बिड संख्या/Bid Number: GEM/2026/B/8209327

दिनांक /Dated: 18-11-2026

बिड दस्तावेज़ / Bid Document

बिड विवरण/Bid Details	
बिड बंद होने की तारीख/समय /Bid End Date/Time	30-11-2026 14:00:00
बिड खुलने की तारीख/समय /Bid Opening Date/Time	01-12-2026 14:00:00
बिड पेशकश वैधता (बंद होने की तारीख से)/Bid Offer Validity (From End Date)	90 (Days)
मंत्रालय/राज्य का नाम/Ministry/State Name	Ministry Of Education
विभाग का नाम/Department Name	Department Of Higher Education
संगठन का नाम/Organisation Name	University Grants Commission
कार्यालय का नाम/Office Name	Consortium For Educational Communication
शिकायत निवारण के संपर्क विवरण/ Contact details of Grievance redressal	HOD Email id :jd-sw@cec.nic.in Buyer Email id: maint-engr.cec@nic.in
वस्तु श्रेणी /Item Category	Cyber Security Audit - Security and Compliance Audit
अनुबंध अवधि /Contract Period	1 Year(s)
उन्हीं/समान सेवा के लिए अपेक्षित विगत अनुभव के वर्ष/Years of Past Experience Required for same/similar service	5 Year (s)
इसी तरह की सेवाओं का पिछला आवश्यक अनुभव है/Past Experience of Similar Services required	Yes
वर्षों के अनुभव एवं टर्नओवर से एमएसई को छूट प्राप्त है / MSE Relaxation for Years Of Experience and Turnover	Yes | Complete
स्टार्टअप के लिए अनुभव के वर्षों और टर्नओवर से छूट प्रदान की गई है /Startup Relaxation for Years of Experience and Turnover	No
विक्रेता से मांगे गए दस्तावेज़/Document required from seller	Experience Criteria,Bidder Turnover,Certificate (Requested in ATC),Additional Doc 1 (Requested in ATC) *In case any bidder is seeking exemption from Experience / Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer
क्या आप निविदाकारों द्वारा अपलोड किए गए दस्तावेज़ों को निविदा में भाग लेने वाले सभी निविदाकारों को दिखाना चाहते हैं? संदर्भ मेनू है/Do you want to show documents uploaded by bidders to all bidders participated in bid?	Yes (Documents submitted as part of a clarification or representation during the tender/bid process will also be displayed to other participated bidders after log in)

बिड विवरण/Bid Details	
बिड लगाने की समय सीमा स्वतः नहीं बढ़ाने के लिए आवश्यक बिड की संख्या। / **Minimum number of bids required to disable automatic bid extension**	3
दिनों की संख्या, जिनके लिए बिड लगाने की समय-सीमा बढ़ाई जाएगी। / **Number of days for which Bid would be auto-extended**	5
ऑटो एक्सटेंशन अधिकतम कितनी बार किया जाना है। / **Number of Auto Extension count**	1
बिड से रिवर्स नीलामी सक्रिय किया/**Bid to RA enabled**	No
बिड का प्रकार/**Type of Bid**	Single Packet Bid
तकनीकी मूल्यांकन के दौरान तकनीकी स्पष्टीकरण हेतु अनुमत समय /**Time allowed for Technical Clarifications during technical evaluation**	2 Days
अनुमानित निविदा मूल्य (सभी करों सहित) भारतीय रुपये में / **Estimated Bid Value in INR (Inclusive of all taxes)**	65000
मूल्यांकन पद्धति/**Evaluation Method**	Total value wise evaluation
मध्यस्थता खंड/**Arbitration Clause**	No
सुलह खंड/**Mediation Clause**	No

ईएमडी विवरण/EMD Detail

आवश्यकता/Required	No

ईपीबीजी विवरण /ePBG Detail

एडवाइजरी बैंक/Advisory Bank	State Bank of India
ईपीबीजी प्रतिशत (%)/ePBG Percentage(%)	5.00
ईपीबीजी की आवश्यक अवधि (माह) /Duration of ePBG required (Months).	14

(a).ईएमडी और संपादन जमानत राशि, जहां यह लागू होती है, लाभार्थी के पक्ष में होनी चाहिए। / EMD & Performance security should be in favour of Beneficiary, wherever it is applicable.

