



The Institution of Engineers (India)

AN ISO 9001 : 2015 CERTIFIED ORGANISATION
(ESTABLISHED 1920, INCORPORATED BY ROYAL CHARTER 1935)
8 Gokhale Road, Kolkata-700 020

A Century of Service to the Nation

No. T-1792

Dated : 15 May 2023

NOTICE INVITING TENDER

Implementation of Information Security Management System (ISMS), ISO 27001:2022 Certification through accredited certification agency and VAPT of IT Infrastructure

The Institution of Engineers (India) [IEI] invites Sealed Tenders in Single Stage two Envelope bid system for engagement of an organization for following work:

"Hiring of a consulting organization to implement Information Security Management System (ISMS) and provide ISO 27001:2022 certification through an accredited certification agency and Conduct Vulnerability Assessment and Penetration Testing (VAPT) Audit of IT Infrastructure/Resource".

The organization who shall be engaged has to perform the above mentioned task as per the scope of work mentioned in the tender document.

The sealed tenders are to be submitted in prescribed format along with details/supporting documents wherever applicable, if attached with the tender should be duly authenticated by the vendor/s. No over-writings shall be accepted unless authenticated with full signature of the vendor/s.

The tender shall be in two parts viz. **Technical Part – (Envelope – 'A')** and **Financial bids (Envelope 'B')** (Envelope 'A' and 'B' with the content shall be clearly marked on the top of the envelopes separately). **Technical Part (Envelope – 'A')** shall comprise of compliance documents against Qualification Requirement, **Earnest Money Deposit of Rs 10,000/-**, GST Registration certificate and any other document in support of technical capability. The Technical bid should not contain any financial indication, violation of which will invite disqualification. Financial bid shall comprise of quoted price only in the format provided with the tender document in **Envelope – 'B'**. Both Envelope – A & B shall be put in a third envelope, sealed and submitted within the prescribed date & time and with signature of the tender applicant over it.

The sealed tender duly superscribed with **"Implementation of ISMS (ISO:27001:2022)"** with Tender No. should be addressed to Director (Administration) sent at the Institution's address either by registered post/speed post/or by hand. Postal / couriered tender must reach to this office within stipulated date & time i.e., **upto 16.00 hrs of 05 June 2023.**

Tenders received after the stipulated date and time shall not be entertained. The Institution shall not be liable for any postal delays what so ever and tender received after the stipulated time/date are liable to be rejected summarily without giving any reason and any correspondence.


Director (Administration)

A. QUALIFICATION OF BIDDER

1. The bidder should be registered company and submit the certificate of incorporation.
 2. The Bidder should be an ISO 9001:2015 and ISO 27001:2013 certified organization (Certificate copies are to be attached as evidence).
 3. The Bidder should have Ten (10) years' experience in the domain of providing Consulting, Implementation & Certification services for ISO 27001 (Self Declaration with Company Profile).
 4. The bidder must have conducted process gap analysis for at least three customers during the last three years as part of the ISO implementation work. (Self-Declaration as per Annexure-IV to be submitted).
 5. The Bidder should provide satisfactory performance certificates *and contact details* from five customers where the Bidder has provided consultancy for ISO 27001 certification during last 3 Years. (work completion certificates are to be attached as evidence).
 6. The Agency must be CERT-In empanelled organization and should continue to remain in panel till the completion of the work. Valid copy of CERT-In empanelment certificate to be submitted (Copy of the certificate to be attached as evidence).
 7. The bidder should have conducted at least 3 VAPT Audit of Govt. / Autonomous / PSU organizations / Private Corporation during the last 3 years. (*Contact details and work completion certificates* are to be attached as evidence).
 8. Bidder should have minimum 5 nos. of experienced resources on their payroll with ISO-27001 Lead Auditor/ Lead Implementer Certification & minimum 3 nos. of resources having more than 5 years' experience in ISO 27001 implementation. (Self HR Declaration and profiles of the persons are to be attached as evidence).
 9. The bidder should have at least 10 Information Security professional / VAPT expert on their payroll with CISA, CISSP, CEH etc. certification to execute the work. (Self HR Declaration and profiles of the persons are to be attached as evidence).
 10. The Bidder should not be blacklisted by any government / Autonomous / public / private organization in India (Self-Declaration to be provided).
 11. The Minimum Average Annual Turnover of the consulting firm from India operations from similar nature of work during the last three financial years should not be less than Rs. 1.5 Crore. The bidder should have positive net worth in each of the last three financial years on the date of bid submission. Audited documentary evidences are to be attached.
 12. The bidder should have an Office in Kolkata. Self-declaration with Address PAN No. & GSTIN (copy of certificates are to be attached as proof).
 13. Failure to provide the desired information documents by the bidder shall lead to disqualification of the Bidder.
 14. Firm should have licensed VA / PT Tool.
 15. Bidder has to accept Un-conditionally accepted the terms and conditions of this Tender Document.
- Mr.

