIFICATION RESPONSE
SECURITY SERVICES
AUTHENTICATION VERIFICATION
BALLOT SUBMISSION DATA
VOTERS
BALLOT CONFIRMATION
2
BALLOT SUBMISSION
STORE BALLOT
BALLOT DATABASE
VOTING RESULTS
IEC ADMINISTRATOR
RETRIEVE BALLOT
3
VOTING COUNTS AND RESULTS
STORE RESULTS
RESULTS DATABASE
STORE RESULTS
SECURITY ALERT
SECURITY SERVICES


4
SYSTEM MONITORING AND SECURITY
MONITORING DATA
SYSTEM LOGS
SYSTEM LOGS DATABASE
IEC ADMINISTRATOR
INCIDENT REPORT

Data Dictionary:

Voter Table

Field name	Data type	Field size	Description	Example
Voter ID	int	13	Unique ID number of a Voter	0205280227081
First Name	varchar	25	First Name of the Voter	Jane
Last Name	varchar	25	Last Name of the Voter	Smith
Date of Birth	date	10	Voter's date of Birth	2002/05/28
Address	varchar	50	Voter's	205 Albert Street Pretoria 0008
Eligible to Vote	boolean	25	Voter meets the Eligibility requirements	YES

Candidate Table

Field name	Data type	Field size	Description	Example
Candidate ID	int	6	Unique ID for candidate	200022
Name	varchar	25	Candidate name	Mathew Nkosi

Party	varchar	50	The name of the party	African National Congress
Biography	text	255	The biography of the candidate	Date of birth, hometown, Education, and party

Election Table

Field name	Data type	Field size	Description	Example
Election ID	int	6	Unique ID for Election	324004
Election Date	datetime	25	Date for Election	2024/05/2**Error! Bookmark not defined.**
Voting Start time	datetime	25	Time to start voting	07:00am
Voting End time	datetime	25	Time to end voting	0**Error! Bookmark not defined.**:00pm

Vote Table

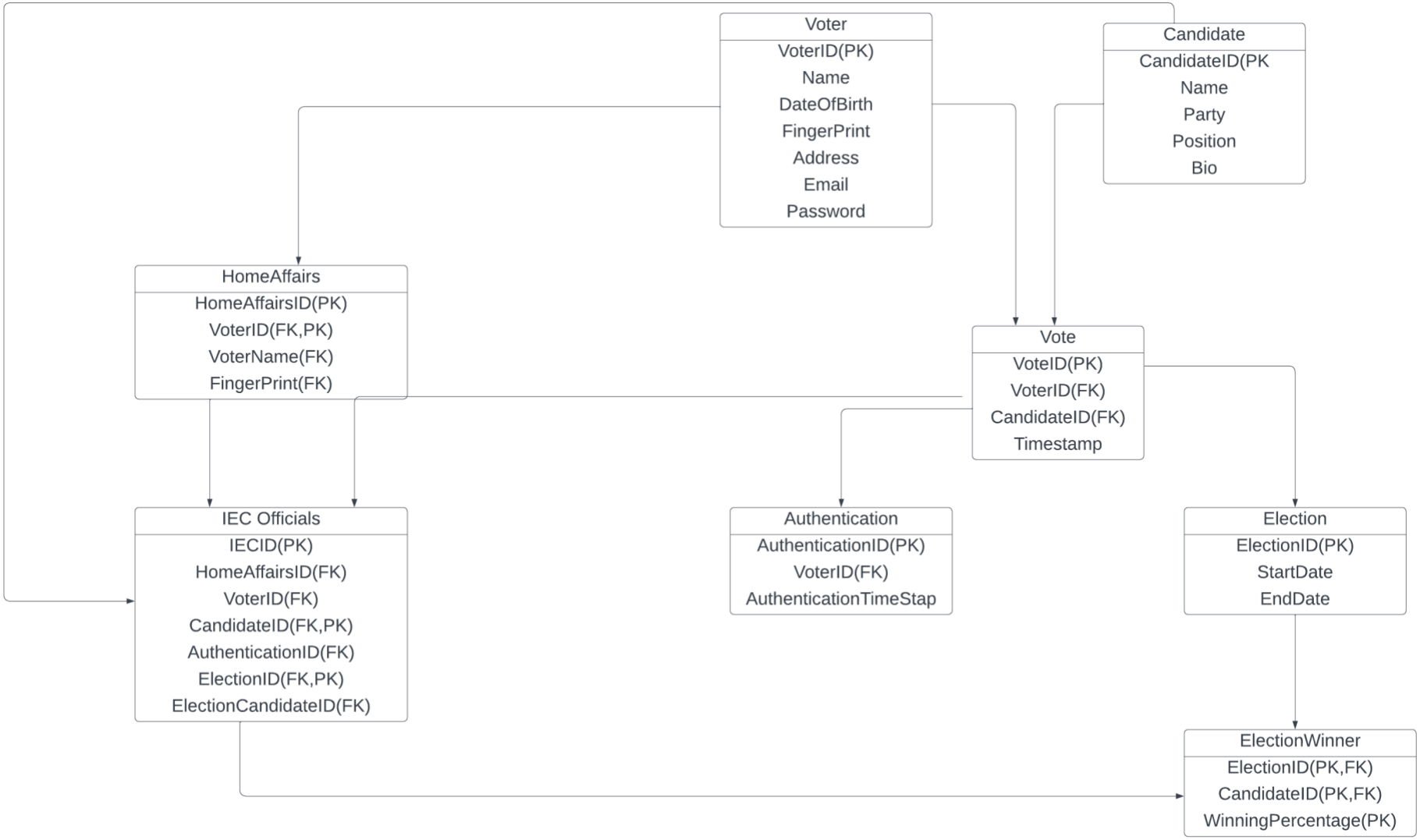
Field name	Data type	Field size	Description	Example
Vote ID	int	6	Unique ID for vote	770047

