ESWATINI ELECTRICITY COMPANY

TENDER: TENDER NO.76 of 2019/20

TENDER NAME: INFORMATION/CYBER SECURITY AUDIT

CLOSING DATE: 28 FEBRUARY 2020

Table of Contents

INVITATION TO BID

1. **PREAMBLE**

   The Eswatini Electricity Company (EEC) is a power utility which was formed in 1963. This is a vertically integrated parastatal company responsible for the generation, transmission and distribution of electricity throughout the Kingdom of Eswatini.
   The company, through its IT department, seeks to invite suitably qualified companies to conduct an Information/Cyber security audit at its Head quarters, Eluvatsini House. Proposals are hereby invited from reputable suppliers to provide Information/Cyber security audit services at Eswatini Electricity Company (EEC).

2. Tender documents may be obtained from http://sppra.co.sz (ESPPRA) website for a non-refundable fee of 1000 SZL/ZAR**.** The method of payment shall be cash or EFT payable to EEC offices**.**

3. Completed Tender Documents shall be delivered in a sealed envelope (Technical and Financial) marked and addressed thus:

   The Tender Committee
   Eswatini Electricity Company
   P. O. Box 258
   Mbanbane, H100

   TENDER NO 76 OF 2019/2020
   TENDER NAME: INFORMATION/CYBER SECURITY AUDIT.

   The location for submission of bids is:
   Eswatini Electricity Company

Head Office, Eluvatsini House,
Mhlambanyatsi Road,
Mbabane, Eswatini

4. SUBMISSION DEADLINE
   The Bid must be delivered at the location specified above, on or before:
   Date: 28 February
   Time: 12:00 hrs (GMT +2)

   Delivery means depositing the bid in the bid box or as otherwise instructed. Any bid received after the specified deadline for submission will not be accepted.
   Faxed, emailed or telegraphic tenders will not be accepted.

5. EEC reserves the right to accept or reject any Tender, and to annul the Tendering process and reject all Tenders at any time prior to award the Contract, without thereby incurring any liability to the affected Tenderer or Tenderers or any obligation to inform the affected Tenderer(s) of the grounds for EEC's action.

6. **LETTER OF TENDER**

   NAME OF CONTRACT: EEC INFORMATION/CYBER SECURITY AUDIT FOR MBABANE HEAD QUARTERS AND DR SITE, TENDER NO: 76 OF 2019/2020

   TO: **Eswatini Electricity Company**
   P. O. Box 258
   Mbabane, H100
   Eswatini

   We have examined the Conditions of Contract, Employer's requirements, schedules and the attached Annexure for the above named Works. We have examined, understood and checked these documents and have ascertained that they contain no

errors or defects. We accordingly offer to supply the required services in conformity with this Tender which includes all these documents and the enclosed Proposal, for the sum of

_____

We agree to abide by this Tender until _____ and it shall remain binding upon us and my be accepted at any time before that date. We acknowledge that the Appendix forms part of this Letter of Tender.

Unless and until a formal Agreement is prepared and executed this Letter of Tender, together with your written acceptance, thereof, shall constitute a binding contract between us.

We understand that you are not bound to accept the lowest or any tender you may receive.

Name: _____ Signature: _____

In the capacity of: _____ Date: _____
(Designation)

Duly authorized to sign bid for and on behalf of:

_____
(Name of Bidding Company)

7. **Declaration of Eligibility**

The Tender Committee
ESWATINI Electricity Company
P.O. Box 258
Mbabane

Dear Sir / Madam

Re: TENDER NO 76 OF 2019/2020 – INFORMATION/CYBER SECURITY AUDIT.

