EDII Invites Proposal for
Engagement of IT / Cyber Security Audit Service Provider

The Existing Setup of the Institute:

EDII has a PAN India presence with 6 Regional and 14 Branch/Project Offices and 255 employees across these offices. The Head office is located at Bhat, Gandhinagar. Around 350 desktop computers/printers are connected to the Local Area Network (Active directory) and internet. A firewall is installed to filter the web content and internet resource allocation. All users are free to use external devices like pen drive, external HDD, CDs etc. G-suite is being used for official emails (user@ediindia.org). Users are advised to take their official data backup to G-Drive. Emails and G-drive data of 50 important users are being backed up daily to the external cloud services. Head Office and one regional office are covered with 170 and 10 CCTV cameras, respectively.

The Branch/Project & Regional Offices do not have LAN structure. They work independently with standalone computer desktop/laptop systems. However, all Branch/Project & Regional Offices are using internet broadband connections for their routine work. They use official G-suite applications. However, they are also advised to take important data backup to the G-drive. Many employees are also working at the field level and prepare/develop required data/information with their laptop system. They are also allowed to use external devices.

The Institute uses authentic Microsoft software only with computer desktop/laptop systems along with anti-virus software. The printers are also freely used by the users.

The Institute is managing a large number of physical documents which also require security.

1. Background and Objective of the Assignment

EDII would like to engage a third party professional firm to perform services including a cyber security audit, review of their existing IT policies, creation of IT policies in line with ISO 27001. The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard ISO 27001, which includes the evaluation and gap analysis of the following with respect to CERT-IN guidelines:

- Current IT infrastructure of EDII
- Network and devices in use
- Operating systems and databases at Server level and User level
- Application packages and databases
- IT Policies including Operational Procedures in the current IT setup at EDII
- Identification of vulnerabilities, security flaws, gaps and loopholes
- Carry out ethical Internal and External Penetration Test for EDII IT setup and network
EDII would like to have the audit performed in a phased manner, wherein the

a. The First IT / Cyber Security Audit exercise needs to be commenced within 10 business days of issuing the Work Order. This needs to be done at all offices Locations (EDII Registered Office and EDII Regional Offices) and Departmental end users for all types of IT systems of EDII for IT / Cyber Security. Report of IT / Cyber Security Gaps along with the recommendations needs to be provided by the service provider and based on the same security Gap analysis and action would be taken at EDII end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 business days of commencement. Creation of Policies, etc need to be completed within next 10 business days

b. After the end of the First Phase of the IT/Cyber Security Audit and Reporting thereof by the service provider, EDII would take some reasonable time to study the Gaps in IT/Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by EDII has been completed, the service provider would be informed accordingly by concerned EDII representative, and thereafter the service provider should commence the Second Phase of Cyber Security Audit exercise. The time taken by EDII for bridging the IT/Cyber Security Gap will not affect the service provider in any way as the service provider will not be held responsible for any delay in the same.

c. The Second IT / Cyber Security audit needs to be completed within 20 business days after concerned EDII representative gives the go ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to review and ensure that remediation action has been taken against all the observation points/gaps. The Second phase audit exercise should also result in a Detailed Report and Analysis to be submitted for the current IT/Cyber Security status of EDII.

2. **Scope of Work:**

   The Scope of work for IT/Cyber Security Audit would be as per the Guidelines of CERT-IN and would be under the following broad categories:

   **2.1 CSAF audit:**

   Audit has to be carried out as per the CERT-IN guidelines and the Cyber Security Assessment Framework (CSAF) Version-2. Audit will include compliance audit as per CSAF markers along with the technical sampling audit for evidence gathering.

   The scope of work would cover the following areas:
   - Assessment against CSAF markers and evidence collection
   - Gap Analysis against CSAF
   - Documented evidences
   - Compliance Audits
2.2 Operating Systems and System Software such as Server Software, Domain controller Server, Server Hardware such as Blade Servers, Rack Servers, etc. The audit will include the server vulnerability assessment, pack and service patch updates, backdoor checks, default configuration.

2.3 Network connections of leased lines between Corporate and Regional Offices. Routers & Firewalls in EDII. Controls of Internet and other network access to various end-users by firewalls and anti-virus policies. The audit will include the network architecture review, network vulnerability assessment and network configuration review based on the vulnerability assessment. The Service Provider is supposed to analyse all reports, logs, etc. of the cyber security devices installed in EDII and provide input on cyber security policies for the same.

2.4 End user device audit: admin/user password control, license control, OS patches, updates, virus updates, shared folders access control, use of external devices, presence of unnecessary software.