Voter ID	int	13	foreign key referencing the Voter entity	0205280227081
Election ID	int	6	foreign key referencing the Election entity	324004
Candidate ID	int	6	foreign key referencing the Candidate entity	200022
Vote Cast	boolean	25	Whether a vote has been successfully cast	Successfully

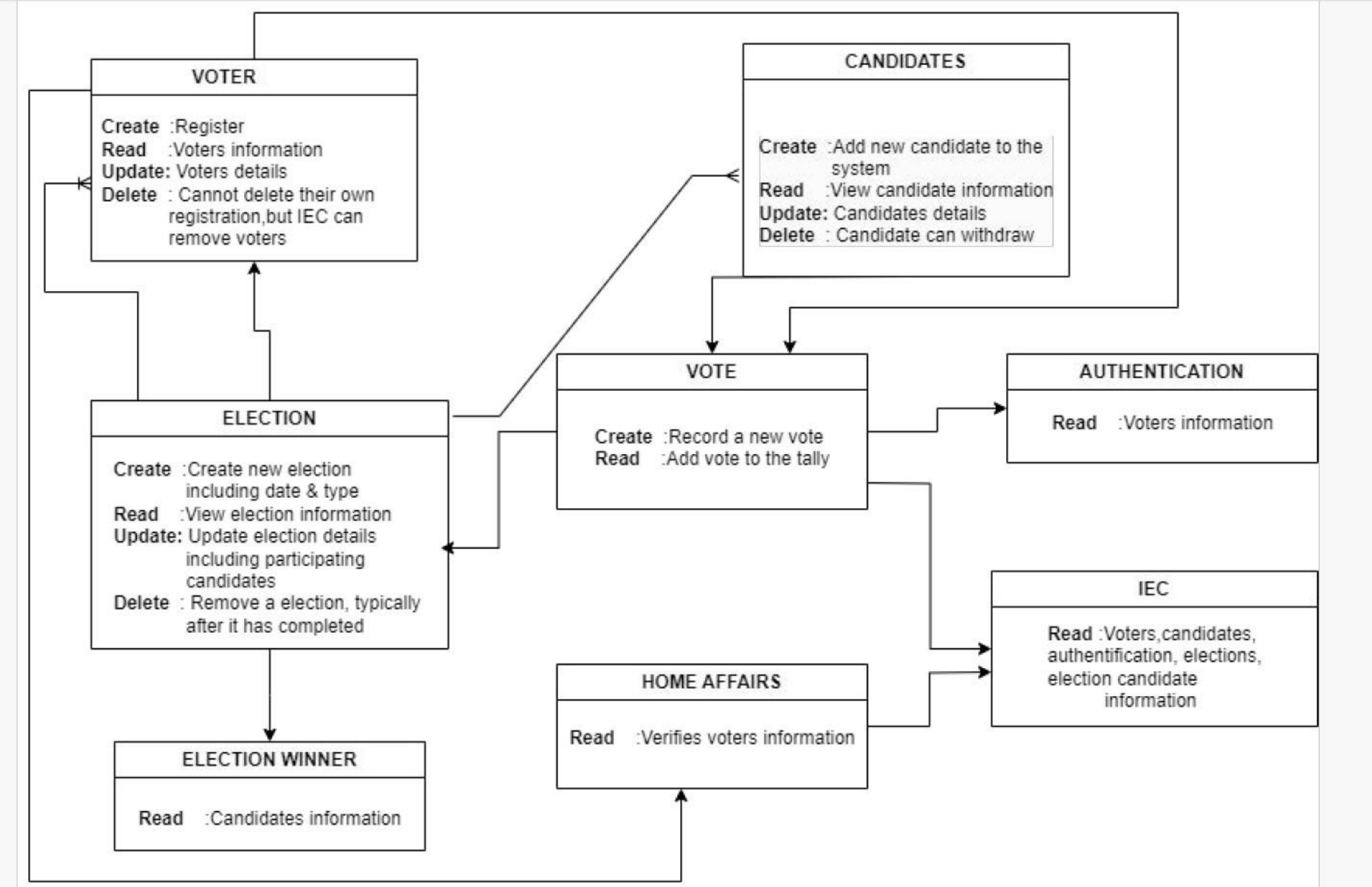
Confirmation Table

Field name	Data type	Field size	Description	Example
Confirmation ID	int	6	Unique ID for confirmation	100011
Vote ID	int	6	foreign key referencing the vote entity	400032
Confirmation Code	varchar	10	Unique code sent to voter	C5J-D43-22