Dear Sirs,

Re Tender Reference_____

In accordance with the eligibility requirement of the Procurement Regulations and the tender documents we hereby declare that::

a) We, including any joint venture partners or consortium partners are a legal entity and have the legal capacity to enter into the contract;
b) We further declare that we are not insolvent, in receivership, bankrupt or being wound up, our affairs are not being administered by a court or a judicial officer, our business have not been suspended and we are not the subject of legal proceedings for any of the foregoing;
c) We declare that we have fulfilled our obligations to pay taxes and social security contributions;
d) We have not, and our directors or officers have not, been convicted of any criminal offence related to our/their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a contract within a period of five years preceding the commencement of the procurement proceedings; and
e) We do not have a conflict of interest in relation to the procurement requirement.

Name: _____ Signature: _____

In the capacity of: _____ Date: _____
(Designation)

Duly authorized to sign bid for and on behalf of:

_____
(Name of Bidding Company)

8. BID SUBMISSION FORM

The Tender Committee
ESWATINI Electricity Company
P.O. Box 258
Mbabane

Dear Sir / Madam

Re: TENDER NO 76 OF 2019/2020 – INFORMATION/CYBER SECURITY AUDIT.

Having examined the Invitation to Bid documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply the services to "CONDUCT AN INFORMATION/CYBER SECURITY AUDIT", in conformity with the said "Invitation to Bid" documents as follows:

i. In accordance with the Schedule of Prices attached herewith and made part of this Bid and which are inclusive of all taxes.

ii. We undertake, if our Bid is accepted, to deliver the good s in accordance with the delivery schedule in the Schedule of Requirements.

iii. We agree to abide by this Bid for a period of one hundred and twenty (120) days from the date fixed for Bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We understand that you are not bound to accept the lowest or any bid you may receive.

Name: _____ Signature: _____

In the capacity of: _____ Date: _____

(Designation)

Duly authorized to sign bid for and on behalf of:

_____

(Name of Bidding Company)

Company Stamp/Seal:

10. COMMITMENT FORM

I (name of tenderer in full), ...hereby agree to deliver all goods and services without altering the tendered price I quoted during tender submission date.

Name and Designation of Signatory:……..

Name of firm:……

Address: ……..

Signature of Authorized Person ……..

Date……

Company Stamp/Seal:

11. INSTRUCTION TO TENDERERS

11.1. All service providers shall include the following information and documents with their bids:

a) Trading License, Original Tax Compliance Certificate, Form J, Form C, Certificate of incorporation, SNFP Compliance certificate, Labour compliance certificate, Police clearance for Directors and Tender Purchase Receipt (or equivalent)

b) Total monetary value of similar work performed for each of the last 3 years.

c) Experience in works of a similar nature and size for each of the last x years and details of work underway or contractually committed; and clients who may be contacted for further information on those contracts.

11.2. Cost of bidding

The service provider shall bear all costs associated with the preparation and submission of his bid, and the employer will in no case be responsible or liable for those costs.

11.3. Contents of the bidding Documents

The facilities required, tendering procedures and technical requirements are prescribed in the Tender Documents. The Tender Documents include the following sections:

a) invitation for Tender
b) Instructions to Tender
c) Forms and Schedules

The Tenderer is expected to examine all instructions, forms, terms, specifications and other information in the Tender Documents. Failure to furnish all information required by the Tender Documents or submission of a Tender that is not substantially responsive to the Tender Documents in every respect will be at the Tenderer's risk and may result in disqualification of its Tender.

11.4. Clarification of bidding Documents

A prospective Tender requiring any clarification of the Tender Documents may notify the Commercial Services Manager in writing. The Commercial Services Manager will respond in writing to any request for clarification of the Tender Documents, which it receives no later than one week prior to the deadline for submission of Tenders prescribed by the Employer. Written copies of the Commercial Services Manager's response (including an explanation of the query but without identifying the source of the inquiry will be sent to all prospective Tenderers who have received the Tender Document.

11.5. Amendment of bidding Documents

At any time prior to the deadline for submission of Tenders, the Employer may, for any reason, whether at its own initiative or in response to a clarification requested

by a prospective Tenderer, modify the Tender Documents by amendment. If this modification occurs later than one week before the deadline for the submission Tenders, the Employer has the right of extending the deadline for the submission in order to give other Tenderers the necessary time for considering the modifications in the preparation of their Tenders.