लाभार्थी /Beneficiary :

Director
Consortium for Educational Communication, Department of Higher Education, University Grants Commission, Ministry of Education
(Director, Cec)

बोली विभाजन लागू नहीं किया गया/ Bid splitting not applied.

एमआईआई अनुपालन/MII Compliance

एमआईआई अनुपालन/MII Compliance	Yes

एमएसई खरीद वरीयता/MSE Purchase Preference

एमएसई खरीद वरीयता/MSE Purchase Preference	Yes
सूक्ष्म और लघु उद्यम मूल उपकरण निर्माताओं/सेवा प्रदाता को खरीद में प्राथमिकता, यदि उनका मूल्य L1+X% / Purchase Preference to MSE OEMs/ Service Provider available upto price within L1+X%	15

1. If the bidder is a Micro or Small Enterprise as per latest orders issued by Ministry of MSME, the bidder shall be relaxed from the eligibility criteria of "Experience Criteria" as defined above subject to meeting of quality and technical specifications. The bidder seeking Relaxation from Experience Criteria, shall upload the supporting documents to prove his eligibility for Relaxation.
2. If the bidder is a Micro or Small Enterprise (MSE) as per latest orders issued by Ministry of MSME, the bidder shall be relaxed from the eligibility criteria of "Bidder Turnover" as defined above subject to meeting of quality and technical specifications. If the bidder itself is MSE OEM of the offered products, it would be relaxed from the "OEM Average Turnover" criteria also subject to meeting of quality and technical specifications. The bidder seeking Relaxation from Turnover, shall upload the supporting documents to prove his eligibility for Relaxation.
3. Years of Past Experience required: The bidder must have experience for number of years as indicated above in bid document (ending month of March prior to the bid opening) of providing similar type of services to any Central / State Govt Organization / PSU. Copies of relevant contracts / orders to be uploaded along with bid in support of having provided services during each of the Financial year.
4. **Purchase preference to Micro and Small Enterprises (MSEs):** Purchase preference will be given to MSEs having valid Udyam Certificate and whose credentials are validated online through Udyam Registration portal as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail themselves of the Purchase preference, the bidder must be the manufacturer / OEM of the offered product on GeM. In respect of bid for Services, the bidder must be the Service provider of the offered Service. Traders are excluded from the purview of Public Procurement Policy for Micro and Small Enterprises and hence resellers offering products manufactured by some other OEM are not eligible for any purchase preference. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service, and Buyer will decide eligibility for purchase preference based on documentary evidence submitted in case of product bids, whereas in case of services the eligibility is automatically validated. If L-1 is not an MSE and MSE Seller (s) has / have quoted price within L-1+ 15% (Selected by Buyer) of margin of purchase preference /price band defined in relevant policy, such MSE Seller shall be given opportunity to match L-1 price and contract will be awarded for % (selected by Buyer) percentage of total quantity. The buyers are advised to refer the OM_No.1_4_2021_PPD_dated_18.05.2023 for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017. Benefits of MSE will be allowed only if seller is validated on-line in GeM profile as well as validated and approved by Buyer after evaluation of documents submitted.
5. If L-1 is not an MSE and MSE Service Provider (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band as defined in the relevant policy, then 100% order quantity will be awarded to such MSE bidder subject to acceptance of L1 bid price.
6. Estimated Bid Value indicated above is being declared solely for the purpose of guidance on EMD amount and for determining the Eligibility Criteria related to Turn Over, Past Performance and Project / Past Experience etc. This has no relevance or bearing on the price to be quoted by the bidders and is also not going to have any impact on bid participation. Also this is not going to be used as a criteria in determining reasonableness of quoted prices which would be determined by the buyer based on its own assessment of reasonableness and based on competitive prices received in Bid / RA process.
7. Past Experience of Similar Services: The bidder must have successfully executed/completed similar Services over the last three years i.e. the current financial year and the last three financial years(ending month of March