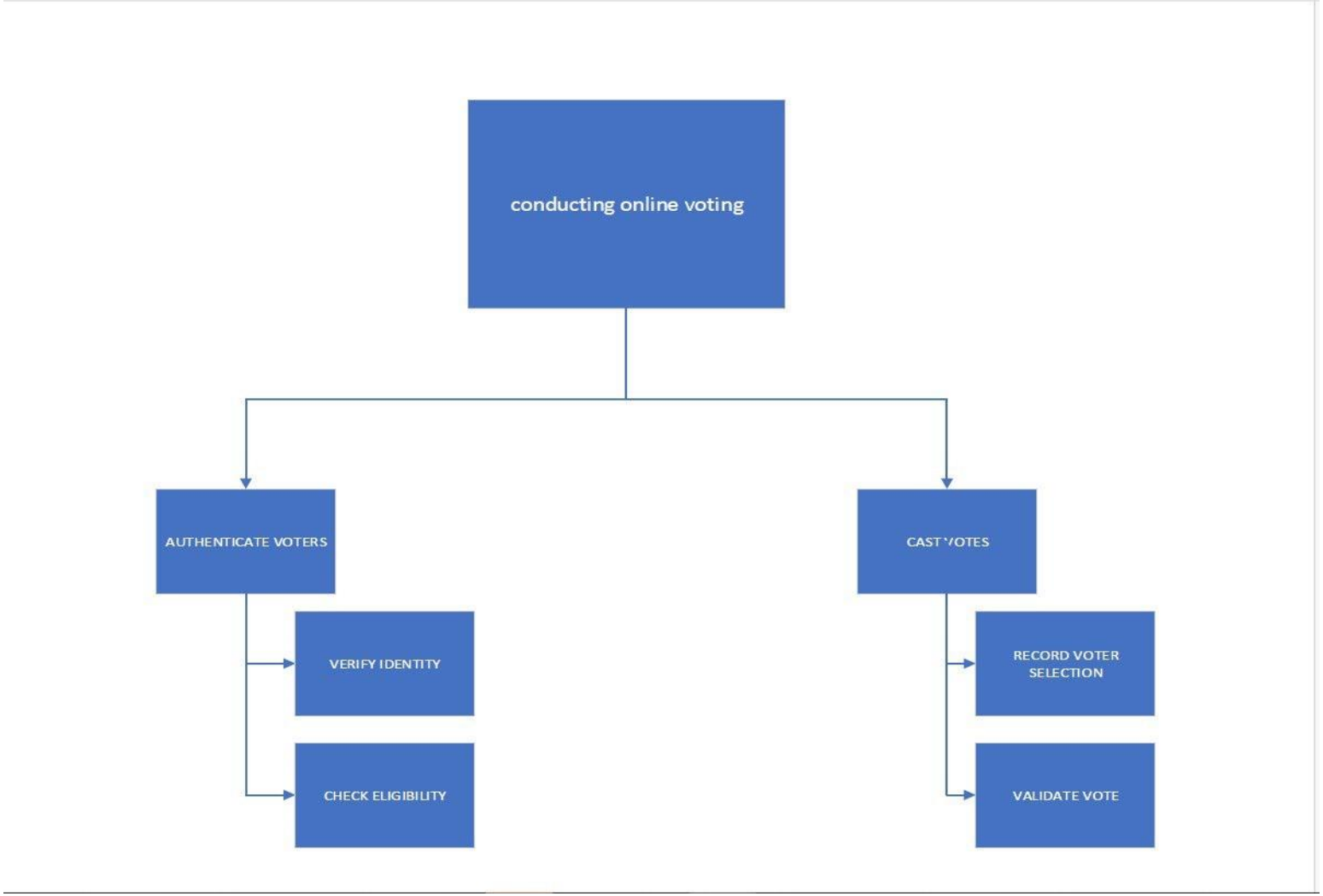
ERD:


Voter
VoterID(PK)
Name
DateOfBirth
FingerPrint
Address
Email
Password
Candidate
CandidateID(PK
Name
Party
Position
Bio
HomeAffairs
HomeAffairsID(PK)
VoterID(FK,PK)
VoterName(FK)
FingerPrint(FK)
Vote
VoteID(PK)
VoterID(FK)
CandidateID(FK)
Timestamp
IEC Officials
IECID(PK)
HomeAffairsID(FK)
VoterID(FK)
CandidateID(FK,PK)
AuthenticationID(FK)
ElectionID(FK,PK)
ElectionCandidateID(FK)
Authentication
AuthenticationID(PK)
VoterID(FK)
AuthenticationTimeStap
Election
ElectionID(PK)
StartDate
EndDate
ElectionWinner
ElectionID(PK,FK)
CandidateID(PK,FK)
WinningPercentage(PK)