The amendment will be notified in writing or by cable (hereinafter, term cable is deemed to include Electronic Data Interchange (EDI), telex or facsimile) to all prospective Tenderers, which have received the Tender Document and will be binding to them.

11.6. Documents Confidential

Tenderers shall treat the details of the Tender Document as confidential, whether they submit a Tender or not.

11.7. Documents comprising the Bid

The bid submitted by the Tenderer shall comprise the following documents:

a) Letter of Tender duly completed and signed by the Tenderer, together with the attachments below:

1. **Attachment 1:** Price Schedule
2. **Attachment 2:** Eligibility and Conformity of supplier
3. **Attachment 3:** Schedule for expected project completion
4. **Attachment 4:** A detailed project implementation plan outlining requirements from the employer as well as timelines for completion of specific milestones.
5. **Attachment 5:** A detailed proposed payment schedule required by the contractor.
6. **Attachment 6:** Detailed design of the proposed solution.

11.8. Tender Prices

The Contract shall be for the whole project, based on the bid price submitted by the bidder. All duties, taxes, and other levies payable by the service provider under the Contract, shall be included in the total bid price submitted by the bidder. The prices quoted by the bidder **shall not be subject** to adjustment during the performance of the Contract.

The bidder, if registered in Eswatini, is liable for income tax or other national or local taxes applicable in the countiry in connection with the execution of the Contract. The bidder, in not registered in Eswatini, is liable only to 15 (fifteen) percent withholding Tax in line with the Income Tax Act Directive on non-resident Contractors/Suppliers.

11.9. Bid Validity

Bids shall remain valid for a period of 90 days (ninety days) from date of tender opening. In exceptional circumstances, the Employer may request that the bidders extend the period of validity for a specified additional period. The request and the bidders' response shall be made in writing. A bidder may refuse the request without forfeiting the bid Security. A bidder agreeing to the request will not be required or permitted to otherwise modify the bid, but will be required to extend the validity of bid security for the period of the extension.

11.10. Format and Signing of Bid

The Tender shall prepare one original and two complete copies of the Tender and clearly marking each one respectively as "Original Tender", "Copy No. 1" and "Copy No. 2." In the Event of any discrepancy between them, the original shall govern.

The original and all copies of the Tender, each consisting of the documents listed above shall be typed or written in indelible ink and shall be signed by the Tenderer or person or persons duly authorised to bind the Tenderer to the Contract. All pages of the Tender except for un-amended printed literature shall be initialled by the person or persons signing the Tender.

The Tender shall contain no alterations, omissions or additions, unless such corrections are initialed by the person or persons signing the Tender.

11.11. Sealing and marking of bids

The Bidder shall Seal the Original and each Copy of the Tender in separate envelopes, duly marking the envelopes as “Original Tender”, “Copy No.1” and “Copy No.2.” The envelopes shall then be sealed in an outer envelope.

In the original and each copy of the Tender, the Technical and Financial Proposals shall be in separate envelopes, each clearly marked “TECHNICAL” and “FINANCIAL”

The inner and outer envelopes shall:

a) Be addressed to the Employer at the address given, and
b) Bear the Tender Number and the statement “DO NOT OPEN BEFORE” and the closing date for Tendering, excluding any notice allowing identification of the Bidder.
c) If the outer envelope is not sealed and marked as requested, then the Employer will assume no responsibility for the misplacement or premature opening of the bid.

11.12. Deadline for submission of bids

Bids shall be delivered to the employer at the address specified in the tender advertisement and no later than the time and date specified. The employer may extend the deadline for submission of bids by issuing an amendment, in which case all rights and obligations of the employer will then be subject to the new deadline.