B. GENERAL TERMS AND CONDITION

1. The price shall include all taxes, duties, levies, various charges etc. and no additional payment shall be admissible on any account.
2. The bidder has to deposit an earnest money of Rs 10,000/- along with quotation. In case of non-execution of the order by the successful bidder, the earnest money deposited will be forfeited. The earnest money deposited by unsuccessful bidders will be refunded on finalization and execution of the contract with the successful bidder. However, EMD of successful bidder shall be retained as Performance Guarantee. The bank Draft should be drawn in favor of "**The Institution of Engineers (India)**", payable at **Kolkata**. The same shall be returned to the vendor without any interest after successful completion of work.
3. The Total work to be completed with 12 months from the issuance of the work order.
4. Standard LD Clause for delay in supply / service @ 2% per week or part thereof subject to maximum of 10% of the order value will be applicable.
5. IEI reserves the right to reject any or all the quotations without assigning any reason whatsoever.
6. IEI reserve the right to reject the tender in part or whole without assigning any reason whatsoever.
7. Vendor shall not subcontract the job to any outside agency including their franchisee.
8. Payment shall be made after successful completion of the work and handover of deliverables services. No advance payment will be made.
9. Vendor is required to make onsite visit before submission of tender document to access the nature and volume of the work.
10. **Jurisdiction:** This Agreement will be governed by and construed in accordance with the laws of India and any dispute arising out of this agreement will be subject to the jurisdiction of Court at Kolkata only.
11. **Confidentiality:** The bidder has to submit an undertaking in their letter head regarding the Non-Disclosure of the information those would be shared with the vendor or learnt by vendor during the course of the work with any third party without consent of IEI and treat them as confidential. All non-disclosure provisions shall continue to be in force at all times even after the completion of the work completely.

C. SCOPE OF WORK

a. Background

The Institution of Engineers (India) (IEI) established in 1920 and statutory body engaged in the services of the engineering fraternity through its functional verticals of Membership, Publication, Seminar & Conferences, Examination and R&D Grant-in Aid activity. The IEI is granted Royal Charter in 1935. The IEI want to implement Information Security Management System for its Headquarter office situated at 8, Gokhale Road, Kolkata 700020.

b. Objective

- i. Identification and Mitigation of various threats and vulnerabilities thorough VAPT Audit of IT Infrastructure and Information Systems.

- ii. Performing gap analysis of the existing policies, procedures and practices with regards to requirements set forth in ISO 27001:2022 standards.
- iii. Development of a comprehensive set of policies and procedures that align with the ISO 27000:2022 standard.
- iv. ISMS Auditing and certification that align with the ISO 27000:2022 standard considering key consideration / extracts from ISO 22301 (BCMS) & ISO 27701 (PIMS) to be considered during deployment for Business continuity & Data Privacy in mind.

c. Job Description

The Scope of Work would encompass the following activities, commensurate with meeting all the requirements for successful implementation of Information Security Management System (ISMS) leading to ISO 27001:2022 certification covering the IT equipment & networks for The Institution of Engineers (India). The scope of work for an ISO 27000:2022 implementation at The Institution of Engineers (India) will include the following major modules:

- VAPT Audit of existing IT Infrastructure and Information Systems by CERT-IN empanelled organization for identification of risk, recommendation for mitigation of threat and issuance of Audit Compliance Certificate.
- Information security management system (ISMS) assessment: A thorough assessment of the organization's current information security management practices and procedures, in order to identify any gaps or areas for improvement.
- Policy and procedure development: Development of a comprehensive set of policies and procedures that align with the ISO 27000:2022 standard and meet the organization's specific information security needs.
- Implementation and training: Implementation of the ISMS, including the development of policies and procedures, and training of relevant personnel on the new practices and procedures.
- Monitoring and measurement: Ongoing monitoring and measurement of the ISMS to ensure it is functioning effectively and is meeting the organization's information security needs.
- Auditing and certification: An external audit of the ISMS to ensure compliance with the ISO 27000:2022 standard and obtaining the certification for the same.
- Maintenance and continuous improvement: Continual maintenance of the ISMS to ensure it remains effective over time and continuous improvement of the system.
- Along with ISMS, key consideration / extracts from ISO 22301 (BCMS) & ISO 27701 (PIMS) to be considered during deployment for Business continuity & Data Privacy in mind.

d. Phases

The Scope of Work would include the following phases:

- **Phase - I: Vulnerability Assessment and Penetration Testing for existing IT Infrastructure and Information Systems should not exceeds 60 days)**

The VAPT Audit includes the following:

| Sl.no. | Items | Nos | Action to taken |
|--------|---|-----|--|
| | Server | 03 | VAPT activity should be comprehensive but not limited to following activities: Network Scanning, Port scanning, system identification and trusted system scanning, Vulnerability scanning, Malware and Adware scanning, Spoofing, Application Security Testing, Access Control Mapping, Denial of Service Attack (DOS), Password cracking, Cookie Security, Functional Validations, Firewall rule review, OS Security configuration, server miss configuration, Errors triggering sensitive information leak, Audit Log Tracking, Brute Force attack etc. |
| | Managed Switches | 12 | |
| | Firewall | 01 | |
| | Endpoint Protection | 01 | |
| | Desktop /PC | 112 | |
| | Wi-Fi Router / AP | 05 | |
| | 1. IEI Application (a In-house ERP Desktop Application) | 01 | Security and vulnerability audit includes but not limited to various Injections including SQL injections, Directory Traversal, Authentication management, Buffer Overflows, Inputs validation, Insecure Storage, Remote Code execution, Web server information security, HTTP Injection, Insecure Direct Object Reference, Information leak, Improper Error Handling, configuration loopholes, API vulnerabilities, Brute Force. Any Other known vulnerability applicable for Windows application are to be considered. Latest OWASP guidelines may be considered as guidelines. |
| | 2. Other Ancillary Applications | 04 | |

Process Review:

- **Scope Definition:**

One of the fundamental aspects for successful adoption of ISO 27001:2022 guidelines and standards is the clear and accurate definition of the scope of the ISO 27001:2022 adoption within The Institution of Engineers (India). The consulting firm shall Identify and document the scope of ISO 27001 certification and assist The Institution of Engineers (India) in outlining the extent and scope of ISMS.

- **Gap Analysis**

Performing gap analysis of the existing information security policies and procedures with regards to requirements set forth in ISO 27001:2022 standards. The gap analysis shall be carried out against the guidelines of ISO 27001:2022 standard. The outcome shall be discussed with nominated IT team through workshop and an input will be obtained on future course of engagement.

- **Risk Assessment & Risk Treatment:**

The objective of the Risk Assessment activity is to carry out a review of the information security (IS) risks faced by The Institution of Engineers (India) from IT perspective and their relative significance as per ISO 27001:2022 standard requirement. This phase culminates with identification of the IS risks that may result in compromise of system and classified information. In this phase, the consultant shall conduct IS risk assessment and formalize the IS risk treatment plan, which will serve as the action plan for development of the information security program.

- **Phase – III: Statement of Applicability (SoA)**

SoA identifies the controls that have selected to address the risks that were identified in the risk assessment process. It explains why those controls have been selected, states whether or not they have been implemented, and explain why any controls have been omitted.

