



SOUTH AFRICA

Electoral Commission

Auction 0010505508

**Network
And
Information Security Audit
(Assessment and Penetration Testing)**

IMPORTANT NOTICE

Failure to comply with the completion of the auction conditions and the required information or submission of the required stipulated documents indicated in the bid specification document will result in disqualification.

1. Purpose

The Electoral Commission requires the services of professional information and network security specialists to audit and assess its ICT network and infrastructure in order to obtain an independent assessment of its network security strength and weakness, including vulnerabilities to potential malicious activities of hostile cyber-attacks and report on the operational soundness and integrity of the ICT environment.

Also required is to identify compliance with ICT security standards and identify existing and/or potential security and access control vulnerabilities throughout the network. Included will be internal and external penetration testing, access control and security review around the local and wide area network, work station and data-centre infrastructure and web and mobile applications.

In summary the Electoral Commission seeks to appoint a suitably qualified and experienced service provider to conduct an audit and assessment of its ICT network and infrastructure. The final deliverable being an independent security audit report which will serve two purposes, as follows:

- a) Executive report for senior management and stakeholder assurance.
- b) Security advisory report – Detailed technical findings and recommendations for technical and operational management.

Bidders must place a bid on the Votaquotes (e-Procurement) system and then provide all the required documentation before the due dates as specified in this document and on the Votaquotes web site.

2. Background Information

The Electoral Commission (IEC) is a permanent body created by the Constitution to promote and safeguard representative democracy in South Africa. Although accountable to Parliament, the Electoral Commission is independent of the government of the day. Its immediate task is the impartial management of free and fair elections at all levels of government.

The Electoral Commission has invested extensively in ICT technologies, which provide a platform to effectively support and enable its business processes, in an effort to meet its goal of delivering free and fair elections in an open and transparent environment. The Electoral Commission's ICT Department intends to continue running a highly efficient, stable and secure ICT infrastructure, making full use of industry standards such as NIST, ISO 27000 etc., best practices and disciplines based upon stable and reliable technologies.

The Electoral Commission has adopted a net-centric architecture that operates on a wide area network connecting more than 300 offices at various locations around the country and around 2000 users, using a combination of platforms including the Multi-Protocol Label Switching (MPLS). In addition, the IEC has an extensive online presence with various websites and web portals including mobile applications, which provide real-time and online data processing capabilities in various forms. The IEC has also recently rolled out in excess of 40,000 Voting Management devices (VMDs) that connect to the IEC via the Access Point Name

(APN) which provide real-time and online data processing capabilities from anywhere where there is connectivity throughout the country. These devices are managed by a Mobile Device Management (MDM) solution that is hosted in the Cloud.

3. Current Environment

3.1. Operating Software Environment

The Electoral Commission has chosen Microsoft Windows Software as its primary operating software platform, and has adopted a client /server web based architecture.

3.2. Organizational Landscape

Below is the landscape of the organisation, its network topology and remote sites include:

- 3.2.1. National Office: Houses the Electoral Commission's national data-center and all major ICT equipment consisting of more than 100 physical servers, 243 virtual servers, routers, network switches, firewalls and approximately 300 desktop machines
- 3.2.2. Disaster Recovery Site: An alternative site hosting and connecting a disaster recovery capability for several key critical systems. It hosts a scaled down version of the national data-center and it is used as a fail-over facility in case of a disaster.
- 3.2.3. Provincial Offices – Nine (9) offices country wide, one per province, each provincial office. Each provincial office connects an average of 40 workstations and 1 server via a wide area network.
- 3.2.4. Warehouses: Eleven (11) warehouses country wide, one per province with an additional National warehouse and a second Gauteng Province Warehouse. Each warehouse connects between 2 - 30 workstations and some have a server via a wide area network. Occasionally the number of warehouses increases based on short-term operational business requirements.
- 3.2.5. Municipal offices – Approximately 300 offices countrywide, located in each municipality in the country, each municipal office connects an average of 5 computers via the wide area network. A variable number, ranging between 9 – 40 of the municipal offices are connected to head office via satellite.
- 3.2.6. Network structure: The Electoral Commission uses private network to provide connectivity to the entire wide area network (WAN). It also used an Access Point Name (APN) to connect laptops and Voting Management Devices (VMDs).

4. Technical Requirements

The technical specification for the required solution is as specified below. It must be noted that the technical specifications below are the minimum requirements; the only deviation that may be accepted will be in case where the bidder's specification is better. Anything below specification will be disqualified.

The bidder is required to provide a detailed methodology including tools and solution which will be used to deliver these required services.

4.1. Scope of Assessments

The objectives of this assessment must focus on the security vulnerability of the Electoral Commission's ICT infrastructure and application security including:

- 4.1.1. **Server security assessment** – the security levels of physical and virtual servers, including (but not limited to) system hardening, malicious software protection, administration processes, logging and auditing configurations, access control and software vulnerabilities.
- 4.1.2. **Workstation security assessment** – the security levels of user and administrator workstations, including (but not limited to) system hardening, malicious software protection, administration processes, logging and auditing configurations, access control and software vulnerabilities.
- 4.1.3. **Perimeter security assessment** – the security levels of the network design in terms of exposure and protection to external, untrusted networks such as the internet and third party networks. This also includes the network design and security levels of the Demilitarized Zone (DMZ) and other public facing systems or services.
- 4.1.4. **Network security assessment** – an assessment of the overall network design, architecture, the configuration and security levels of switches, routers, firewalls and Intrusion Prevention System (IPS) devices.
- 4.1.5. **Remote access assessment** – an assessment in terms of the remote access capabilities, including VPN and APN design, configuration, architecture, access control and encryption.
- 4.1.6. **Web application assessment** – Vulnerability assessment of all public facing websites and applications including OWASP Top 10 web security risks.
- 4.1.7. **Mobile application assessment** – Vulnerability assessment from the IEC mobile application perspective.
- 4.1.8. **VMD assessment** - Vulnerability assessment from the IEC VMD system perspective.