11.13. Late Bids

Any bid received by the employer after the prescribed deadline will be rejected and returned unopened to the bidder.

11.14. Modification and withdrawal from Bid

The bidder may modify or withdraw its Tender after submission, provided that written notice of the modification or withdrawal is received by the Employer prior to the deadline prescribed for Tender submission.

The bidder's modifications shall be prepared, sealed, marked and dispatched as follows:

a) The bidder shall provide an original and the number of copies specified of any modifications to its Tender, clearly identified as such, in tow inner envelopes duly marked "Tender Modification – Original" and "Tender Modification – Copies". The inner envelopes shall be sealed in an outer envelope, which shall be duly marked "Tender Modifications"

A Tenderer wishing to withdraw its Tender shall notify the Employer in writing prior to the deadline prescribed for Tender submission.

The notice of withdrawal shall:

b) Be addressed to the Employer at the address specified, and
c) Bear the Tender Number and the words "Tender Withdrawal Notice." Tender withdrawal notices received after the Tender submission deadline will be ignored, and the submitted tender will be deemed to be a validly submitted tender.
d) No tender may be withdrawn in the interval between the Tender submission deadline and the expiry of the Tender validity period specified. Withdrawal of a Tender during this interval may result in the Bidder's forfeiture of its Tender Security.

11.15. Tender Opening and Evaluation

a) Envelopes marked "Withdrawal" shall be opened first and the name of the Bidder shall be read out. Tenders for which an acceptable notice of withdrawal has been submitted shall not be opened.
b) Subsequently, all envelopes marked "Modification" shall be opened and the submissions therein read out in appropriate detail.
c) No Tender shall be rejected at Tender opening except for late Tenders.

d) The Employer shall prepare minutes of the Tender opening, including the information disclosed to those present.

e) Tenders not opened and read out at the Tender opening shall not be considered further for evaluation, irrespective of the circumstances.

11.16. Clarification of Tenders

To assist in the examination, evaluation, and comparison of bids, the employer may, at the Employer's discretion, ask any Bidder for clarification ot the Bidder's bid, including breakdowns of unit rates.

The request for clarification and the response shall be in writing, or email, but no change in the price or substance of the bid shall be sought, offered, or permitted.

11.17. Preliminary Examination of Tenders

a) The Employer will examine the Tenders to determine they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the Tenders are generally in order.

b) Arithmetic errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price, which is obtained by multiplying the unit price and quantity, or between subtotals and the total price, the unit or subtotal price shall prevail, and the total price shall be corrected. If there is a discrepancy between words and figures the amount in words will prevail. If the Bidders does not accept the correction of errors, their Tender will be rejected.

c) Prior to the detailed evaluation, the Employer will determine whether each Tender is of acceptable quality, is complete and substantially responsive to the Tender Documents. For purposes of this determination, a substantially responsive Tender is one that conforms to all terms, conditions and specifications of the bidding documents without material deviations and objections, conditionalities or reservations. A material deviation, objection, conditionality or reservation is one

1. that affects in any substantial way the scope, quality or performance of the contract;

2. that limits in any substantial way, inconsistent with the Tender Documents, the Employer's rights or successful Bidder's obligations under the contract; or
3. whose rectification would unfairly affect the competitive position of other Bidders who are presenting substantially responsive.

d) If a Tender is not substantially responsive, it will be rejected by the Employer, and may not subsequently be made responsive by the Bidder by correction of the non-conformity. The Employer's determination of a Tender's responsiveness is based on the contents of the Tender itself without recourse to extrinsic evidence.

11.18. Evaluation Criteria

The evaluation will be separated into two parts. First will be the technical evaluation after which the financial evaluation will be done for those consultants that surpass the minimum accepted score for technical proposals.