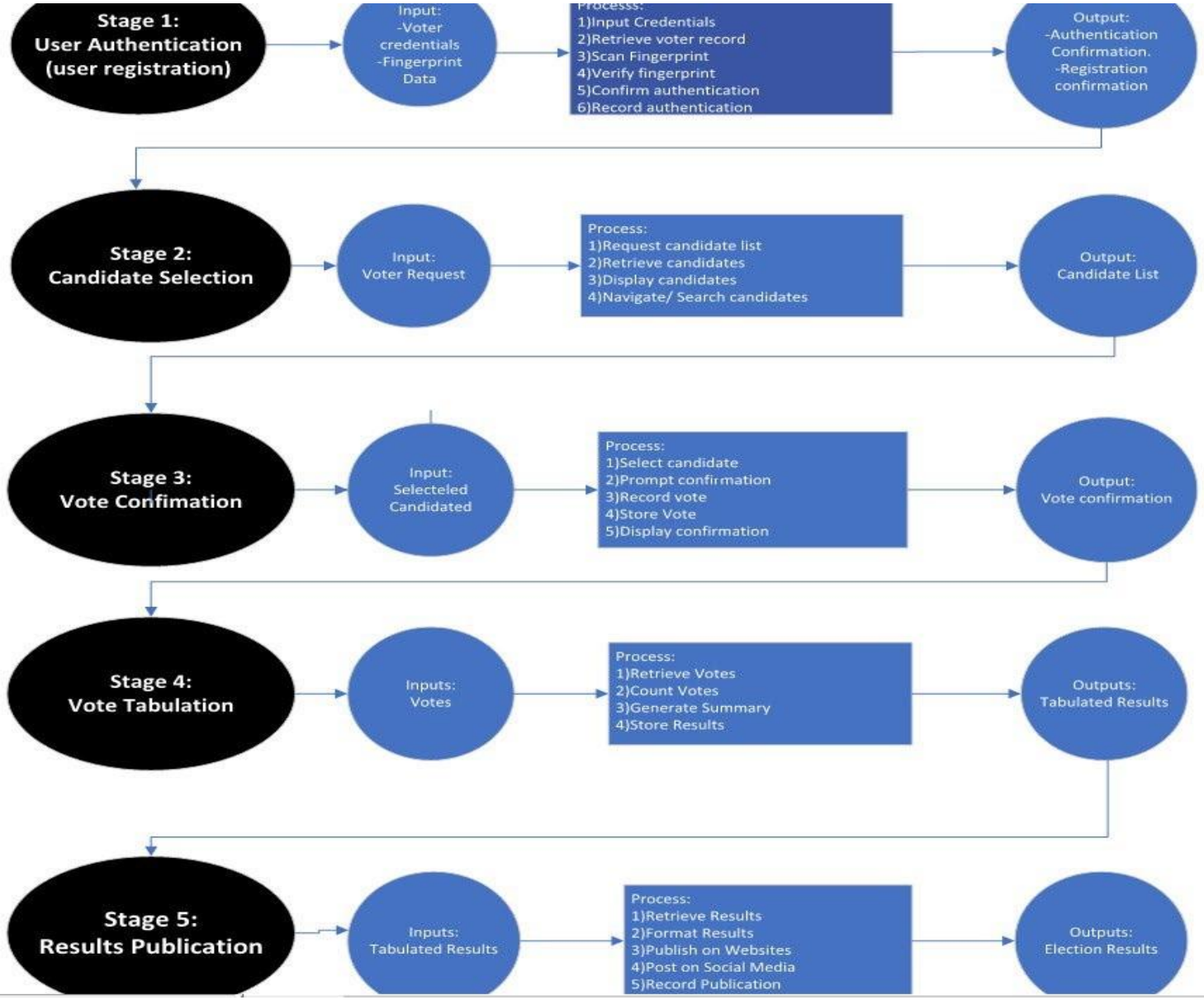
Crud:


VOTER
Create :Register
Read :Voters information
Update: Voters details
Delete : Cannot delete their own registration,but IEC can remove voters
CANDIDATES
Create :Add new candidate to the system
Read :View candidate information
Update: Candidates details
Delete : Candidate can withdraw
VOTE
Create :Record a new vote
Read :Add vote to the tally
AUTHENTICATION
Read :Voters information
ELECTION
Create :Create new election including date & type
Read :View election information
Update: Update election details including participating candidates
Delete : Remove a election, typically after it has completed
IEC
Read :Voters,candidates, authentification, elections, election candidate information
HOME AFFAIRS
Read :Verifies voters information
ELECTION WINNER
Read :Candidates information

Functional Decomposition Diagram:



Process Specification Diagram:


Stage 1:
User Authentication
(user registration)
Input:
-Voter
credentials
-Fingerprint
Data
Processs:
1)Input Credentials
2)Retrieve voter record
3)Scan Fingerprint
4)Verify fingerprint
5)Confirm authentication
6)Record authentication
Output:
-Authentication
Confirmation.
-Registration
confirmation
Stage 2:
Candidate Selection
Input:
Voter Request
Process:
1)Request candidate list
2)Retrieve candidates
3)Display candidates
4)Navigate/ Search candidates
Output:
Candidate List
Stage 3:
Vote Confimation
Input:
Selecteled
Candidated
Process:
1)Select candidate
2)Prompt confirmation
3)Record vote
4)Store Vote
5)Display confirmation
Output:
Vote confirmation
Stage 4:
Vote Tabulation
Inputs:
Votes
Process:
1)Retrieve Votes
2)Count Votes
3)Generate Summary
4)Store Results
Outputs:
Tabulated Results
Stage 5:
Results Publication
Inputs:
Tabulated Results
Process:
1)Retrieve Results
2)Format Results
3)Publish on Websites
4)Post on Social Media
5)Record Publication
Outputs:
Election Results

Phase 6: System test plan

Introduction to Phase 6

This document details how we are going to test the systems that we are going to implement. It details how tests are going to be performed and who will be conducting which tests.

This is a crucial part of the development process and must be performed before the system is deployed to ensure that the system has no errors, and it can run accordingly.

Relationship to other documents

This document is related to all the other documents because it states how we are going to validate this project. Without this document we would not know how we are going to confirm

whether our project works well or not. It is going to state different test cases and scenarios and then tell us how to confirm whether the project is working or not.

it relates to other documents because it dictates whether the other documents are correct or not.

System Overview

Purpose

Our Online Voting System aims to modernize the voting process by transitioning from traditional pen-and-paper methods to a secure, efficient, and user-friendly online platform. This system addresses issues such as manual vote counting, long queues, and voter fraud, ensuring a more reliable and streamlined electoral process.

Key Features

1. **User Authentication**:
    - Secure login using email and password.
    - Biometric authentication with fingerprint scanning.
    - Integration with the Home Affairs System to verify voter identity and prevent ghost voting.
2. **Candidate Selection**:
    - Display candidates in alphabetical order, 20 per page.
    - Search functionality to quickly find preferred candidates.
3. **Vote Casting and Confirmation**:
    - Easy-to-use interface for selecting and confirming votes.
    - Prompt for vote confirmation before final submission.
4. **Automated Vote Tabulation**:
    - Real-time vote counting and result generation.
    - Graphical representation of election outcomes.
5. **Results Publication**:
    - Immediate display of election results on the IEC website and social media platforms.
    - Detailed results showing the number of votes each candidate received.
6. **Security and Compliance**:
    - End-to-end encryption for secure data transmission.
    - Regular security assessments and monitoring for threats.
    - Compliance with electoral laws and regulations.