4.1.9. Identity and Access Management – Review and assessment of identity and access management including Multi-Factor Authentication (MFA).

4.1.10. Social Engineering Assessment – tests of the human vulnerabilities including phishing, baiting spear phishing etc.

The proposed methodology and processes should cover the above mentioned objectives, without undermining established business processes of carrying out security audits. This framework is not necessarily prescriptive but indicative of what is understood to be the scope of the project. The successful bidder will be expected to independently select a sample number of areas and sites to be tested based on his/her own professional consideration and established norms and standards.

Latest vulnerability assessment and penetration testing methodologies and techniques must be used when providing the service.

4.2. Assessment Deliverables

The bidder is required to provide a detailed methodology for the testing of all of the following security assessment requirements.

4.2.1. Perform penetration tests of all public facing IP addresses including internal IP addresses.

4.2.2. Review the Electoral Commission existing security policies. Identify, propose and advise on any changes and improvements that may be required.

4.2.3. Review the Electoral Commission network architecture and network segments. Recommend if changes in architecture are necessary to improve security.

4.2.4. Review the Electoral Commission security architecture such as firewalls and intrusion detection and prevention systems, including hardware, software, and configuration(s) as well as rule base. Recommend, if necessary, new solutions in hardware and software and/or configuration changes to improve security.

4.2.5. Perform vulnerability scans on all key applications such Email server, Database, Web Application Server, Enterprise Resource Planning (ERP) and Directory Services.

4.2.6. Perform physical security assessments on ICT Infrastructure including Server Room, Network Cabinets, IT Equipment Store Room etc.

4.2.7. Perform vulnerability scans to determine if any vulnerabilities exist, including on workstations, servers, printers, switches, routers and networked telephony devices.

- 4.2.8. Perform penetration testing of all of the Electoral Commission websites against OWASP Top 10 web security risks.
- 4.2.9. Perform vulnerability assessment of the Voting Management Devices (VMDs).
- 4.2.10. Perform vulnerability assessment of the Electoral Commission's Mobile Application.
- 4.2.11. Review the Electoral Commission logging and auditing capabilities and procedures. Provide recommendations for any changes and improvements.
- 4.2.12. Review operating system security settings and provide recommendations for improvements.
- 4.2.13. Review configurations of critical ICT infrastructure components.
- 4.2.14. Review the Electoral Commission's server implementation process, including installation, hardening and implementation.
- 4.2.15. Review the Electoral Commission software development process and provide recommendations to ensure the development process includes security in design, architecture and testing.
- 4.2.16. Review the Operations Change Management process and if necessary recommend changes to improve security.
- 4.2.17. Review the Operations Configuration Management process and if necessary recommend changes to improve security.
- 4.2.18. Assess any unexpected network access routes, such as the existence of modems and/or wireless access points that may be used to access the Electoral Commission networks through unprotected routes.
- 4.2.19. Perform switch vulnerability scans. Recommend, if necessary, changes to improve security.
- 4.2.20. Perform router vulnerability scans. Recommend, if necessary, changes to provide best security.
- 4.2.21. Review remote access architecture and perform penetration testing to determine if the configuration is secure and if necessary, provide recommendations to improve security.
- 4.2.22. Ethical hacking and testing techniques should be applied so as to avoid disrupting ongoing business operations.
- 4.2.23. Review and review identity and access management policies and processes.
- 4.2.24. It is required that the bidder should include Red, Green, Blue, Purple and White Teaming exercises as part of the engagement

4.2.25. It is required that the bidder should also include war games exercise as part of the engagement

4.2.26. It is required that the services should include Cryptography analysis as part of the engagement

4.2.27. It is recommended that the bidder includes following sample sites for assessment and testing:

4.2.27.1. National Office, DR and Hosting Environment

4.2.27.2. Three provincial offices.

4.2.27.3. Nine municipal offices.

4.2.27.4. Two warehouses.

4.2.27.5. Externally from Internet.

4.3. Project Delivery Framework

Subject to the alignment of the bidder's project plan and methodology, the following processes will be preferred:

4.3.1. Assessments and penetration testing will start externally from the external unknown and gradually move inside.

4.3.2. Should the need arise the ICT team will gradually assist in enabling access into internal inaccessible areas.

4.3.3. Identified vulnerabilities should be reported immediately, with recommended remediation processes, once addressed a re-assessment will be required to determine the effectiveness of the remediation done.

4.3.4. At the end of this engagement the Electoral Commission expects the recommended bidder to provide a report which describes the Electoral Commission's current security posture; identifying any existing weaknesses; and provide a prioritized list of short and long-term actions for improving the information security and risk posture.

4.3.5. For each assessment, the following reports are required:

4.3.5.1. High-level executive summary report

4.3.5.2. Detailed technical findings and remediation report after initial assessment

4.3.5.3. Final detailed technical findings and remediation report after re-assessment

4.3.6. A final summary report with a detailed report of findings not remediated by the end of the project.

4.3.7. The assessment reports will be treated as highly confidential and must not be shared with external parties outside the key role-players to be agreed.

4.3.8. The high-level executive summary report is intended for executive management assurance and will be shared with key stakeholders such as political parties and government security services.

4.4. Re-assessment

After the initial assessment has been performed and all reports have been submitted, the Electoral Commission shall implement remediation processes. The bidder will be required to perform a reassessment of all identified vulnerabilities and recommendations after the remediation exercise has been completed.

