



SOUTH AFRICA

Auction 0010460409

Bid Specifications

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 above (i.e. non submission of the required reseller authorization details and warranty stipulations) shall invalidate a bid.

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.

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 Technical 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.

The Electoral Commission's run on the following systems:

- a) Windows Desktop Operating System
- b) Windows Server Operating System
- c) Database Servers
- d) Development Tools
- e) Database Reporting Tools

3.2 Organisational Landscape

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

- a) **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
- b) **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.
- c) **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.
- d) **Provincial Warehouses:** Ten (10) warehouses country wide, one per province with an additional warehouse at national office. 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.
- e) **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.
- f) **Network structure:** The Electoral Commission uses private network to provide connectivity to the entire wide area network (WAN).

4 Technical Specifications

4.1 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.

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

- a) **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
- b) **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
- c) **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.
- d) **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.

- e) **Remote access assessment** – an assessment in terms of the remote access capabilities, including VPN and APN design, configuration, architecture, access control and encryption.
- f) **Web application assessment – Vulnerability assessment** of all public facing websites and applications including OWASP Top 10 web security risks.
- g) **Mobile application assessment – Vulnerability assessment** from the IEC mobile application perspective.
- h) **VMD applications assessment - Vulnerability assessment** from the IEC VMD application perspective.
- i) **Identity and Access Management** – Review and assessment of identity and access management including Multi-Factor Authentication (MFA).

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.

- a) Perform penetration tests of all public facing IP addresses including internal IP addresses.

- b) Review the Electoral Commission existing security policies. Identify, propose and advise on any changes and improvements that may be required.
- c) Review the Electoral Commission network architecture and network segments. Recommend if changes in architecture are necessary to improve security.
- d) 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.
- e) Perform vulnerability scans on all key applications such Email server, Database, Web Application Server, Enterprise Resource Planning (ERP) and Directory Services.
- f) Perform physical security assessments on ICT Infrastructure including Server Room, Network Cabinets, IT Equipment Store Room etc.
- g) Perform vulnerability scans to determine if any vulnerabilities exist, including on workstations, servers, printers, switches, routers and networked telephony devices.
- h) Perform penetration testing of all of the Electoral Commission websites against OWASP Top 10 web security risks.
- i) Review the Electoral Commission logging and auditing capabilities and procedures. Provide recommendations for any changes and improvements.
- j) Review operating system security settings and provide recommendations for improvements.
- k) Review configurations of critical ICT infrastructure components.
- l) Review the Electoral Commission's server implementation process, including installation, hardening and implementation.
- m) Review the Electoral Commission software development process and provide recommendations to ensure the development process includes security in design, architecture and testing.

- n) Review the Operations Change Management process and if necessary recommend changes to improve security.
- o) Review the Operations Configuration Management process and if necessary recommend changes to improve security.
- p) 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.
- q) Perform switch vulnerability scans. Recommend, if necessary, changes to improve security.
- r) Perform router vulnerability scans. Recommend, if necessary, changes to provide best security.
- s) Review remote access architecture and perform penetration testing to determine if the configuration is secure and if necessary, provide recommendations to improve security.
- t) Ethical hacking and testing techniques should be applied so as to avoid disrupting ongoing business operations.
- u) Review and review identity and access management policies and processes.
- v) It is recommended that the bidder includes following sample size for assessment and testing outside the national office:
 - 1) Three provincial offices.
 - 2) Nine municipal offices.
 - 3) Two warehouses.
 - 4) 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:

- a) Assessments and penetration testing will start externally from the external unknown and gradually move inside.
- b) Should the need arise the ICT team will gradually assist in enabling access into internal inaccessible areas.
- c) 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.
- d) 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 prioritised list of short and long-term actions for improving the information security and risk posture.
- e) The following reports are required:
 - 1) High-level executive summary report
 - 2) Detailed technical findings and remediation report after initial assessment
 - 3) Final detailed technical findings and remediation report after re-assessment
- f) 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.
- g) 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 eight (8) weeks from start to end.

The project is intended to be delivered over the period as soon as the Purchase Order is issued in time before Local Government Elections 2021.

4.6 Capacity and Track Record

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

- a) The bidder must be able to demonstrate expertise in the information security field
- b) The bidder must provide at least two (2) 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:
 - i. Service value defined in terms of budget.
 - ii. Similar service value are those services of comparative value and not less than 50% of this bid price.
 - iii. Similar services are those services, which includes supply of similar services (campus switch) as per the technical requirements and of comparative value
- c) The bidder must submit the names and curriculum vitae (CVs) of key project team members demonstrating their skills and experiences for this project in Annexure 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).

- d) Bidders to also provide an organogram showing the team structure and how the team fits together to deliver on the IEC's requirement.
- e) The bidder should demonstrate an understanding of the relationship between business needs and information security requirements
- f) The successful bidder will be required to enter into a SLA with the Electoral Commission to provide the above mentioned.
- g) 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.