System Architecture

The Online Voting System is composed of several interconnected components, each responsible for specific functionalities. The architecture includes:

1. **Frontend**:
    - User interface for voters to authenticate, select candidates, and confirm votes.

- Accessible via web browsers on desktops, tablets, and smartphones.

2. **Backend**:
    - Application server managing business logic, authentication, and vote processing.
    - Secure communication with external systems (e.g., Home Affairs System).
3. **Database**:
    - Voter Information Database: Stores voter details and fingerprint data.
    - Candidate Database: Stores information about candidates.
    - Vote Database: Records cast votes and associated metadata.
    - Authentication Database: Logs authentication attempts and timestamps.
4. **External Systems**:
    - Home Affairs System: Verifies voter identity using national records.
    - IEC Website and Social Media: Publishes election results.

Workflow

1. **User Authentication**:
    - Voter logs in with email and password.
    - System prompts for fingerprint scan.
    - System verifies credentials and fingerprint with the Home Affairs System.
    - Upon successful authentication, voter accesses the voting interface.
2. **Candidate Selection**:
    - Voter navigates through candidate list or uses the search bar.
    - Voter selects a candidate and proceeds to the confirmation screen.
3. **Vote Confirmation**:
    - Voter confirms the selected candidate.
    - System records the vote in the Vote Database.
    - Voter receives a confirmation message.
4. **Vote Tabulation and Results Publication**:
    - At the end of the voting period, the system aggregates votes.
    - Tabulated results are formatted for publication.

- Results are displayed on the IEC website and shared on social media.

Organizational Structure

1. **Project Manager**: (Neo Mokoatle)
    - Oversees project scope, schedule, and budget.
    - Coordinates activities between teams and stakeholders.
2. **Technical Developer**: (Thembelihle Mabanga)
    - Responsible for development, deployment, and maintenance of the system.
3. **Security and Compliance**: (Thato Lesudi)
    - Ensures the security and integrity of the voting system.
    - Conducts regular security assessments.
4. **Infrastructure Team**: (Tisetso Maila and Masungu Shiviti)
    - Manages servers, databases, and network infrastructure.
    - Ensures system availability and performance.

Benefits

- **Efficiency**: Automated vote counting and real-time result generation.
- **Security**: Robust authentication and data encryption to prevent fraud.
- **Accessibility**: Convenient online access for voters, reducing the need for physical presence.
- **Transparency**: Clear and immediate publication of results.

Features to be tested:

1. Control Mode (Test Mode):
This feature makes it possible to simulate different situations and states in order to evaluate the behavior and functionality of the system. It is very helpful for confirming that the system is operating correctly in various operational scenarios.

2. Simulation:

To test the behavior and performance of the system, this function allows the simulation of different settings and scenarios. It is helpful for confirming that the system is operating correctly under various operational circumstances.

3. Functional Safety:
Testing the system for functional safety involves verifying that it can perform appropriately and safely in a variety of scenarios. This covers testing for fault tolerance, maintainability, and reliability.

4. Software Validation and Verification:
The system's software needs to undergo extensive testing in order to be validated and verified. This covers accuracy, dependability, and performance testing.

5. Risk-Based Testing:
A risk-based strategy, which ranks testing according to the degree of risk connected with each feature or function, should be used to test the system. This guarantees that the system's most important components are adequately tested.

Features not be tested:

1. Hardware Integration Testing:
This is not required because the system is up and running. The hardware components of the system have already been assembled and individually tested.

2. Offline Numerical Analysis:
An online system does not require offline numerical analysis. Dynamically testing the system's behavior and performance while it's in operation

3. Testing of Data Analysis and Recording:
An online system does not require testing of data analysis and recording. During operation, the system's capacity for data recording and processing can be dynamically checked.

4. Certification of Tools and Translators:
An online system does not require the certification of tools or translators. The translators and tools in the system are already integrated and certified.

5. Equivalency classes and input partition testing:
An online system does not require input partition testing or equivalency classes. During operation, the behavior and performance of the system can be dynamically tested.

To guarantee that the online IEC system functions accurately, securely, and effectively, these aspects ought to be verified and tested.

Describe the generic pass/fail criteria to be used for the online voting system.

1. **Authentication and authorization**:
    - **Pass**: The system verifies that only the voters can access the system and are able to vote in the specific election. The voters' identities and voting rights are verified and protected throughout the process of voting.
    - **Fail**: The voters not having access to the system and no being able to select the specific election they want. The voters' identities not verified and protected throughout the voting process which may lead to duplicate registrations.
2. **Voter Registration**:
    - **Pass**: The system verifies that the voter's personal information is accurate and completed, and that the voter meet the eligibility criteria to cast a vote in the special election. To also verify that the voter's details match the information stored in the voter registry of the system to prevent fraudulent registration.
    - **Fail**: The system cannot able to verify that the voter's details provided matches with the information in the voter registry and allowing duplicate registrations. The system cannot verify that the voter meets the eligibility criteria to cast a vote.
3. **Voting process**:
    - **Pass**: The system can confirm that the voter's vote can be successfully casted and recorded, and that the recorded cast is secure and accurate. The voter gets the vote confirmation is sent to the voter verifying that the vote is casted and recorded and the system ensures that the voting process is complies with relevant voting regulations and laws.

- **Fail**: The voter encounter errors when casting votes which may lead to vote not being accurate and some wrong vote being recorded or not recorded at all. The voter no receiving vote confirmation that can verify if the vote was successful.