4.5. Project Plan and Timelines

The bidder is required to submit a suggested project plan for these services as part of the submission. The project plan must detail timelines and resource requirements. The project plan must provide for at most ten (10) weeks from start to end.

The project is intended to be delivered over the period mentioned above as soon as the official Purchase Order is issued in time before National and Provincial Elections (NPE) 2024.

4.6. Capacity and Track Record

This project will require the bidder to have the following competencies:

4.6.1. The bidder must be able to demonstrate expertise in the information security field. The bidder must have at least 5 years' experience providing IT Security Audits. Bidder must include a company profile showing years of experience.

4.6.2. The bidder must provide reference letters from at least three (3) contactable references of past services of a similar nature that the bidder provided or was involved in to demonstrate experience. Reference details must include the following: customer name, contact person, contact details (telephone, email, physical address) and service description and value of services offered. Some guideline definitions:

4.6.2.1. Service value defined in terms of budget.

4.6.2.2. Similar services are those services, which includes supply of similar services (Information Security Audit / Vulnerability Assessments) as per the technical requirements and of comparative value

4.6.2.3. Please refer Appendix C: Guideline Reference for guideline

4.6.3. The bidder must submit the names and curriculum vitae (CVs) of key project team members demonstrating their skills and experiences for this project in Appendix B. The list should include at least two (2) IT Security resources with at least the following qualifications must be included: Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) and Certified Information Systems Security Professional (CISSP).

4.6.4. Bidders to also provide an organogram showing the team structure and how the team fits together to deliver on the IEC's requirement.

4.6.5. The bidder should demonstrate an understanding of the relationship between business needs and information security requirements

4.6.6. The successful bidder and their project team members may be subjected to security clearance assessment by the relevant state security institution. It must be noted that non-South African citizens are unlikely to receive security clearance and are therefore not recommended.

4.6.7. The successful bidder will be required to sign a Non-Disclosure Agreement (NDA) with the Electoral Commission.

5. Planning Assumptions

5.1. The Electoral Commission will provide technical resources for all the Electoral Commission's designated work including setup and configuration of own systems and databases.

5.2. Wherever the need arises the successful bidder shall do initial equipment configuration of environmental specific requirements.

5.3. The delivery of the service required must be completed within the days as stipulated in the delivery and

implementation schedule stipulated in section 12.

- 5.4. The bidder's change control management process must be flexible enough to facilitate speedy deployment and resolution of problems without compromising management controls and security.

6. General Auction Conditions

The following standard bid conditions must be adhered to and complied with; failing which the bid proposal will be disqualified.

- 6.1. All bids must be placed online on the Votaquotes website <https://votaquotes.elections.org.za>.
- 6.2. Bidders must complete and submit Appendix A - Technical Bid Response Sheet to demonstrate compliance with the required technical specification.
- 6.3. Bidders must complete and submit Appendix D – List of Tools to be used on the project including the versions of the tools to be used.

7. Data Protection and Confidentiality of Information

Due to the sensitive nature of the information and data which will become available to the successful bidder, it will be required that the successful bidder sign a Service Level Agreement which will, *inter alia*, incorporate a clause addressing the protection of same in line with paragraphs 7.1 and 7.2 below (read together with paragraph 15 of the Technical Bid Response Sheet).

7.1. Data Protection

- 7.1.1. During the course of executing on this contract, the successful bidder will have access to the data collected or provided and stored by the Electoral Commission on the service provider's disk storage units and data backup facilities. The successful bidder shall have the responsibility for protecting information resources against accidental or intentional damage or loss of data, interruption, or the compromise of this information into the hands of third parties. The successful bidder or its members of staff, whether employed or contracted shall also not process the data without a prior written agreement with the Electoral Commission or without written instructions from the Electoral Commission beyond what is necessary to fulfil its obligations towards the Electoral Commission.
- 7.1.2. The successful bidder shall keep confidential all the Electoral Commission's information that they have in their possession. The successful bidder shall ensure that each member of their staff, whether employed or contracted, having access to or being involved with the processing of the Electoral Commission's data undertakes a duty of confidentiality and is informed of and complies

with the data privacy obligations of this bid.

7.1.3. The successful bidder shall also ensure that the Electoral Commission's data in its possession is returned to the Electoral Commission and/or deleted from its computer systems as per instruction by the Electoral Commission at the end of the contract period.

7.2. Confidentiality of Information

7.2.1. "Confidential Information" means irrespective of its format, confidential trade, commercial, financial and management information and data, or other proprietary information which is either designated as confidential or by its nature is confidential howsoever such confidential information may be disclosed or made available to the Recipient including, without limiting the afore-going, whether direct or indirect, orally, visually or in electronic format or by reason of inspection of documentation or other matter on or at the Discloser's premises or elsewhere including, but not limited to:

7.2.2. The successful bidder shall irrevocably undertake and agree:

7.2.2.1. to protect all confidential information that they may get access to in course of executing the resulting contract. Without limiting the generality of confidential information, Confidential Information shall include any information that falls within the definition of 'Personal Information' as defined in the Protection of Personal Information Act 4 of 2013, as amended or substituted and/or

7.2.2.2. not to divulge or disclose to any third party in any form or manner whatsoever, either directly or indirectly, any confidential information of the Discloser without the Consent of the Discloser;

7.2.2.3. not to, directly or indirectly, detract from, expand on, amend, decompile, reverse engineer, use, exploit, permit the use of, or in any other manner whatsoever apply the confidential information for its own benefit or the benefit of any other person or for any purpose whatsoever other than for the Engagement and otherwise than in accordance with the provisions of this Agreement;