The weights to be used for the evaluation are as follows:

- Technical – 70%
- Financial – 30%

Technical Evaluation

Technical	**Description**	**Maximum Points %**
Approach and Methodology	Understanding of the project and scope of work (100% filled in schedule)	30
	Detailed work plan with timeframes for the overall project	20
Maximum Points		50

Relevant Experience of Service Provider	Experience in the implementation of projects of this kind and magnitude.	30
	Quality certfication by a recognised body (ISO etc)	10
Maximum Points		40
Team Structure	Qualification, Competence and experience of key personnel	5
	Professional body affiliation (ISACA, ISSA etc)	
Maximum Points		10
Total Score for Technical Proposal		100
Minimum Acceptable Score for Technical Proposal		70

Financial Evaluation

The financial evaluation of the bids will follow the following process:

- The evaluation team will review the financial bids and determine the evaluation price for each proposal;
- The financial evaluation formula

$$Financialpoints = \frac{Lowestbid}{Tenderedbid} X30$$

Final Evaluation

- The weighted technical and financial scores shall be added together to give a total score for each proposal
- Proposal with highest score shall be recommended for award.

11.19. Contacting the Employer

a) From the time of the tender opening to the time of Contract award, if any Bidder wishes to contact the employer on any matter related to its Tender, it should do so in writing. Queries are to be forwarded to the procurement office through busisiwe.masangane@eec.co.sz

b) Any effort by a Bidder to influence the Employer's Tender evaluation, Tender comparison or Contract award decisions may result in rejection of the Bidder's Tender.

11.20. Award of Contract

1. **Intention to award**

   Following the contract award decision, EEC shall prepare a notice of intention to award which notice shall be sent directly to all Bidders who submitted tenders. **All Bidders are required to provide contact email addresses, through which they will be notified of the intention to award on the day that the Intention is sent to the Eswatini Public Procurement Authority (ESPPRA)**

2. **Employer's Right to Accept Any Tender and to reject any or All Tenders**

   The Employer reserves the right to accept or reject any Tender, and to annul the Tendering process and reject all Tenders at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for the Employer's action.

3. **Signing the Contract Agreement**

   The Employer will send the Bidder the Contract Agreement provided in the Tender Documents, incorporating all agreements between parties.

   Withing 30 (thirty) days of receipt of the Contract Agreement, the successful Bidder shall sign and date the Contract Agreement and return it to the Employer.

4. **Corrupt of Fraudulent Practices**

   Any Bidder that is found to be, or who attempts to be involved in any corrupt or fraudulent activity or practice involving any party concerned in

the Tender process, shall be disqualified. The Bidder may forfeit the Tender Security.

12 Description of Work:

EEC, through this Tender would like to identify and select an appropriate firm/vendor to perform a cyber security audit, review of her IT policies and creation of IT policies in line with an appropriate Cyber Security Framework, e.g. ISO 27000 or equivalent.

The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality for a recognized cyber security standard e.g. ISO 27000, which includes the evaluation and gap analysis of the following (and any other deemed necessary):

12.1 Current IT infrastructure of EEC

12.2 Network and devices in use

12.3 Operating systems and databases at Server level and User level

12.4 IT Policies including Operational Procedures in the current IT setup at EEC

12.5 Identification of vulnerabilities, security flaws, gaps and loopholes

12.6 Perform Internal and External Penetration test for EEC IT setup and network.

The Cyber Security Audit exercise must commence within thirty (30) business days of issuing the Work Order. The exercise shall be carried out at EEC HQ and DR site, and for all Departmental users for all types of IT systems. Report of gaps along with recommendations must be provided by the firm/vendor so as EEC can take action. After the completion of the audit and reporting exercise by the firm, EEC would take some reasonable time to study the gaps in cyber security and would therefore attempt to bridge those gaps as much as possible.

13 Eligibility Criteria

Only the firm/vendor that fulfills the following criteria are eligible to respond to the Tender. Offers received from the firm/vendor that does not fulfill any of the following is liable to rejection.