4. **Vote storage and security**:
    - **Pass**: The system can store the vote securely after the voter cast it and with proper encryption. The stored votes are protected from being tampered with or accessed by unauthorized users.
    - **Fail**: The system storing the votes without sufficient security measures that can make the vote secure. Unauthorized users can access the stored vote and temper with them.
5. **Voting counting and results**:
    - Pass: The system counts the votes accurately and the counting is secure and temper evident as well as being protected from unauthorized users. The counted votes reflect the correct number of votes casted for each option. The system updates result in real-time.
    - **Fail**: The system not counting the votes accurately and the counting not being secure, this leading to it being accessed by unauthorized users. The counted votes not reflecting the correct number of votes casted and not updating results in real-time.
6. **Scalability and performance**:
    - Pass: The system is always available and accessible to voters during the voting period, and it can handle a larger number of concurrent voters. The voters can cast their votes quickly and efficiently.
    - **Fail**: The voters are not able to access the system during the voting period, and it can not handle a large number of concurrent voters. The system being slow when the voters are casting their votes.

Describes the general approach to the testing process.

1. REQUIREMENT ANALYSIS

Recognize the Needs: Make sure you fully comprehend and record the system's functional and non-functional needs. This covers the needs of the user, security requirements, performance benchmarks, and legal compliance.

Risk assessment: Determine any threats and weaknesses, like security lapses, system outages, and usability problems, that might influence the voting process.

2. TEST PLANNING

Specify the Test Objectives: Clearly state the goals of the testing procedure, together with the things that must be examined and the results that should be anticipated.

Test Approach: Create a thorough testing plan that addresses all system facets, such as user acceptability, security, performance, unit, integration, and system testing.

Planning Resources: Determine the people, equipment, and testing settings that are needed.

Test Timetable: Make a thorough testing schedule activities, ensuring alignment with the overall project timeline.

3. TEST DESIGN

Developing Test Cases: Write thorough test cases for every facet of the system. This ought to consist of:

Unit tests: To confirm the functionality and individual parts.

Integration tests: To make sure various modules and parts function together as they should.

System tests: To confirm that the system meets the criteria and functions as intended generally.

Security tests: To find weak points and make sure the system is safe from intrusions.

Performance tests, such as stress and load testing, are used to evaluate the system's performance under various circumstances.

Usability tests: To guarantee that all voters can easily navigate and utilize the system.

Test Data Preparation: To ensure thorough testing, create realistic test data that closely resembles real user data.

4. ENVIRONMENT SETUP

Establish a test environment that is identical to the production setting as nearly as feasible.
Configuration Management: To preserve the uniformity and integrity of the test environment, make sure that appropriate configuration management procedures are followed.

5. TEST EXECUTION

Execute Test Cases: Follow the test plan when executing the test cases. This comprises:

Automated Testing: For lengthy and repetitive test cases, use automated technologies.

Manual Testing: Carry out manual testing in situations where usability testing and human judgment are needed.

Keep Track of Results: Keep track of each test case's results, noting any variations from anticipated results.

6. DEFECT MANAGEMENT

Determine Errors: Record any flaws or problems that are found during testing.

Make Defects a Priority: Sort flaws according to their seriousness and systemic influence.

Resolve Issues: Assist the development team in resolving issues by fixing detected defects and doing tests again.

7. REGRESSION TESTING

Retest the System: Perform regression testing following defect fixes to make sure that modifications haven't brought up any new problems and that the system is still stable.

8. USER ACCEPTANCE TESTING(UAT)

Involve the Parties: Involve actual users and stakeholders in a controlled system test.

Feedback: Get end users' opinions on the system's performance, functionality, and usability.

Include Modifications: Based on user feedback, make the appropriate adjustments and revalidate the changes.

9. SECURITY AND COMPLIANCE TESTING

Penetration Testing: To find and fix possible security flaws, thoroughly test for penetrations.

Verify that the system complies with all applicable legal and regulatory requirements by performing compliance checks.

10. PERFORMANCE AND LOAD TESTING

Simulate Load: To make sure the system can withstand peak voting times without experiencing performance deterioration, test it under varied load circumstances.

Examine Performance: Find any areas where the system is performing poorly and improve its efficiency.

11. FINAL VALIDATION AND SIGN-OFF

Testing from end to end: Conduct a last round of end-to-end testing to make sure everything works flawlessly and replicates the real voting process from beginning to end.

Examine the test results one last time and obtain clearance from all relevant parties, such as end users, performance analysts, and security specialists.

Documentation: To help guide future testing procedures, keep a record of all testing operations, outcomes, and lessons discovered.

12. DEPLOYMENT TESTING

Staging Environment: To verify the deployment procedure, deploy the system in a staging environment that closely resembles the production environment.

Verify that the system functions as intended in the staging environment and that the deployment procedure goes without a hitch.

13. MONITORING AND MAINTENANCE

Continuous Monitoring: After deployment, put monitoring tools in place to keep an eye on the security and functionality of the system in real time.

Frequent Updates: To handle any new security risks or performance problems, schedule routine updates and maintenance.

User Support: Offer users continuous assistance and make sure there is a system in place for reporting and resolving problems that come up during the actual voting times.

Key Considerations

Security: Given the sensitivity of an online voting system, security testing must be rigorous. This includes encryption, secure communication channels, multi-factor authentication, and regular security audits.

Scalability: The system must be able to handle a large number of users simultaneously, especially during peak voting times.

Accessibility: Ensure the system is accessible to all users, including those with disabilities, following international standards for web accessibility.

Compliance: Ensure the system complies with South African electoral laws and international standards for electronic voting systems.

Transparency and Trust: Build features that promote transparency and trust, such as verifiable audit trails, voter receipts, and robust mechanisms for verifying voter identity without compromising privacy.