7.2.2.4. to treat all Information as confidential information where it is uncertain of the nature of the Information until written notice to the contrary is received from the Electoral Commission;

7.2.2.5. to take reasonable security (including IT security) measures in line with its own security measures to keep the confidential information confidential;

- 7.2.2.6. to immediately notify the Electoral Commission upon discovery of any unauthorised use or disclosure of the confidential information or any other breach of this clause;
- 7.2.2.7. to take all necessary steps or assist the Electoral Commission to regain possession of the confidential information or to prevent its further unauthorised use;
- 7.2.2.8. to immediately at the Electoral Commission's reasonable request or in any event at the completion of an Engagement to forthwith return all originals, copies, reproductions, summaries or extracts of the confidential information, or at the Electoral Commission's option destroy these and certify that it has done so; and
- 7.2.2.9. that all confidential information is and shall remain the property of the Electoral Commission and that disclosure thereof does not grant the Receiver any express or implied license to use such Confidential Information or right other than as provided for in this Agreement.

7.2.3. Notwithstanding the above, the successful bidder shall be entitled:

- 7.2.3.1. in compliance with the applicable laws and its professional obligations, to retain copies of all Information of the Electoral Commission which is relevant to or forms part of the Services;
- 7.2.3.2. to share the confidential information with its Personnel and any of the Service Provider's parties to the extent required to render the Services; and
- 7.2.3.3. to share the confidential information with its Professional Advisors or insurers in the event of a claim arising from or in connection with this Agreement, provided that the provisions of this clause shall still apply to such copies.

7.3. This clause shall not apply to:

- 7.3.1. information in the public domain otherwise than by breach of this Agreement;
- 7.3.2. information that was not obtained under any obligation of confidentiality; and
- 7.3.3. information obtained from a third party who the receiving Party believes, after reasonable inquiry, is free to divulge the information so long as such information was not obtained by the receiving Party under any obligation of confidentiality to the third party.

8. Quality Control

- 8.1. The bidder takes responsibility for the completeness and quality of their bid submission.
- 8.2. The IEC may also call on bidders to make presentations in order for the Electoral Commission to ensure full compliance with all its requirements and as part of the bid evaluation process prior to the conclusion of the adjudication of the bid. Any such request for presentations shall only be for clarification purposes in support of mandatory requirements that must be adhered to as part of the written submission requirements of this bid. Failure to submit mandatory requirements shall not be rectified by the call for presentations.
- 8.3. Any restrictions or conditions associated with any elements of the service offering/s must be detailed. The Electoral Commission reserves the right to reject conditions which are considered unfavourable to its business or unacceptable.
- 8.4. The submission of a bid implies acceptance of the terms specified in the provisions laid down in the specifications, the procurement and, where applicable, additional documents.
- 8.5. Bidders are expected to examine carefully and respect all instructions and standard formats contained in these specifications.
- 8.6. A bid that does not contain all the required information and documentation will be disqualified.
- 8.7. Although the Electoral Commission will only deal with the principal service provider, if a bidder plans to sub-contract any of the services in this bid, they are required to attach copies of sub-contracting agreements in their bid response documentation.
- 8.8. Notwithstanding any shortcomings in these specifications, service providers must ensure that the proposed solution will form a workable and complete solution.
- 8.9. The Electoral Commission will issue a formal purchase order to the successful bidder before any services can be delivered.
- 8.10. The bidder's personnel working may be subjected to security clearance.
- 8.11. The bidder will be required to enter into a Non-Disclosure Agreement (NDA) with the Electoral Commission.
- 8.12. The Electoral Commission reserves the right and discretion to amend the quantities or cancel or not award this bid based on any reason including operational or financial requirements.
- 8.13. The supplier must undertake and warrant that all goods and services shall at the time of delivery

comply with the bid specifications.

9. Supplier Performance

- 9.1. Contracting of any service provider to render goods and/or services to the Electoral Commission are subject to the fulfilment of the Electoral Commission's due diligence audit requirements.
- 9.2. An essential component of the Electoral Commission's due diligence audit requirements may involve site visits to potential suppliers/contractors as well as inspection of various key documents underpinning the establishment of the companies involved in bids of the Electoral Commission. This also includes confirmation of capability and capacity requirements to execute the services specified in such bids.
- 9.3. Upon notification of the Electoral Commission's intention to award a contract, the successful bidder may be required to enter into a service level agreement (SLA/contract) with the Electoral Commission.
- 9.4. The purpose of the SLA (if applicable other than what the Electoral Commission's standard purchase orders provide for) is to fix performance criteria within the key requirements of this request for quotation, namely quantity, quality and delivery.
- 9.5. The SLA may contain elements such as supplier progress milestones, delivery schedules, quality checkpoints and invoicing procedures.
- 9.6. The Electoral Commission reserves the right to reject any services delivered not conforming to the bid specification.
- 9.7. Where previously-agreed delivery schedules are not met by a supplier, the Electoral Commission shall have the right to appoint an alternative supplier to make good the shortfall in supply. Any additional costs incurred by the Electoral Commission in obtaining such corrective services or products from another source will be for the account of the defaulting supplier.
- 9.8. During the course of executing on this contract, the successful bidder will have access to the data collected or provided and stored by the Electoral Commission on the service provider's disk storage units and data backup facilities. The successful bidder shall have the responsibility for protecting information resources against accidental or intentional damage or loss of data, interruption, or the compromise of this information into the hands of third parties. The successful bidder or its members of staff, whether employed or contracted shall also not process the data without a prior written agreement with the Electoral Commission or without written instructions from the Electoral Commission beyond what is necessary to fulfil its obligations towards the Electoral Commission.
- 9.9. The successful bidder shall keep confidential all the Electoral Commission's information that they have in their possession. The successful bidder shall ensure that each member of the staff, whether employed or contracted, having access to or being involved with the processing of the Electoral Commission's data undertakes a duty of confidentiality and is informed of and complies with the data

privacy obligations of this bid.