Bidders shall submit proofs of minimum eligibility as below:

No.	CRITERIA	Documentary proof to be submitted
1	The Bidder should be a company/firm with registered office and operations in South Africa (SA)/Eswatini. The bidder should be operational in SA/Eswatini for at least 5 financial years as of current date.	The Certificate of Incorporation issued by the Registrar of Companies, Eswatini (or SA equivalent)
2	The Bidder should not have been blacklisted by any State/Central Government institution or any Public sector unit. The bidder shall give an undertaking (on their letter head) that they have not been black listed by any authorities.	Undertaking by bidder (Annexure #1)
3.	The bidder should have, during the last 5 years, neither failed to perform on any agreement, as evidenced by imposition of a penalty by an arbitral or judicial authority against the Applicant or its Associate, nor been expelled from any project or agreement nor have had any agreement terminated for breach by such bidder or its associate.	Undertaking by bidder (Annexure #1)
4.	The bidder should have a minimum annual turnover of SZL/ZAR 1 million for 4 Financial years	Annexure #3 audited Balance sheet, Profit and loss accounts for the last 4 years to be submitted.
5.	The bidder should have experience and expertise in handling assignments *services related to*	Annexure #2 copies of work completion certificate for the assignments to be enclosed.

	comprehensive security review of Data centre / Enterprise network, Directory services, application security including Vulnerability Assessment and Penetration Testing.	
6.	Bidder must have carried out minimum 3 information/cyber Security audits in central/state government or banks in the past 3 years of publishing this Tender. Reference site, customer name and contact information to be provided.	Annexure #2 copies of work completion certificate for the assigments to be enclosed or Auditor's Certificate endorsing the completion of the audit in Central /state government or Banks with man-days & period.
7	The Bidder should have a minimum **2** each of (**any of**) CISA, CISSP, ISO 27000 LA/LI, CEH certification holder as permanent employees in their organization. In addition to this, Bidder should also have minimum **5** staff with any of the following qualification /certifications (or equivalent). • CISM • COBIT Certificate Holder • CCNA /CCNP • CHFI • GIAC • CRISC • SSCP • ECSA • Offensive Security Certified Professional	Annexure #4 & Annexure #5 copy of the certificates of the should be enclosed.

	• ECIH	
8.	Project Team (Minimum Composition & Eligibility) 1. Project Manager • The Project manager must have completed 5 IS Audits as Lead Auditor 2. Team member • Team members must have completed minimum 3 IS Audit	The persons deployed should have suitable auditor qualification and certifications such as CISA/ CISSO *ISO 27000 Assessor*/ISA or any other formal IT security auditor qualifications. The details are required to be submitted as per format in Annexure #6 & 7.

Note:

The Bidder is required to comply with all the above listed criteria. The listed requirements are mandatory such that non-compliance of any will result in rejection. Eligibility criteria must be observed by all Bidders in order to ensure qualification for further evaluation. Photocopies of relevant documents/certificates should be submitted as proof. EEC reserves the right to verify and/or evaluate the claims made by the bidder independently.

14 Deliverables of the Engagement – Reports and Schedule of Deliverables

14.1 Reports

Third party Audit firm will produce a report which should include the overall IT/Cyber security protection status considering people, process and technology. The Cyber security assessment report should include expert recommendations which will make EEC IT environment secure and sustainable. Report should include the following sections but not limited to:

14.1.1 Assessment report on the IT Security Policy of EEC and provide recommendations for a road map to quality standard ISO 27001, including suggestions for best practices and procedures of EEC.