2.5 Application audit
Audit has to be carried out on all the Software Applications and Packages that are exposed to Internet in EDII such as:

a. Website https and http services.
b. Biometric attendance system

2.6 The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard ISO 27001, which includes the evaluation and gap analysis of the following with respect to CERT-In guidelines:

a. Current IT infrastructure of EDII.
b. Network and devices in use.
c. Operating systems at Server level and User level.
d. Application packages and database.
e. Operational Procedures in the current IT setup at EDII.
f. Identification of vulnerabilities, security flaws, gaps and loopholes.
g. Carry out ethical Internal and External Penetration Test for EDII IT setup and Network.

2.7 Review the current IT Security Policy and provide recommendations for a roadmap to quality standard ISO 27001, including suggestions for best practices and procedures for EDII.

2.8 The Service Provider should provide the below mentioned details at the starting of the IT/ Cyber Security Audit exercise:

a. Methodology in which the Cyber Security Audit activity to be done, this will include the time frame of each activity so as to organize the cyber audit activity for better control and monitoring.
b. Standards of Security and Quality that are to be followed during the Cyber Security Audit activity.

c. Tools and Software that may be used for the cyber security audit activity. All tools and software used by the Service Provider need to be licensed.

d. Any Additional and Mandatory standards of Cyber Audit regulation as required for CERT-IN Audit, should be made available and applicable by the Auditor.

2.9 Schedule of Conducting Cyber Security Audit:

Cyber Security Audit in EDII needs to be conducted Two Times for the sake of cross-checking the effective implementation of the recommendations provided during the first Audit exercise. The First Cyber Security Audit exercise needs to be commenced within 10 days of issuing the Work Order. This needs to be done at all offices Locations and Departmental end users for all types of IT systems of EDII for Cyber Security. Audit will include compliance audit as per CSAF markers along with the technical sampling audit for evidence gathering. Report of Cyber Security Gaps need to be provided by the Service Provider and based on the same security Gap analysis and action would be taken at EDII end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 days of commencement.

a. After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the Service Provider, EDII would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by EDII has been completed, the Service Provider would be informed accordingly by concerned EDII representative, and thereafter the Service Provider should commence the Second Phase of Cyber Security Audit exercise. The time taken by EDII for bridging the Cyber Security Gap will not affect the Service Provider in any way as the Service Provider will not be held responsible for any delay in the same. The Report of the Gap Analysis of the First Phase of Cyber Security Audit should be made in such a way that it should help EDII in bridging the Gap.

b. The Second Cyber Security Audit need to be completed within 20 days after concerned EDII representative gives the go ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to identify and specify whether the Security Gap Report Submitted in the First Phase exercise, still exists or the Cyber Security Gaps are plugged-in to make the IT system of EDII secure and as much foolproof as possible. The Second phase audit exercise should also result in a Detailed Report and Analysis to be submitted for the current Cyber Security status of EDII.
2.10 Reports required by EDII, during and at the end of the Cyber Security Audit exercise:

a. Audit Plan and proposed and actual progress in the Cyber Audit exercise on a weekly basis.

b. Dates and Locations of Proposed and Actual Cyber Audit exercise.

c. Summary of Cyber Audit findings, including identification tests and the results of the tests need to be shared with concerned EDII officials on a weekly basis and as and when required by EDII.

d. Analysis of vulnerabilities and issues of concern of Cyber Security needs to be reported on a weekly basis.

e. Recommendations in line with CERT-IN guidelines to make EDII’s IT infrastructure CERT-IN compliant.

f. All the cyber security reports, device logs, etc. have to be shared with CERT-IN office representatives by the Service Provider. The purpose of the same is to keep CERTIN informed about the perceived and possible cyber threat to EDII at present and in future.

2.11 Report Presentations Applicable to be submitted for Cyber Security Audit:

a. Summary of Cyber Security Audit findings including identification tests, tools used and results of tests performed, to be submitted to EDII on a weekly basis.

b. Analysis of the vulnerabilities and issues of concern in EDII’s IT setup concerning Cyber Security to be reported on a weekly basis.

c. Recommendation for action to plug-in the Cyber Security gaps to be reported on a weekly basis.

d. Weekly progress reports to be submitted on the Cyber Security Audit activity to keep EDII informed about the status and completion of the same.

e. Final Report of Cyber Security Audit in EDII across all locations to be submitted immediately after the completion of the Audit activity.

f. Presentations on the Cyber Security Audit Report, its findings, conclusions, and recommendations for Gap Analysis and Plugging, as per CERT-In guidelines, need to be made to the management of EDII as required. Recommendations should also be given for Quality Standard ISO 27001, as this is also a prime objective of the Cyber Security Audit Output.
2.12 The Service Provider will analyse all reports, logs etc. from the cyber security devices in EDII, which has to be shared with CERT-IN office representatives to keep EDII and CERT-IN informed about cyber threats at present and in future at EDII IT facilities. The Service Provider will identify current and future cyber threats to EDII IT facilities and propose take actions to mitigate such upcoming cyber threats and vulnerabilities so identified.