Standards for Testing Suspensions

If any of the following serious problems occur, IEC South Africa's online voting system testing should be put on hold:

- **Breach of System Security :**

Identification of any unapproved penetration or access to the system significant flaws found that could jeopardize election integrity or voter data.

- **Important Functionality Deficit :**

malfunction in key features such voting casting, calculating votes, voter authentication, or result reporting severe flaws that make it impossible for the system to consistently carry out necessary functions.

- **Problems with Data Integrity**:

voting records or votes being lost or tampered with Inconsistencies in vote tallying that cannot be remedied soon.

- **Degradation of Performance:**

Throughput or system reaction times falling short of allowable limits, particularly during periods of high utilization.

The system's failure to manage the anticipated demand, which results in crashes or noticeable lags.

- **Violations of Compliance:**

Finding of violations of security, legal, or regulatory requirements unique to electronic voting system matters that transgress the voting process's availability, confidentiality, and integrity.

- **Extreme Usability Problems:**

Voters are unable to accurately cast their ballots due to interface problems difficulties with accessibility that make it difficult for some user groups to use the system efficiently.

Activities to Repeat When Testing is Resumed

To guarantee system stability and dependability, the following test tasks must be carried out once the key problems that led to the suspension have been resolved:

1) Testing for Regression:

To ensure that the deployed fixes have not resulted in the introduction of new flaws, thoroughly test the regressions.
Make that the tests that passed before the modifications still pass.

2) Testing for security:

Verify that security breaches have been fixed by conducting penetration tests and vulnerability assessments on the system once more.
Verify that any recently implemented security measures are operating as intended.

3) Testing for core functionality:

Rerun test cases pertaining to essential features including voting casting, counting votes, voter authentication, and result reporting.
Verify that there are no problems and that these functions are operating as intended.

4)Testing for data integrity:

To confirm that data integrity has been restored, run tests. Check the accuracy and consistency of the voter data and votes.

5) Testing for performance and load:

To ensure the system can withstand the anticipated load without experiencing any deterioration, rerun the load and performance tests.
Verify that the system performs as expected under a range of circumstances.

6) Testing for Compliance:

Reassess the system in light of the needs for security, law, and regulation compliance.
Make sure that no compliance rules are broken by any changes that are made.

7) Testing for Usability and Accessibility:

To ensure that the system is accessible and easy to use, assess its usability.
Make sure that everyone who wants to vote can utilize the system, including people with disabilities.

8) Testing from end to end:

Verify the voting process's overall functionality and component integration by running a thorough end-to-end test.
Make certain that the whole voting procedure, from voter registration to the outcome, Reporting functions flawlessly.

List of all possible test cases

Test case ID	Test Case Description	Preconditions	Test Steps	Expected Results
01	User Login with valid credentials	Voter is registered in the system	1)Navigate to login 2) Enter valid email and password 3)Click “Login”	User is authenticated and redirected to the voting page
02	User Login with invalid credentials	None	1)Navigate to login page 2) Enter invalid email or password 3) Click "Login"	Error message displayed: "Invalid credentials"
03	Fingerprint Authentication with valid data	User is logged in	1) Prompt for fingerprint scan 2) Scan valid fingerprint	Fingerprint is verified and user is authenticated

04	Fingerprint Authentication with invalid data	User is logged in	1)Prompt for fingerprint scan 2)Scan invalid fingerprint	Error message displayed: "Fingerprint mismatch"
05	Display candidate list	User is authenticated	1)Request candidate list	List of candidates is displayed (20 per page, alphabetical order)
06	Search candidate by name	User is authenticated and candidate list is displayed	1) Select a candidate from the list 2) Click "Vote"	Candidate is selected and prompt for confirmation is displayed
07	Select candidate to vote for	User is authenticated and candidate list is displayed	1)Select a candidate from the list 2)Click "Vote"	Candidate is selected and prompt for confirmation is displayed
08	Confirm vote	User has selected a candidate	1) Click "Confirm"	Vote is recorded, confirmation message is displayed
09	Vote without confirmation	User has selected a candidate	1)Navigate away without confirming	Vote is not recorded, user can re-select candidate
10	Prevent double voting	User has already voted	1) Attempt to vote again	Error message displayed:

				"You have already voted"
11	View election results	Voting period has ended	1. Navigate to results page	Election results are displayed
12	Secure vote data transmission	User is voting	1) . Monitor data packets during voting	Data is encrypted during transmission
13	Verify vote tabulation	Voting period has ended	1)Retrieve votes from database 2) Count votes for each candidate	Total vote count matches the number of votes cast
14	Publish election results	Vote tabulation is complete	1) Format results 2)Publish on IEC website 3) Post on social media	Results are published on IEC website and social media, timestamp recorded
15	Unauthorized access attempt	None	1) Attempt to access voting page without authentication	Access is denied, user is redirected to login page
16	System performance under load	High number of concurrent users	1) Simulate multiple users logging in and voting simultaneously	System remains responsive, no crashes or significant delays

17	Data integrity check	System is running	1)Inspect database records for votes 2)Verify no duplication or tampering	All records are unique and untampered
18	User logout	User is logged in	1) Click "Logout" button	User is logged out and redirected to the login page

Test Schedule

Phase 1: Unit Testing

Week	Testing Activities	Responsibilities	Risks	Contingencies
1	- Develop unit test cases - Test authentication module	-Software Engineer -Technical Development Team	-Incomplete test coverage -Module interdependencies may cause issues to go undetected	- Ensure comprehensive test cases -Mock dependencies during unit testing
2	- Test candidate selection module - Test vote recording module	-Technical Development Team -Software Engineers	- Missing edge cases - Potential for false positives or negatives	- Review test cases with peers - Use test-driven

				development practices

Phase 2: Integration Testing

Week	Testing Activities	Responsibilities	Risks	Contingencies
3	- Integrate authentication and candidate selection modules - Test data flow between modules	-Technical Development Team -Software Engineers	- Integration issues - Data inconsistencies	- Perform thorough integration testing - Use test data that covers all scenarios
4	- Integrate vote recording and tabulation modules - Test end-to-end data flow	-Technical Development Team -Software Engineers	- Inter-module communication failures - Potential performance bottlenecks	- Use automated integration tests - Monitor performance metrics