- 9.10. The successful bidder shall also ensure that the Electoral Commission's data in its possession is returned to the Electoral Commission and/or deleted from its computer systems as per instruction by the Electoral Commission at the end of the contract period.

10. Pricing requirements

- 10.1. Total bid price must be submitted online on the Votaquotes portal. The bid price must be inclusive of VAT.
- 10.2. The Electoral Commission will pay for the services at the end of the project. The service is costed as a fixed cost service.
- 10.3. Bidders must complete and submit Appendix B: Pricing Schedule. This will be primary price consideration for the bid evaluation
- 10.4. The bidder must submit a price schedule or quotation for the service proposed. Details of all the components on the service that include the product code where applicable and the description must be included in the price schedule / quotation.
- 10.5. Bid prices must be firm for a period of one hundred and eighty (180) days and must be inclusive of VAT. Once awarded the price will be firm for the duration of the project / contract.
- 10.6. When pricing bid proposals, bidders are advised to take into account that all items required for this service over the execution period as per project plan and as outlined in the technical specifications. A detailed breakdown must be provided to make it possible to adjust services and costs should the need arise. Where possible the breakdown must include the following costs:
- 10.6.1. Initial Assessments
 - 10.6.2. Preparation of reports
 - 10.6.3. Re-Assessments after remediation by the Electoral Commission.
 - 10.6.4. Preparation of Final Reports.
 - 10.6.5. Project Governance Meetings
 - 10.6.6. Project Meetings
 - 10.6.7. Any software licensing costs
- 10.7. Travel between the bidder's offices/ the homes of the deployed resources and the Electoral

Commission's national office in Centurion is not covered and must not be charged.

- 10.8. The bid price must be all inclusive for the proposed services, there should be no dependency on additional costs, additional optional items applicable can be listed and submitted but should not be such that the service cannot be delivered without the optional items.
- 10.9. The Electoral Commission reserves the right to adjust costs by excluding some cost factors.
- 10.10. All costs associated with the solution must be captured on the pricing schedule - no additional costs will be entertained.
- 10.11. Travel and accommodation as may be required by project team members will be arranged by the Electoral Commission in accordance with National Treasury guidelines.

11. Adjudication and Award of Contract

Bidders are advised to refer to the Bid Evaluation Criteria to ensure that they have addressed all critical bid requirements.

- 11.1. The bid will be awarded to a bidder whose solution successfully conforms to specifications and is able to deliver and support the product, and in terms of the provisions of the Preferential Procurement Policy Framework Act, 2022
- 11.2. The Electoral Commission will issue an official purchase order before any services can be delivered.
- 11.3. It should be noted that the Electoral Commission seeks to gain the best solution technically and financially and will select from the results of the bid a solution it deems to give the best investment.
- 11.4. Awarding the bid to a successful bidder is subject to the bidder entering into a service level agreement (SLA) with the Electoral Commission that will formalize and regulate the final deliverables and associated processes and procedures.

12. Delivery and Implementation Timeframe

The successful bidder will be required to complete delivery within ten (10) weeks from receipt of an official purchase order including at least 80 hours of re-assessments.

13. Technical Enquiries

Enquiries pertaining to the specifications can be directed to Bridget Ndlovu at telephone number 012 622 5700 or email ndlovub@elections.org.za or to Libisi Maphanga at email maphangal@elections.org.za.

14. Briefing Session

A virtual briefing session will be held on a date and time to be published on eProcurement.

Although the briefing session is voluntary/optional and not mandatory, bidders are encouraged to attend so as to get the opportunity to ask questions of clarification and get a better understanding of the bid requirements.

15. Written Submissions

All submissions must be received before the closing date and time for submissions as stipulated on the Votaquotes website <https://votaquotes.elections.org.za>

Submissions received after the final date and time will lead to bids being disqualified and not considered.

All bids must be placed online on the Votaquotes website <https://votaquotes.elections.org.za>. Supporting documentation can be submitted in any or both of the following options:

- Upload to the auction site.
- Place in the Electoral Commission tender box situated in the foyer of the Electoral Commission National Office in Centurion at the following address before the closing date and time of this auction

Election House

Riverside Office Park,
1303 Heuwel Avenue,
Centurion,
0157

Note: Clearly mark your submission: For the attention of Procurement and Asset Management Department – Auction 0010505509

Fax or emailed submissions will not be accepted.

Failure to submit all of the required documentation before the closing date and time shall invalidate the bid. It remains the responsibility of the bidder to confirm receipt of the required documentation with the Electoral Commission Procurement and Asset Management Department.

15.1. Summary list of submission requirements:

The following must be submitted together with the bid:

15.1.1. **Cover Letter** – A cover letter including the bidders primary and secondary contact persons and

contact information.

15.1.2. **Bid Document Returnables:** Bidder must complete and submit Appendix A, B and C

15.1.3. **Bid Proposal** – A comprehensive and detailed bid proposal addressing the key requirements for this bid specification and detailing how the bidder intends delivering on this project.

15.1.4. **Methodology and Procedures** – Provide information on the methodologies and procedures that will be used to perform all the reviews detailed in section 4, including testing from the lowest SQL layer to the highest functional layer.

15.1.5. **Capacity**, Track Record and References – Bidders must include evidence of successfully implementing at least three (3) similar projects. Provide a skills and experience matrix with references to South African clients where similar audits were conducted. The bidder must also include a profile showing years of experience of the bidder.