14.1.2 Development of the Information Security/IT related policies as per recommended standards which should include:

- 14.1.2.1 Access control
- 14.1.2.2 Asset management
- 14.1.2.3 Change management
- 14.1.2.4 Backup and Recovery
- 14.1.2.5 IT system operations security
- 14.1.2.6 Network and Communications security
- 14.1.2.7 System acquisition, development and maintenance
- 14.1.2.8 IT Risk Management
- 14.1.2.9 Information security incident management
- 14.1.2.10 Information security aspects of business continuity management (BCM)
- 14.1.2.11 Information and information related devices disposal policy
- 14.1.2.12 Compliance and Regulatory requirements management
- 14.1.2.13 Physical and environment security

14.1.3 IT/Cyber Security Audit Report , along with recommendations, on EEC's IT environment (as per recommended guidelines, which should include but not limited to:

- 14.1.3.1 Access control
- 14.1.3.2 Network Security Management
- 14.1.3.3 Database Management Process
- 14.1.3.4 Backup & Restore Policy and Backup Plan
- 14.1.3.5 Log Management and monitoring policies for databases, applications, router, switch, firewall and operating systems
- 14.1.3.6 Incident Management and resolution process of the incidents
- 14.1.3.7 Patch update, bug fix and anti-Virus update process within EEC
- 14.1.3.8 Report on Penetration Testing and Vulnerability scan.

14.1.4 Drafting the Cyber Crisis Management Plan for EEC IT Facilities

14.1.5 Drafting a check/report template for purposes of monthly reports

14.1.6 Implement (or provide access to) phishing attack simulation

14.2 Schedule of Deliverables

Deliverable	**Tentative Duration/Periodicity**
➢ Inception report including outline of IT/Cyber security and ISO 2001 requirements, audit Plan, Reporting Formats, work plan, documentation formats, dates and location of proposed IT/Cyber audit exercise.	
➢ Weekly Status Reports showing proposed vs actual progress, delays (if any), and support required, gaps identified so fa .	Every week
➢ Summary of IT/Cyber Audit findings, including identification tests and the results of the tests must be shared with EEC officials on a weekly basis and as and when required.	Weekly / As and when required.
Prepare and submit the following: a) Draft Cyber security and IT audit report b) Cyber Crisis Management Plan (CCMP) for EEC facilities c) Expert Recommendations on the identified gaps d) Draft Information/IT Security related policies which should include: • Access control • Asset management • Change management • Backup and Recovery • IT system operations security • Network and Communications security • System acquisition, development and maintenance	

• IT Risk Management • Information security incident management • Information security aspects of business continuity management (BCM) • Information and information related devices disposal policy • Compliance and Regulatory requirements management • Physical and environment security e) Assessment Report, along with recommendations on EEC's IT environment which should include but not limited to: • Access control • Network Security Management • Database Management Process • Backup & Restore Policy and BMPackup Plan • Log Management and monitoring policies for databases, applications, router, switch, firewall and operating systems • Incident Management and resolution process of the incidents • Patch update, bug fix and anti-Virus update process within EEC • Report on Penetration Testing and Vulnerability scan.	
➢ Presentation of the IT/Cyber Security Audit Report, its findings, conclusions, and recommendations as per CERT-IN guidelines, need to be made to management of EEC. Recommendations should also be given for Quality Standard ISO 27000 as this is the prime objective of the audit output.	

➢ Submission of the final reports with required guidelines and documents.	

15 **Audit Approach and Audit Considerations**

The Independent IT/Cyber security audit will be undertaken through an evaluation of risk management by assessing total chain process of IT environment for operation integrity and operational management.

The consultant shall sign a confidentiality Agreement before starting the assignments, which will ensure the confidentiality and integrity of the content, data, applications, logics, structure, designs and other property of the Client, which should be shared, given access, and will be used by the Consultant during execution of the assignment.

The Consultant should take care of the following consideration and details at the beginning of the IT/Cyber Security Audit exercise:

a) Approach and Methodology in which the IT/Cyber Security Audit is to be done. This will include the time frame of each activity so as to organize the IT/Cyber audit activity for better control and monitoring.
b) Standards of Security and Quality that are to be followed durigh the IT/Cyber Security Audit Activity
c) Tools and Software that may be used for the IT/Cyber security audit activity. All tools and software used by the consultant need to be licensed.
d) All the IT/Cyber security reports, device logs, etc have to be shared with EEC IT representatives by the consultant. The purpose is purely to keep EEC IT informed about the perceived and possible cyber threat to EEC at present and in future.