Phase 3: System Testing

Week	Testing Activities	Responsibilities	Risks	Contingencies
5	- Conduct full system testing - Test all functional requirements	-Quality Assurance Team -System Testers	- Uncovered bugs - System may not meet all functional requirements	- Detailed test plan covering all requirements - Regular reviews and updates

6	- Perform load and stress testing - Evaluate system performance under high load	-Quality Assurance Team -System Testers	- System crashes - Performance degradation	- Use load testing tools - Identify and address performance bottlenecks
7	- Test security features - Conduct vulnerability assessments	-Security and Compliance Team -Security Analysts	- Security vulnerabilities - Data breaches	- Regular security audits - Immediate patching of discovered vulnerabilities

Phase 4: User Acceptance Testing (UAT)

Week	Testing Activities	Responsibilities	Risks	Contingencies
8	- Conduct UAT with a group of end-users - Gather feedback on usability and functionality	-Project Management Team -Selected End-users	- User dissatisfaction - Usability issues	- Incorporate user feedback - Conduct iterative testing and improvements
9	- Validate all user-reported issues - Ensure system meets user expectations	-Project Management Team -Technical Development Team	- Unresolved issues - Missed requirements	- Address all reported issues promptly - Reassess requirements and expectations

Phase 5: Final Testing and Deployment

Week	Testing Activities	Responsibilities	Risks	Contingencies
10	-Conduct final regression testing - Verify all previous issues are resolved	-Quality Assurance Team -Technical Development Team	- New bugs introduced - Regression failures	- Maintain a comprehensive regression suite - Prioritize critical bug fixes
11	- Prepare deployment plan - Execute final system deployment	-Project Management Team -Infrastructure Team	- Deployment failures - Downtime during deployment	- Detailed deployment checklist - Backup and rollback plans

Test Responsibilities

- **Project Management Team**: Oversee the entire testing process, ensure milestones are met, and coordinate between teams.
- **Technical Development Team**: Develop unit tests, perform integration tests, and fix identified bugs.
- **Quality Assurance Team**: Conduct system testing, load/stress testing, and regression testing.
- **Security and Compliance Team**: Perform security assessments and ensure compliance with regulations.
- **Infrastructure Team**: Manage deployment and ensure system stability during testing phases.
- **Selected End-users**: Participate in UAT to validate system functionality and usability

Risks and Contingencies:

1) **Incomplete Test Coverage**:

- **Risk**: Some parts of the system may not be tested thoroughly.
- **Contingency**: Develop a comprehensive test plan covering all system aspects, and regularly review and update test cases.

2) **Integration Issues**:

- **Risk**: Modules may not work seamlessly when integrated.
- **Contingency**: Perform thorough integration testing with test data covering all scenarios, and mock dependencies where necessary.

3) **Performance Bottlenecks**:

- **Risk**: The system may perform poorly under high load.
- **Contingency**: Use load testing tools to simulate high load conditions, monitor performance metrics, and address bottlenecks.

4) **Security Vulnerabilities**:

- **Risk**: The system may have security flaws that could be exploited.
- **Contingency**: Conduct regular security audits, vulnerability assessments, and patch discovered vulnerabilities immediately.

5) **User Dissatisfaction**:

- **Risk**: Users may find the system difficult to use or have other usability issues.
- **Contingency**: Gather user feedback during UAT and incorporate improvements iteratively.

6) **Deployment Failures**:

- **Risk**: Issues may arise during system deployment.
- **Contingency**: Prepare a detailed deployment checklist, backup the system, and have rollback plans in place.

References

((IEC), 1994)

(Büthe, 2017) (Nic Cheeseman, 2020 September)

(Lekorwe, 2006)

IEC Home - Electoral Commission of South Africa (elections.org.za)

Electoral Commission of South Africa. (n.d.). About the IEC. Retrieved from https://www.elections.org.za/About-Us/About-the-IEC/

Republic of South Africa. (1996). Constitution of the Republic of South Africa, 1996. Government Gazette, 378(17678).

[1] https://www.elections.org.za/content/WorkArea/DownloadAsset.aspx?id=2075

[2] https://www.elections.org.za/content/Documents/Annual-reports,-reports-and-strategic-documents/Annualreports---IEC/2023-IEC-Annual-Report-%28Double-page-Spreads%29/

[3] https://pmg.org.za/committee-meeting/32819/

[4] https://www.elections.org.za/content/Documents/Election-reports/National-and-Provincial-Elections/2019-National-and-Provincial-Elections-Report-%28PDF%29/

[5] https://pmg.org.za/committee-meeting/38023/

[6] B Springer - 2022 - morrisoninstitute.asu.edu. Examining the Ease of

[7] Voting in Arizona. asu.edu

[8]
[9] SJ Turnbull-Dugarte, D Devine - Electoral Studies, 2023 -
[10] Elsevier. Support for digitising the ballot box: a systematic review of ivoting pilots and a conjoint experiment. sciencedirect.com
[11] Cited by **1**
[12]
[13] N Lytvyn, M Starynskyi, E Karpushova… - J. Legal Ethical & Regul …, 2021 - HeinOnline. Settlement of administrative disputes with the participation of a judge: Foreign experience and implementation in

[14] Cited by **17**