prior to the bid opening): -
1. Three similar completed services costing not less than the amount equal to 40% (forty percent) of the estimated cost; or
2. Two similar completed services costing not less than the amount equal to 50% (fifty percent) of the estimated cost; or
3. One similar completed service costing not less than the amount equal to 80% (eighty percent) of the estimated cost.

अतिरिक्त योग्यता /आवश्यक डेटा/Additional Qualification/Data Required

Payment Terms: Website Security Audit

Scope of Work:1794996726.pdf

Format of Non disclosure agreement:1794996768.pdf

Format to be uploaded by buyer for the breakup of components on cost/price offered by Service Provider in the Bid:1794996791.pdf

Cyber Security Audit - Security And Compliance Audit (1)

तकनीकी विशिष्टियाँ /Technical Specifications

विवरण/ Specification	मूल्य/ Values
कोर / Core	
Type of Audit needed	Security and Compliance Audit
Team Deployment	Off-site
Standards against which compliance needed	ISO 27001: Information Security Management System (ISMS)
एडऑन /Addon(s)	

क्रेता द्वारा निर्धारित न्यूनतम मूल्य/Minimum Floor Price defined by Buyer

क्रेता द्वारा निर्धारित न्यूनतम मूल्य/Minimum Floor Price defined by Buyer	No

अतिरिक्त विशिष्टि दस्तावेज़ /Additional Specification Documents

परेषिती/रिपोर्टिंग अधिकारी /Consignees/Reporting Officer and Quantity

क्र.सं./S.No.	परेषिती/रिपोर्टिंग अधिकारी /Consignee Reporting/Officer	पता/Address	Quantity	अतिरिक्त आवश्यकता /Additional Requirement
1	Mangesh Wamanrao Lede	110067,Consortium for Educational Communication, IUAC Campus, Aruna Asaf Ali Marg	Project / Lumpsum Based	N/A

क्रेता द्वारा जोड़ी गई बिड की विशेष शर्तें/Buyer Added Bid Specific Terms and Conditions

1. **Generic**

   OPTION CLAUSE 25% : The buyer can increase or decrease the contract quantity or contract duration up to 25 percent at the time of issue of the contract. However, once the contract is issued, the contract quantity or contract duration can only be increased up to 25 percent. Bidders are bound to accept the revised quantity or duration.
   For lumpsum-based service contracts, the buyer may increase the scope of work and contract value up to 25 percent with the consent of the service provider

2. **Buyer Added Bid Specific Scope Of Work(SOW)**

   File Attachment Click here to view the file.

अस्वीकरण/Disclaimer

The Additional Terms and Conditions (ATC) have been incorporated by the Buyer after approval of their Competent Authority. The Buyer ,is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any restriction arising in the bidding process due to these ATCs and including the modification of technical specifications and / or terms and conditions governing the bid.All representations / grievances pertaining to the ATC clauses shall be raised with the buyer organization directly and not with GeM.If any of the clause(s) is/are incorporated by the Buyer regarding the following, the bid & resultant contract shall be treated as null & void. Further, GeM reserves the right, at its sole discretion, to cancel the bid forthwith, without issuance of any prior notice or intimation :-