2.13 The Service Provider will develop and document IT/Cyber Crisis Management Plan (CCMP) for EDII IT Facilities. The CCMP will be a separate document than the IT Security Policy of EDII and will contain strategy followed in case of a Cyber attack or threat in EDII. The CCMP will encompass all units of EDII as the cyber attack may happen at any branch location of EDII.

2.14 Details of the Authorized Contact person for the Cyber Security Audit Exercise need to be provided by the Service Provider, designated for EDII, to be the single point of contact for the Service Provider.

3. SCOPE OF IT INFRASTRUCTURE TO BE AUDITED:

<table>
<thead>
<tr>
<th>Sr.No.</th>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Organization locations</td>
<td>6 Regional &amp; 14 Branch offices</td>
</tr>
<tr>
<td>2</td>
<td>Inter Connectivity between locations</td>
<td>Not connected</td>
</tr>
<tr>
<td>3</td>
<td>No. of end user stations under Scope</td>
<td>Approx. 430</td>
</tr>
<tr>
<td>4</td>
<td>No. of Servers</td>
<td>Three</td>
</tr>
<tr>
<td>5</td>
<td>Operating systems:</td>
<td>MS Windows</td>
</tr>
<tr>
<td>6</td>
<td>No. of Routers</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>No. of L2 Switches/access Switches</td>
<td>38 Switches</td>
</tr>
<tr>
<td>8</td>
<td>Firewall devices</td>
<td>One – Sophos</td>
</tr>
<tr>
<td>9</td>
<td>No. of SAN/NAS Storage</td>
<td>Two</td>
</tr>
<tr>
<td>10</td>
<td>Information Security policy</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>Software Applications</td>
<td>MS office, Web browsers, Acrobat Reader, Tally,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SPSS, CorelDraw, Adobe Design, Gsuite apps etc.</td>
</tr>
<tr>
<td>12</td>
<td>Outsourced applications/servers</td>
<td>ERP</td>
</tr>
<tr>
<td>13</td>
<td>Online payment transactions</td>
<td>Third Party Merchandised</td>
</tr>
</tbody>
</table>

4. Deliverables of the Engagement - 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 IT/Cyber
security assessment report/audit report should include expert recommendations which will make the EDII IT environment secure and sustainable. Report should include the following sections but not limited to:

1) Assessment report on the Information/IT Security Policy of EDII and provide recommendations for a roadmap to quality standard ISO 27001, including suggestions for best practices and procedures for EDII

2) Development of the Information Security/IT related Policies, as per ISMS 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 environmental security

3) IT/Cyber Security Audit Report (along with recommendations) on EDII’s IT environment, as per CERT IN guidelines which should include but not limited to:
   - Access Control
   - Network Security Management
   - Database Management Process
   - Backup & Restore Policy and Backup Plan
   - Log management and monitoring policies for database, applications, router, firewall and operating systems
   - Incident Management and resolution process of the incidents
   - Patch update, bug fix and anti-Virus update process within EDII
   - Report on Penetration Testing and Vulnerability scan

4) Drafting the Cyber Crisis Management Plan (CCMP) for EDII IT Facilities

5. 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 assignment, 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 the execution of the assignment.

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

1. Approach and Methodology in which the IT/Cyber Security Audit activity 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.

2. Standards of Security and Quality that are to be followed during the IT/Cyber Security Audit activity.

3. Tools and Software that may be used for the IT/Cyber security audit activity. All tools and software used by the Service Provider need to be licensed.

4. Any Additional and Mandatory standards of Cyber Audit regulation as required for CERT-IN Audit, should be made available and applicable by the Auditor.

5. All the IT/Cyber security reports, device logs, etc. have to be shared with CERT-IN office representatives by the Service Provider. The purpose of the same is to keep CERT-IN informed about the perceived and possible cyber threat to EDII at present and in future.

Kindly submit your proposal along with your company profile, financial and customer list with contact details on or before: September 10, 2020 to manishdamani@ediindia.org

You may contact Mr. Manish Damani 079-23969151-53 OR Mr. Vimal Dagli - 9879556583 for query related to the above