15.1.6. **Project Team Structure** – The proposal must include the proposed team structure of project resources that will be working on this particular engagement, with their experience and qualification in information security and audits. The team should include at least two (2) IT Security resources with at least the following qualifications: Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) and Certified Information Systems Security Professional (CISSP). It must be noted that non-South Africans may not be part of the project team, as they are unlikely to get security clearance.

15.1.7. **Project Plan** – The bidder must include a project plan together with the bid. The project timeframe must include timelines for the entire scope of the project. It must be noted that the project plan must not exceed two months in elapsed time from start to finish.

15.1.8. **Pricing Schedules** – The total cost along with a detailed breakdown schedule is required

15.1.9. **Tools and Solution** – The bidder must provide a list of all tools and solution which they intend using in the project, including the purpose there-off.

16. Closing Date

The closing dates and times of this auction are specified on the Votaquotes website. The closing dates and times are determined by the clock on the Electoral Commission's servers and is not negotiable. Bidders must also take note that supporting documentation must be delivered as specified on the auction.

17. Appendix A: Technical Bid Response Sheet

Appendix A: Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.					
	Area	Description	Bidder must indicate whichever is applicable		Bidder's response/technical specification for proposed solution – if providing more than minimum requirement
			Yes	No	
1.	Approach	The bidder is required to provide a detailed methodology including tools and solution which will be used to deliver these required services			
2.	Assessments	The bidder to perform server security assessment – the security levels of physical and virtual servers, including (but not limited to) system hardening, malicious software protection, administration processes, logging and auditing configurations, access control and software vulnerabilities			
3.		The bidder to perform workstation security assessment – the security levels of user and administrator workstations, including (but not limited to) system hardening, malicious software protection, administration processes, logging and auditing configurations, access control and software vulnerabilities.			
4.		The bidder to perform perimeter security assessment – the security levels of the network design in terms of exposure and protection to external, untrusted networks such as the internet and third party networks. This also includes the network design and security levels of the Demilitarized Zone (DMZ) and other public facing systems or services.			

Appendix A: Technical Bid Response Sheet

Completion of this technical response sheet by the bidder is compulsory.

Bidder must respond to each and every item in the response sheet.

Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.

	Area	Description	Bidder must indicate whichever is applicable		Bidder's response/technical specification for proposed solution – if providing more than minimum requirement
			Yes	No	
5.		The bidder to perform network security assessment – an assessment of the overall network design, architecture, the configuration and security levels of switches, routers, firewalls and Intrusion Prevention System (IPS) devices.			
6.		The bidder to perform remote access assessment – an assessment in terms of the remote access capabilities, including VPN and APN design, configuration, architecture, access control and encryption.			
7.		The bidder to perform web application assessment – Vulnerability assessment of all public facing websites and applications including OWASP Top 10 web security risks.			
8.		The bidder to perform Mobile application assessment – Vulnerability assessment from the IEC mobile application perspective.			
9.		The bidder to perform VMD assessment - Vulnerability assessment from the IEC VMD system perspective.			
10.		The bidder to perform Identity and Access Management review – Review and assessment of identity and access management including Multi-Factor Authentication (MFA).			
11.		The bidder to perform Social Engineering Assessments – tests of the human vulnerabilities including phishing, baiting spear phishing etc.			

Appendix A: Technical Bid Response Sheet

Completion of this technical response sheet by the bidder is compulsory.

Bidder must respond to each and every item in the response sheet.

Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.

	Area	Description	Bidder must indicate whichever is applicable		Bidder's response/technical specification for proposed solution – if providing more than minimum requirement
			Yes	No	
12.	Reviews	The bidder to review Electoral Commission's network architecture and network segments and recommend if changes are necessary to improve security posture			
13.		The bidder to review security architecture including firewall rules base and recommend if changes are necessary to improve security posture			
14.		The bidder to review Electoral Commission's existing security policies. Identify, propose and advise on any changes and improvements that may be required.			
15.	Data Confidentiality and Privacy Requirements	The bidder undertakes to agree and comply will the Electoral Commission's requirements on data protection and confidentiality of information, as stated in paragraph 6 of this bid specification			

18. Appendix B: Pricing Schedule

Appendix B –Bid Price Schedule Completion and submission of this pricing schedule is compulsory. Bidder must indicate the durations of each Failure to complete and submit shall lead to disqualification. The total must not exceed 8 weeks			
	Description of Services	Duration	Total Cost including VAT
A	Primary Review (Assessments) and preparation of initial reports		R.....
B	Post Audit Remediation Re-assessment		R.....
C	Reports Compilation and Acceptance		R.....
	TOTAL BID PRICE [A+B+C]:		R.....

* The Total Bid Price is the bid price that must be captured on eProcurement and will be used for the adjudication purposes. The project may be completed within a shorter period than anticipated.

19. Appendix C: Project Team Structure and Qualifications

<u>Appendix C – Project Team Structure</u>			
Completion and Submission of the project team structure and associated personnel qualifications is compulsory. Failure to submit shall lead to disqualification.			
	Name of Personnel	Role (Position)	Qualifications
1			
2			
3			
4			
5			
6			

20. APPENDIX D: GUIDELINE REFERENCE TABLE

Reference #1

<u>Appendix D – Guideline Reference Table</u>		
THE REFERENCE MUST CONTAIN THE FOLLOWING DETAILS		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Description of the service	
	Number of users (estimate) – size of the client	
Services Provided	Estimate Contract Value	
	When was the service provided?	

Reference #2

<u>Appendix D – Guideline Reference Table</u>		
THE REFERENCE MUST CONTAIN THE FOLLOWING DETAILS		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Description of the service	
	Number of users (estimate) – size of the client	
Services Provided	Estimate Contract Value	
	When was the service provided?	