5 General Auction Conditions and Award

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

- a) Documentation must be complete, clearly marked and in accordance with the *Technical Specifications* (section 4) and *Required Responses* (section 5).
- b) Details of any sub-contractor must be included in the written proposal should a sub-contractor be used.
- c) The bidder must submit the names and curriculum vitae (CVs) of key project team members demonstrating their skills and experiences for this project in Annexure 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).
- d) The selection process may include short-listing, presentation and demonstration of the solution by the short-listed finalists.

- e) The contract will be awarded to a bidder whose services successfully conforms to specifications and is able to deliver and support the product, as well as in terms of the provisions of the Preferential Procurement Policy Framework Act, 2000.
- f) Awarding of the Auction to any successful bidder shall be subject to the Electoral Commission's due diligence audit requirements.
- g) The successful bidder shall also be required to enter into a Service Level Agreement (SLA/Contract) with the Electoral Commission in order to formalize and confirm the exact solutions to be delivered.
- h) The Electoral Commission will issue a formal purchase order to the successful bidder before commencement of any services.
- i) No payment shall be made until the project has been completed in line with the requirements.

6 Pricing Requirements

With respect to cost, bidders are advised to ensure that the following issues are factored into the price. The Electoral Commission requires the pricing to be stated as follows:

- a) Provide the total cost of the project along with a detailed breakdown covering all the reviews outlined in technical specifications. Bidders are required to submit a fixed bid amount for the delivery of the project as per the bidder's proposed project plan, included should be an 80 hour estimated work for reviewing fixes to finding from the first round.
- b) Bidder must complete the Pricing Schedule in Annexure A. This will be primary price consideration for the bid evaluation.
- c) The total cost along with a detailed breakdown per review is required (as per Annexure A). Bidders are required to provide their team of resources with hourly rates, in case additional rework and review beyond the scope of this brief is required (as per Annexure B).

- d) Travel between home and the project office at the Electoral Commission's national office in Centurion will not be charged.
- e) Provide a schedule containing the names of proposed resources with hourly rates. This is provisional to deal with additional work that may arise from review of remediation work.
- f) All prices must be inclusive of VAT (Value Added Tax).
- g) The required detailed costs schedule set out below must be completed. Indicative hours are required to enable the Electoral Commission to compare the costs of proposals on a like for like basis. The actual scope of the work may be amended in the project planning phase subject to budget availability, rates will however be fixed as per the Auction submissions.
- h) The hours allocated for reassessment will be claimed against reassessment activities up to a maximum of 80 hours.
- i) Travel and accommodation as may be required by project team members will be arranged by the Electoral Commission in accordance with National Treasury guidelines. Travel using a project team members own vehicle will be reimbursed at the prevailing rate per kilometer as applicable in the Electoral Commission on the date of travel.
- j) All travel requiring re-imbursement must be pre-approved by an authorized management representative of the Electoral Commission on the project.

7 Project Timeframe

The successful bidder will be required to adhere to the proposed project time lines as follows:

Project Timeline	Period
Project start	As soon as the PO is issued
Project end	Before LGE 2021
Final reports to be submitted	5 days after Project End day

8 Briefing Session

A virtual briefing session will be held on a date and time to be published on eProcurement. Bidders may, however, direct enquiries concerning the technical requirements to Siviwe Gwadiso at 012 622-5700 or gwadisos@elections.org.za.

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.

9 Required Bid Response

All submissions must be received before the closing date and time for submissions as stipulated on the eProcurement website <https://votaquotes.elections.org.za>. Submissions received after the date and time will lead to bids being disqualified and not considered.

All bids must be placed online on eProcurement 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 Auction 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 0010460409**

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. The following must be submitted together with the bid:

- a) **Cover Letter** – A cover letter including the bidders primary and secondary contact persons and contact information.
- b) **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.
- c) **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.
- d) **Capacity, Track Record and References** – Bidders must include evidence of successfully implementing at least two (2) similar projects. Provide a skills and experience matrix with references to South African clients where similar audits were conducted. The Electoral Commission requires reference sites and their contact details, including at least the name of company/institution, contact person(s), contact number(s), physical address, project cost, and size of the project team and a short description of the nature of the project. The Electoral Commission prefers details of open reference sites where contact does not have to be arranged via the bidder.
- e) **Project Team Structure** – The proposal must include the proposed team structure and the CVs of project resources that will be working on this particular engagement, with their experience and qualification in information security and audits as per section 6c. 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.

- f) **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.
- g) **Pricing Schedules** – The total cost along with a detailed breakdown per review is required (as per Annexure A). Bidders are required to provide their team of resources with hourly rates, in case additional rework and re-review beyond the scope of this brief is required (as per Annexure B). All prices quoted must be VAT inclusive.
- h) **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.

10 Closing Date

The closing date and time of this auction is as specified on the eProcurement (Votaquotes) website, <https://votaquotes.elections.org.za> in accordance with the bidding requirements. The closing date and time is determined by the clock on the Electoral Commission's servers and is not negotiable. Late submission will lead to bids being disqualified and not considered. All auction conditions, as stated in this bid document, must be complied with at all times. Bidders must also take note supporting documentation must be delivered before the closing date and time.