Undertaking by Bidder **Annexure #1**

Dear Sirs,

Reference: Information /Cyber security audit at EEC

In accordance with the eligibility requirements of the Procurement Regulations and the tender documents we hereby declare that:-

a) We, including any joint venture partners or consortium partners are a legal entity and have the legal capacity to enter into the contract;
b) We declare that we have fulfilled our obligations to pay taxes and social security contributions;
c) We hereby also confirm that there is no litigation (including court, arbitration and other proceedings), inquiry or order from any regulatory authority, current or pending against us, which if adversely determined might have material adverse impact on our ability to carry on our business or pay our debts as they fall due or on our ability to enter into any of the transactions contained in or contemplated in respect of providing the services to EEC.
d) We have not, and our directors or officers have not, been convicted of any criminal offense related to our/their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a contract within a period of five years preceding the commencement of the procurement proceedings; and
e) We do not have a conflict of interest in relation to the procurement requirement.

Name and Designation of Signatory:……..

Name of firm:……

Address: ……..

Signature of Authorized Person ……..

Date…….

Information security audit Experience of Bidder **ANNEXURE #2**

(Use separate sheets for each Project and attach appropriate evidences. Ensure that the number of projects presented are with specific reference to the Evaluation Criteria of this bid Document**)**

Requirement	**Details**
Name of the Project	
Project Location	
Name of the Company	
The company address, contact name, contact number	
The company size (number of users at the time of audit services	
Project scope	
List of audit tools used	
Security standards used	
Value of the work done in (ZAR)	
Date of award / signing of contract	
Date of commencement of the work	
Date of completion	
Man-months effort	

Name and Designation of Signatory:……..

Name of firm:……

Address: ……..

Signature of Authorized Person ……..

Date…….

Profile of the Bidder **ANNEXURE #3**

General Information				
Registered Name of the company				
Address of the Registered office or Head Office				
Mailing address of the Bidder				
Company Registration number				
Phone number				
Type of entity				
Date of establishment				
Name of Chief Executive				
Name of authorized signatory				
Name of the contact person				
Total number of Employees & consultants of the proposed audit service activities.				
Commercial Information				
	2015-16	**2016-17**	**2017-18**	**2018-19**
Revenue (in ZAR/SZL)				
Profit before Tax (in ZAR/SZL)				
Net Worth (in ZAR/SZL)				

Name and Designation of Signatory:……..

Name of firm:……

Address: ……..

Signature of Authorized Person ……..

Date…….

Profile of the project team **ANNEXURE #4**

(The personnel proposed to be deployed shall be professionally qualified and have adequate experience in implementing the proposed services**)**

no.	Name	Designation	Qualification	Proposed Position	Task proposed to be assigned	Duration of Team member
1.						
2.						
3.						

NOTE:

Provide details of at least two most relevant project experiences (including roles and responsibilities) having scope similar to us.

Name and Designation of Signatory:……..

Name of firm:……

Address: ……..

Signature of Authorized Person ……..

Date……

CV of the Team Members **Annexure #5**

(Use separate sheets for each Team Member)

The company name	
Name	
Proposed Deployment Role of the Candidate	
Expertise/Training on	
Professional Qualifications	
Number of Years with present Employer	

Summarized Professional Experience in implementing relevant activity/service (for which the candidate is proposed for Company team) in reverse chronological order.		
From	**To**	**Company/Project/Position/Relevant Technical and Management Experience**

Certification by the Authorized Signatory

I, the undersigned, certify that to the best of my knowledge and belief, this resume reflects correct information and that the willful misstatement described herein may lead to disqualification or dismissal of the above candidate.

Name and Designation of Signatory:……..

Name of firm:……

Address: ……..

Signature of Authorized Person ……..

Date…….