The Statement of Applicability is a critique of the objectives and controls applicable to the needs of The Institution of Engineers (India). The consulting firm shall arrange needful in defining and documenting a Statement of Applicability.

Information Security Management System Documentation

The consulting firm shall review the existing IT & Cyber security policy, and other policy document/plan in accordance with the information security guidelines outlined by the ISO 27001 standards and assist in update of the policy document, if require.

The consulting firm shall also prepare ISMS policy, processes and systems and procedures relevant to managing risk and implementation of ISMS for improving information security to deliver results in accordance with the organization's overall policies and objectives as per IT&C perspective

The consulting firm would have to review and formulate new required documentation (if required) such as Disaster Recovery Plan (DRP), Standard & guidelines, Procedures, subordinate documents, Baseline security, Crisis Management Plan etc. The required documentation should also include the steps to be performed for ISO 27001 compliance.

The information security policy document will direct the ISMS implementation at The Institution of Engineers (India) and provide guidelines for the development and / or updation of the relevant information security and other related procedures and practices.

Further, the consulting firm shall also review the related information security procedures and these procedures shall be formalized by The Institution of Engineers (India).

- **Phase –IV: Implementation of ISO 27001 controls: Program Management of internal Rollout:**

Program Management of internal roll out - Procedures and Technical rollout strategy formulation. A core team from the Consulting Agency would manage the entire program of Implementation. The broad activities that are to be supported by the consulting firm are as under:

- Planning the roll out activities.
- Guiding the nominated team of IEI to carry out the defined activities.
- Detailed workshops for each policy area to explain and conduct a walkthrough.
- Initiate roll outs and monitor/check the progress, and provide the inputs.

- **Phase – V: Pre-Certification Review [Internal Audit]**

Carrying out a one-time review post implementation of information security controls by The Institution of Engineers (India). The Pre-Assessment exercise is to be conducted prior to the Certifying Agency audit and post/during the Implementation Activity.

The following steps are taken as part of the Pre- Assessment

- Review of Documentation
- Review of Training for Users
- Conducting Internal Audit
- Finding Non-Conformances
- Fixing Non-Conformances
- Final Review by The Institution of Engineers (India).

- **Phase – VI: Certification Audit & Acceptance [Engaging External Agency]**

The following steps are taken:

- Vendor shall arrange for an external audit by an authorized organization
- Assist IEI in conducting external audit of ISO 27000:2022 standard
- Assist IEI for necessary compliance
- Obtaining the ISO 27000:2022 certification
-

e. Deliverables:

| Sl. | Phase | Deliverable description |
|-----|-------------------|---|
| | Phase- I | <p><u>VA/PT for existing IT Infrastructure and Information Systems</u></p> <ul style="list-style-type: none"> ✓ Submission of VA/PT Audit Report ✓ Assist IEI is mitigating the Vulnerabilities as per the Audit Report ✓ Review audit after incorporations of the mitigations ✓ Issuance of the Audit Compliance Certificate <p>Duration: should not exceed 60 days from issuance of the work order</p> |
| 1 | Phase- II | <p>Carrying out business understanding sessions with IT function and sub function to understand processes, Information assets viz. IT equipment & network across The Institution of Engineers (India) underlying in purview of IT function. Preparation of a Gap Assessment Report and submission for The Institution of Engineers (India) comments. After incorporating suggestions of The Institution of Engineers (India), the final report shall be constructed. Deliverables in Phase-II shall be as given below:</p> <ul style="list-style-type: none"> ✓ ISMS Scope: This deliverable will be in form of a document defining purview of the ISMS detailing the geographical locations, assets, technology, organization structure, key business relationships and/or processes covered, and scope limitations, if any. ✓ Gap Analysis Report: This report will highlight the gaps in existing security controls framework vis-à-vis the ISO 27001:2022 standard. ✓ Risk Assessment Report: This deliverable will be a report highlighting the risk rating of information assets based on the asset values and threats and vulnerabilities identified. <p>Duration: should not exceed 60 days from issuance of the work order</p> |
| 2 | Phase- III | <ol style="list-style-type: none"> 1. Statement of Applicability: This deliverable will be a document consisting of: <ol style="list-style-type: none"> a. Summary of Controls applicable based on Risk Assessment b. Reasons for inclusion / exclusion. 2. ISMS Documents: This will include the following documents: <ol style="list-style-type: none"> a. Information Security Policy and applicable procedures; b. Information Security Organization Structure and responsibilities. <p>Duration: should be completed within 90 days from issuance of the work order</p> |
| 3 | Phase-IV | <p>Rollout Strategy, Project Plan for Implementation, Implementation Activity Status Reports.</p> <p>Duration: should be completed within 90 days after completion of phase-III</p> |
| 4 | Phase- V | <p>Pre-assessment / Internal Audit Report: This deliverable will be provided post-implementation of information security controls by IT team of The Institution of Engineers (India). The report will highlight the gaps in existing security controls framework vis- à-vis the ISO 27001 standard.</p> <p>Duration: should be completed within 90 days after completion of phase-IV</p> |
| | Phase- VI | <p>ISO 27001:2022 Certification & Acceptance.</p> <p>Duration: Should be concluded within within 90 days after completion of phase-V.</p> <p>The total work must be concluded within 12 months from the date of issuance of work order under any circumstances.</p> |