1. Publishing Custom / BOQ bids for items for which regular GeM categories are available (unless such Custom / BOQ item is bunched with the major regular product Category Item).
2. Mandating procurement of / from specific Brand / Make / Model / Manufacturer / Dealer except in case of Single Bid / Proprietary Article Certificate (PAC) Buying.
3. Inclusion of disqualification criteria related to suspension of seller / service provider, where such suspension period has already expired.
4. Mandating submission of documents (other than EMD and signed Integrity Pact - which can be submitted within 5 days of bid opening) in physical form as a pre-requisite to qualify bidders.
5. Publishing bids on GeM for procurement of works.
6. Procurement of Goods by creating a Service bid on GeM & vice-versa.
7. Seeking sample with bid or approval of samples during bid evaluation process. However, trial / sample, as the case may be, shall be permitted in cases where trial / sample are allowed as per approved and published procurement policy of the Buyers' controlling Ministry / Department / State / Public Sector Enterprises Headquarters. If there is any violation of trial / sample clause with regard to approved policy of the Buyers' Ministry / Department / State / Public Sector Enterprises Headquarters, then this is to be determined and redressed by the concerned Buyer Organisation only.
8. Seeking experience from specific organization / department / institute only or from foreign / export experience.
9. Creating bid for items from incorrect categories.
10. Reference of conditions published on any external site or reference to external documents/clauses.
11. Asking for any Tender fee / Bid Participation fee, as the case may be.
12. Buyer added ATC Clauses which are in contravention of clauses defined in bid detail section, including specifications, EMD Detail, ePBG Detail and MII and MSE Purchase Preference sections of the bid, unless otherwise allowed by the applicable GeM GTC.
13. Any ATC clause in contravention with GeM GTC Clause 4 (xiii) (h) will be invalid. In case of multiple L1 bidders against a service bid, the buyer shall place the Contract by selection of a bidder amongst the L-1 bidders through a Random Algorithm executed by GeM system.
14. In a category based bid, adding additional items, through buyer added, additional scope of work/ additional terms and conditions/or any other document. If buyer needs more items along with the main item, the same must be added through bunching category based items or by bunching custom catalogues

or bunching a BoQ with the main category based item, the same must not be done through ATC or Scope of Work.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

All GeM Sellers/Service Providers shall ensure full compliance with all applicable labour laws, including the provisions, rules, schemes and guidelines under the four Labour Codes i.e. the Code on Wages, 2019; the Industrial Relations Code, 2020; the Occupational Safety, Health and Working Conditions Code, 2020; and the Code on Social Security, 2020 as and when notified and brought into force by the Government of India.

For all provisions of the Labour Codes that are pending operationalisation through rules, schemes or notifications, the corresponding provisions of the pre-existing labour enactments (such as The Minimum Wages Act, 1948, The Payment of Wages Act, 1936, The Payment of Bonus Act, 1965, The Equal Remuneration Act, 1976, The Payment of Gratuity Act, 1972, etc. and relevant State Rules) shall continue to remain applicable.

The Seller/ Service Providers shall, therefore, be responsible for ensuring compliance under:

- **All notified and enforceable provisions of the new Labour Codes as mentioned hereinabove; and**
- **All operative provisions of the erstwhile Labour Laws until their complete substitution.**

All obligations relating to wages, social security, safety, working conditions, industrial relations etc. and any other statutory requirements shall be strictly met by the Seller/ Service Provider. Any non-compliance shall constitute a breach of the contract and shall entitle the Buyer to take appropriate action in accordance with the contract and applicable law.

This Bid is governed by the General Terms and Conditions, conditions stipulated in Bid and Service Level Agreement specific to the Service, as the case may be, as provided in the Marketplace.

However, in case of Service, if any condition specified in General Terms and Conditions is contradicted by the conditions stipulated in Service Level Agreement specific to said Service, then it will over-ride the conditions in the General Terms and Conditions.

This Bid is governed by the सामान्य नियम और शर्तें/General Terms and Conditions, conditions stipulated in Bid and Service Level Agreement specific to this Service as provided in the Marketplace. However in case if any condition specified in सामान्य नियम और शर्तें/General Terms and Conditions is contradicted by the conditions stipulated in Service Level Agreement, then it will over ride the conditions in the General Terms and Conditions.