11 Annexure A – Total Bid Price Schedule

Annexure A – Total Bid Price Schedule

Completion and submission of this pricing schedule is compulsory.

Failure to complete and submit shall lead to disqualification. The total must not exceed 8 weeks

	Description of Services	Duration	Total Cost for the project Including VAT
A	Primary Review		R.....
B	Post Audit Remediation Re-assessment	80 hours	R.....
	TOTAL BID PRICE [A+B]:		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.

Declaration:

The bidder and proposed project team members agree to undergo a Security Clearance

Process: (Yes or No): _____

Name of Company (Bidder): _____

Authorised Representative's Name: _____

Signature: _____

Date: _____

12 Annexure B – Project Team Structure and Hourly Rates

<u>Annexure B – Project Team Structure and Hourly Rates</u>			
Submission of the project team structure and associated personnel hourly rates is compulsory. Failure to submit shall lead to disqualification.			
	Name of Personnel	Role (Position)	Hour Rate Including VAT
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

13 Annexure C – Bid Evaluation Criteria

Service Provider:	
Date of Bid Evaluation:	

Annexure C – Bid Evaluation Criteria			
Phase 1 – Disqualifying Factors			
No.	Description	Yes/No	Comments
1.	Submitted required bid proposal detailing service offerings (as per section 9 b)		
2.	Submitted project methodology (as per section 9 c)		
3.	Submitted contactable references (as per section 4.6 b)		
4.	Submitted Team Structure including CVs of key personnel with experience demonstrating relevant experience and relevant qualifications (as per section 5 (c))		
5.	Submitted project plan (as per section 4.5)		
7.	Submitted details of tools and/or solutions to be used.		
8	Completed and submitted Annexure A as per section 6c		
Phase 1 Results: Bidder qualifies/does not qualify for further consideration			

Annexure C – Bid Evaluation Criteria Phase 2 – Technical Scoring Criteria Failure to achieve at least 75% (41 / 54) will lead to disqualification					
No.	Item Description	Assessment Criteria	Weighted Score	Bidder Score	Comments
1.	Project methodology (as per paragraph 4)	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 (1 point each)	10		
2.	Capacity and track record – 2 relevant References (as per paragraph 5)	Total for references = Maximum 6 points for each of 2 reference: a) Company name and address = 1 point b) Project value = 1 point c) Project description = 1 point d) Contact name = 1 point e) Email address = 1 point f) Cell or telephone number = 1 point	12		

Annexure C – Bid Evaluation Criteria Phase 2 – Technical Scoring Criteria Failure to achieve at least 75% (41 / 54) will lead to disqualification					
No.	Item Description	Assessment Criteria	Weighted Score	Bidder Score	Comments
3.	Team Structure and Personnel skills and experience (as per paragraph 6 (c)).	a) Completed Annexure B with Team Resources and provision of CVs with Relevant Experience – 2 points b) Provided an organogram showing team structure – 2 points c) Provided for a Project Manager – 2 points d) Provided for a Project Sponsor / Account Manager / Escalation manager – 2 points e) Submission of at least 2 CVs with the following qualifications: i. CEH qualification – 2 points ii. OSCP Qualification – 2 points iii. CISSP Qualification – 2 points	20		
4.	Relevance of project plan (as per paragraph 4.5)	a) Plan to complete in required time frame – 2 points	12		

Annexure C – Bid Evaluation Criteria Phase 2 – Technical Scoring Criteria Failure to achieve at least 75% (41 / 54) will lead to disqualification					
No.	Item Description	Assessment Criteria	Weighted Score	Bidder Score	Comments
		b) Plan includes all assessment requirements – 2 point c) Plan has timelines / milestones – 2 point d) Plan includes follow up assessment – 2 points e) Plan has resources – 2 point f) Plan shows dependencies – 2 point			
10.	Total Score		54		
Phase 2 Results: Bidder qualifies/does not qualify for further consideration					

Phase 3 - Evaluation Based on the 80/20 Preference Point System (PPPFA Scoring)

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

Adjudication of qualifying bids will be done in accordance with the 80/20 preference point system provided for in the Preferential Procurement Regulations, 2017. Pre-scoring of bids on the eProcurement system is illustrative only in respect of the potential outcome of the Auction and serves to enhance transparency in the bidding process as well as to encourage competitive bidding and B-BBEE compliance. Qualifying bids will be scored in the final PPPFA scoring to conclude the bid evaluation process and final price and total bid points may change accordingly. The ranking of the qualifying bids in terms of the scoring will be confirmed. The order of ranking of the qualifying bids will, however, remain the same since price, B-BBEE status levels and preference points claimed will not change once the Auction has closed.

Bid Evaluation Committee

	Name	Signature
1		
2		
3		
4		
5		