TECHNICAL BID EVALUATION CRITERIA

Technical evaluation shall be made as per Table -A below and minimum 70 Marks required in order to qualify the Technical Criteria.

The Bidder has to mention their relevant remarks against each Requirements as mentioned in Table-A in their letterhead and sign it. Bidder is also required to enclose the relevant documents as annexure

| Sl. No. | Requirement | Response of Bidder | Max Credit Point | Documents to be attached |
|---------|--|--|------------------|--|
| 1 | GST Registration Certificate & PAN | YES/ NO | 5 | Copy of both documents to be attached. |
| 2 | Un-conditionally accepted the terms and conditions of this Tender Document | YES/ NO | 5 | 1. Declaration as per the Annexure-I is to be enclosed 2. Duly stamped, signed and dated on each page of the tender document is to be enclosed. |
| 3 | Bidder has 10 years experience in the domain of Consulting, Implementation & Certification services for ISO 27001 | YES/ NO | 20 | Copy of Work order / Completion Certificate to be submitted as proof of 10 years experience in the domain of ISO 27001 |
| 4 | Firm should not be currently blacklisted by any Govt./ Autonomous / public / private corporations | YES/ NO | 5 | Declaration as per the Annexure-II is to be enclosed |
| 5 | CERT-IN empanelled Organization | YES/ NO | 15 | Copy of the empanelment certificate showing the duration of the validity is to be attached |
| 6 | Bidder should be Certified with ISO 9001:2015 and ISO 27001:2022 | YES/ NO | 5 | Copy of both documents to be attached |
| 7 | Bidder should have process gap analysis for at least three customer during last 3 years | YES/ NO | 5 | Declaration as per the Annexure-IV is to be enclosed |
| 7 | Completed least 3 VAPT Audit during the last three years | YES/ NO | 5 | Copy of relevant Work order along with completion certificate to be attached |
| 8 | Firm should have licensed VA/PT Tool: (Below 5 = 2 marks 5 and Above = 5 marks) | YES/ NO | 5 | Declaration as per the Annexure-III is to be enclosed |
| 9 | Number Lead Auditor / Lead Implementer with 5 years experience (Below 5 = 5 marks 5 and Above = 10 marks) | Applicable Number be mentioned by Bidder | 10 | Declaration in letter head with name, certification details |
| 9 | Number of professionals & Consultants with certification like CEH, CISA, CHE, CISSP, ISO:27001 etc. (in own payroll) (Upto 10 = 5 marks Between 11-20 = 10 marks Between 21-30 = 15 marks More than 30 = 20 marks) | Applicable Number be mentioned by Bidder | 20 | Declaration in letter head with name, certification details |

Table: A

PART - B
FINANCIAL BID

Financial Bid for Implementation of Information Security Management System (ISMS), ISO 27001:2022 Certification through accredited certification agency and VAPT of IT Infrastructure

A. Rate of Services

| Sl. No. | Description | Rate | % of GST | Amount |
|---------|--|------|----------|--------|
| 1. | VA/PT and Security Audit IT Infrastructure | | | |
| 2. | ISO 27001:2022 Implementation | | | |
| 3. | ISO 27001:2022 Certification | | | |
| | Total | | | |

Total Amount against Sl. No. _____ to _____ as mentioned above will be
Rs.....