Reference #3

<u>Appendix D – Guideline Reference Table</u>		
THE REFERENCE MUST CONTAIN THE FOLLOWING DETAILS		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Description of the service	
	Number of users (estimate) – size of the client	
Services Provided	Estimate Contract Value	
	When was the service provided?	

21. Appendix E: List of Tools

List of Tools to be used by Bidder Completion and Submission of the project team structure and associated personnel qualifications is compulsory. Failure to submit shall lead to disqualification.		
Tool Name	Description	Version

22. Appendix F: Evaluation Criteria

Bidders are advised to refer to Appendix F to ensure that they have addressed all critical bid requirements which will be used for assess the bids. Bidders are NOT expected to complete and submit this section.

22.1. Stage 1: Assessment of Bidder's Disclosure

All bids received will be evaluated and assessed in respect of the mandatory information provided in the Bidder's Disclosure (SBD4) as well as the register for restricted suppliers and tender defaulters.

Any potential issues that may arise or transgressions that may identified will be pursued in accordance with statutory obligations and requirements.

In this regard, the following must be noted:

- 1.1.1 The Electoral Commission must, as part of its supply chain management (SCM) processes, identify and manage all potential conflicts of interest and other disclosures made by a person participating in procurement process to enable the accounting officer or delegated authority to make informed decisions about the person participating in the SCM process.
- 1.1.2 As such, the Bidders Disclosure form, issued as Standard Bidding Document (SBD) 4, is attached herewith for all entities who participate in the bid process.
- 1.1.3 As part of the evaluation of the procurement process, the information provided by a person on the SBD4 form must be evaluated.
- 1.1.4 In so doing, it must be noted that if the bid evaluation establishes that:
 - (a) a person within the bidding entity is an employee of the State, the Electoral Commission's CEO must request the relevant accounting officer/accounting authority whether the person-
 - (i) Is prohibited from conducting business with the State in terms of Section 8 of the Public Administration Management Act, 2014; or
 - (ii) has permission to perform other remunerative work outside of their employment, where the PAMA does not apply to such employee;
 - (b) the conduct of a person constitutes a transgression of the Prevention and Combating of Corrupt Activities Act, 2004;
 - (c) the conduct of a person constitutes a transgression of the Competition Act, 1998, the conduct must be reported to the Competition Commission; and
 - (d) the conduct of a person must be dealt with in terms of the prescripts applicable to the Electoral Commission.

- 1.1.5 If it is established that a person has committed a transgression in terms of the above, or any other transgression of SCM prescripts, the bid may be rejected and the person may be restricted.
- 1.1.6 The Electoral Commission's CEO must inform National Treasury of any action taken against a person within 30 days of implementing the action.
- 1.1.7 During the bid evaluation process, the Electoral Commission must in addition to other due diligence measures, establish if a person is not listed in-
- (a) the Register of Tender Defaulters; and
 - (b) the list of restricted suppliers.
- 1.1.8 A bid related to a restricted bidder or tender defaulter shall be rejected.
- 1.1.9 The under-mentioned assessment criteria will be used to evaluate the elements relating to SBD4, CSD registration, tax compliance, restricted suppliers and tender defaulters:

	Assessment Criteria	Bidder Requirement (YES/NO)	Comments
1.	Bidder is registered on the National Treasury Central Supplier Database (CSD). *		
2.	Bidder is tax compliant. **		
3.	The bidder is not an employee of the state.		
4.	Having certified the SBD4, it is accepted that the bidder's conduct does not constitute a transgression of the Prevention and Combating of Corrupt Activities Act.		
5.	Having certified to the SBD4, it is accepted that the bidder's conduct does not constitute a transgression of the Competition Act.		
6.	The bidder is not a tender defaulter as per the register published on the National Treasury website.		
7.	The bidder is not a restricted supplier as per the register published on the National Treasury website.		

* No bid shall be accepted if a supplier is not registered on the National Treasury Central Supplier Database (CSD).

** A bidder must be tax compliant before a contract is awarded. A bid will be disqualified if the bidder's tax affairs remains non-compliant as per the provisions of National Treasury Instruction No 09 of 2017/2018 Tax Compliance Status Verification.

22.2. Stage 2: Key Qualifying Criteria

Stage 2 – Mandatory Qualifying Criteria				
Failure to comply with any of the requirements below will result in the bid being disqualified				
No.	Description	Yes	No	Comments
1.	Did the bidder place their bid online as per section 6.1?			
2.	Did the bidder complete and submit technical specification as per section 6.2?			
3.	Did the bidder submit three (3) contactable references as per section 4.6.2?			
4.	Did the bidder submit a project plan as per section 4.5			
5.	Did bidder submit at least two (2) CVs of key project team members as per section 4.6.3			
6.	Did bidder submit an Assessment Methodology or Approach as per section 4			
Overall Stage 2 Outcomes:		<u>Assessment Comments:</u>		
		Bid qualifies for further consideration: (YES/NO):		

22.3. Stage 3: Technical Bid Evaluation

Stage 3: Technical Bid Evaluation Failure to comply with any of the below shall lead to disqualification..					
	Area	Description	Bidder must indicate whichever is applicable		Bidder's response/technical specification for proposed solution – if providing more than minimum requirement
			Yes	No	
1.	Approach	The bidder is required to provide a detailed methodology including tools and solution which will be used to deliver these required services			
2.	Assessments	The bidder to perform server security assessment – the security levels of physical and virtual servers, including (but not limited to) system hardening, malicious software protection, administration processes, logging and auditing configurations, access control and software vulnerabilities			
3.		The bidder to perform workstation security assessment – the security levels of user and administrator workstations, including (but not limited to) system hardening, malicious software protection, administration processes, logging and auditing configurations, access control and software vulnerabilities.			
4.		The bidder to perform perimeter security assessment – the security levels of the network design in terms of exposure and protection to external, untrusted networks such as the internet and third party networks. This also includes the network design and security levels of the Demilitarized Zone (DMZ) and other public facing systems or services.			