(Rupees.....)

Name :
Designation :
Signature :
Company Name :
Address :
Phone No. :
E-mail :
Date :

Seal of the Company

DECLARATION ON ACCEPTANCE OF TERMS AND CONDITIONS

(TO BE GIVEN ON A LETTER HEAD OF THE COMPANY / FIRM)

Ref: T-1792 dated 15.05.2023

To,
The Secretary and Director General
The Institution of Engineers (India)
8, Gokhale Road,
Kolkata – 700020

Sub: Acceptance of Terms and Conditions against your
Tender No. T-1792 dated 15.05.2023

Dear Sir,

1. We have carefully read and understood all the terms and conditions of the Tender document and hereby convey our un-conditional acceptance to the same. Also duly stamped, dated and signed by us on each page of the tender document is enclosed as proof of the terms and condition mentioned in the Tender Document.
2. The information / documents furnished along with the Tender Document Application are true and authentic to the best of my knowledge and belief. We are well aware of the fact that, furnishing of any false information / fabricated document would lead to rejection of our bid / application at any stage besides liabilities towards prosecution under appropriate law.
3. We have apprised ourselves fully about the job to be done during the period of engagement and also acknowledged to bear consequences of non-performance or deficiencies in the services on our part.
4. We also declare that
 - We have no objection, if enquiries are made about the work listed by us.
 - We have not been found guilty by a court of law in India for fraud, dishonesty or moral turpitude.
 - We agree that the decision of The Institution of Engineers (India) in selection of the Agency will be final and binding to us.

Thanking you,
Yours sincerely,

Name.....

Designation.....

Date.....

Company stamp / Seal.....



DECLARATION ON NOT BEING BARRED / BLACK LISTED

(TO BE GIVEN ON A LETTER HEAD OF THE COMPANY / FIRM)

Ref: T-1792

To,
The Secretary and Director General
The Institution of Engineers (India)
8, Gokhale Road,
Kolkata - 700020

Dear Sir,

We hereby declare that our organization <<***Name of the organization***>> is a Cert-in empanelled organization and have not been currently blacklisted by any Central Govt. / State Govt. / Autonomous Bodies / PSUs / Private Corporations.

Thanking you,

Yours sincerely,

Name.....

Designation.....

Date.....

Company stamp / Seal.....



DECLARATION ON USE OF LICENSED VAPT TOOLS
(TO BE GIVEN ON A LETTER HEAD OF THE COMPANY / FIRM)

Ref: T-1792

To,
The Secretary and Director General
The Institution of Engineers (India)
8, Gokhale Road,
Kolkata - 700020

Dear Sir,

We hereby declare that our organization <<***Name of the organization***>> is a Cert-in empanelled organization and use the following tools for Cyber Security Audit and Vulnerability and Penetration Testing (VAPT):

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

We also confirm that the above mentioned tools used by us are having valid license / subscriptions.

Thanking you,

Yours sincerely,

Name.....

Designation.....

Date.....

Company stamp/ Seal.....



ANNEXURE-IV**DECLARATION ON PROCESS GAP ANALYSIS**
(TO BE GIVEN ON A LETTER HEAD OF THE COMPANY / FIRM)**Ref: T-1792**

To,
The Secretary and Director General
The Institution of Engineers (India)
8, Gokhale Road,
Kolkata – 700020

Dear Sir,

We hereby declare that our organization <<***Name of the organization***>> has conducted process gap analysis during last three years for below mentioned customers.

| Sl.No | Customer Name | Year |
|-------|---------------|------|
| 1. | | |
| 2. | | |
| 3. | | |

Thanking you,

Yours sincerely,

Name.....

Designation.....

Date.....

Company stamp/ Seal.....

Note: The declaration of all annexure(s) is to be signed and sealed by the authorized signatory of the company.

MB.