Stage 3: Technical Bid Evaluation Failure to comply with any of the below shall lead to disqualification..					
	Area	Description	Bidder must indicate whichever is applicable		Bidder's response/technical specification for proposed solution – if providing more than minimum requirement
			Yes	No	
5.		The bidder to perform network security assessment – an assessment of the overall network design, architecture, the configuration and security levels of switches, routers, firewalls and Intrusion Prevention System (IPS) devices.			
6.		The bidder to perform remote access assessment – an assessment in terms of the remote access capabilities, including VPN and APN design, configuration, architecture, access control and encryption.			
7.		The bidder to perform web application assessment – Vulnerability assessment of all public facing websites and applications including OWASP Top 10 web security risks.			
8.		The bidder to perform Mobile application assessment – Vulnerability assessment from the IEC mobile application perspective.			
9.		The bidder to perform VMD assessment - Vulnerability assessment from the IEC VMD system perspective.			
10.		The bidder to perform Identity and Access Management review – Review and assessment of identity and access management including Multi-Factor Authentication (MFA).			
11.		The bidder to perform Social Engineering Assessments – tests of the human vulnerabilities including phishing, baiting spear phishing etc.			
12.	Reviews	The bidder to review Electoral Commission's network architecture and network segments and recommend if changes are necessary to improve security posture			

Stage 3: Technical Bid Evaluation Failure to comply with any of the below shall lead to disqualification..					
	Area	Description	Bidder must indicate whichever is applicable		Bidder's response/technical specification for proposed solution – if providing more than minimum requirement
			Yes	No	
13.		The bidder to review security architecture including firewall rules base and recommend if changes are necessary to improve security posture			
14.		The bidder to review Electoral Commission's existing security policies. Identify, propose and advise on any changes and improvements that may be required.			
15.	Data Confidentiality and Privacy Requirements	The bidder undertakes to agree and comply will the Electoral Commission's requirements on data protection and confidentiality of information, as stated in paragraph 6 of this bid specification			
Overall Stage 3 Result		<u>Assessment Comments:</u> 			
		Bid qualifies for further consideration (YES/NO):			

22.4. Stage 4: Technical Scoring

Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (45/60)					
	Product Description	Available Score	Points Allocation	Actual Score	Comments
1	Project methodology (as per paragraph 4)	10	<p>The methodology includes the following assessments</p> <ul style="list-style-type: none"> a) Network Security Assessment (WAN and LAN) b) Workstations Security Assessment c) Server Security Assessment d) Policy and Procedure Reviews e) External and Internet Access Assessment f) Network & Security Design & Architecture Assessment g) Application Security Assessment h) Software Development Security Assessment i) IEC Mobile App Security Assessment j) IEC VMD Applications Security Assessment <p>(1 point each)</p>		
2.	Capacity and track record – 2 relevant References (as per paragraph 5)	21	<p>References x 3:</p> <ul style="list-style-type: none"> a) Company name and address = 1 point b) Project value = 1 point c) Project description = 2 point d) Size of the project = 1 point 		

Stage 4 – Technical Scoring

To qualify to the next phase of adjudication a bidder must score a minimum of 75% (45/60)

	Product Description	Available Score	Points Allocation	Actual Score	Comments
			e) Contact name = 0.5 point f) Email address = 0.5 point g) Cell or telephone number = 0.5 point h) Done in the past 2 years = 0.5 points (3 References: 7 points per reference)		
3.	Team Structure and Personnel skills and experience (as per paragraph).	19	a) Profile showing experience of 5 years or more (2 points) b) Completed Appendix C with Team Resources with Qualifications (4 points) c) Provided a team structure / organogram (1 point) d) Submission of at least 2 CVs with the following qualifications: (6 points per CV) <ul style="list-style-type: none"> i. CEH qualification – 2 points ii. OSCP Qualification – 2 points iii. CISSP Qualification – 2 points (total of 12 CV points)		
4	Relevance of project plan (as per paragraph 4.5)	10	a) Plan to complete in required time frame – 3 points b) Plan includes all assessment requirements – 3 points c) Plan has timelines / milestones – 2 points d) Plan includes follow up assessment – 2 points		
TOTAL POINTS:		60			

Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (45/60)					
	Product Description	Available Score	Points Allocation	Actual Score	Comments
Overall Stage 4 Result		<u>Assessment Comments:</u>			
		Bid qualifies for further consideration (YES/NO):			

22.5. Stage 5: Adjudication of Bids

Only bids that comply with the requirements and conditions of the bid and that meet the minimum criteria in the bid evaluation process as stipulated above will be considered for bid adjudication purposes.

Acceptable bids must be market related.

This bid is deemed not to exceed R50 million including VAT.

Therefore, the 80/20 preference point system (PPPFA scoring) in terms of the Preferential Procurement Policy Framework Act, 2005 (PPPFA) and the Preferential Procurement Regulations, 2022 shall apply in the adjudication process of this auction where all acceptable bids received are equal to or below R50 million including VAT. Preference points will be allocated as follows:

B-BBEE Status Level of Contributor	Number of Points
1	20
2	18
3	14
4	12
5	8
6	6
7	4
8	2
Non-compliant contributor	0

22.6. Bid Evaluation Committee

	Name:	Signature:
1		
2		
3		
4		
5		