जेम की सामान्य शर्तों के खंड 26 के संदर्भ में भारत के साथ भूमि सीमा साझा करने वाले देश के बिडर से खरीद पर प्रतिबंध के संबंध में भारत के साथ भूमि सीमा साझा करने वाले देश का कोई भी बिडर इस निविदा में बिड देने के लिए तभी पात्र होगा जब वह बिड देने वाला सक्षम प्राधिकारी के पास पंजीकृत हो।बिड में भाग लेते समय बिडर को इसका अनुपालन करना होगा और कोई भी गलत घोषणा किए जाने व इसका अनुपालन न करने पर अनुबंध को तत्काल समाप्त करने और कानून के अनुसार आगे की कानूनी कार्रवाई का आधार होगा।/In terms of GeM GTC clause 26 regarding Restrictions on procurement from a bidder of a country which shares a land border with India, any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. While participating in bid, Bidder has to undertake compliance of this and any false declaration and non-compliance of this would be a ground for immediate termination of the contract and further legal action in accordance with the laws.

---धन्यवाद/Thank You---

WEB SECURITY AUDIT OF
CEC WEBSITE AND WEB-BASED LIBRARY MANAGEMENT SYSTEM

The Consortium for Educational Communication (CEC), New Delhi, hereby invites bids through the Government e-Marketplace (GeM) Portal from interested and eligible NICSI-empanelled or CERT-In-empanelled companies/firms/agencies for conducting a Web Application Security Audit of its website and Web-Based Library Management System.

The participating agencies must have prior experience in conducting security audits for Government Organisations. Documentary evidence, such as copies of work orders issued by the concerned organisations, must be submitted along with the bid for verification.

Terms and Conditions -

1. The Consortium for Educational Communication (CEC) intends to conduct a routine IT Security Audit of the following web-based applications:

   a. **CEC Official Website**

   b. **Web-Based Library Management System**

2. The bidder must quote against all items/columns specified in the Financial Bid as per **Annexure-A**. Failure to quote against any item shall render the bid non-responsive and incomplete, and the bid shall be liable to be rejected.

3. The detailed Scope of Work for the proposed Web Security Audit is enclosed with the tender document and shall form an integral part of the tender.

4. Each page of the tender document and all supporting documents submitted along with the bid must be serially numbered, duly signed and stamped by the authorised signatory of the participating agency.

5. All entries in the tender documents must be legible, complete and clearly filled in. Any unavoidable overwriting or correction must be duly authenticated by the authorised signatory.

6. The participating agency must have successfully completed at least **two IT Security Audit assignments during the last three years** for Central Public Sector Undertakings (CPSUs), Government Organisations or reputed commercial organisations. Documentary evidence in the form of work orders/completion certificates must be submitted along with the bid.

7. The participating agency must have a support office in India with an operational helpdesk facility to provide necessary technical assistance and support.

8. The bid submitted by the participating agency shall remain valid for a period of **90 days** from the date of opening of the bid.

9. CEC reserves the right to accept or reject any or all bids, either in full or in part, without assigning any reason thereof.

10. The IT Security Audit must be completed within **three (03) weeks** from the date of issuance of the Work Order.

11. Wherever applicable, the bidder must quote the cost of the Security Audit and applicable taxes separately in the prescribed Financial Bid format. Failure to provide the cost breakup in the prescribed format may render the bid liable to rejection.

12. Payment shall be released through NEFT/RTGS after successful completion of the IT Security Audit, submission of the final Security Audit Report and issuance/submission of the requisite Security Audit Certificate, subject to acceptance by CEC.

13. **Empanelment validity:** Require bidders to submit valid NICSI or CERT-In empanelment certificates as applicable.

14. **Security Audit Certificate:** Clearly specify that the audit certificate must be issued by a CERT-In-empanelled agency, wherever required under applicable Government/NIC guidelines.

15. **Audit report:** Require submission of the Vulnerability Assessment and Penetration Testing (VAPT) report, including identified vulnerabilities and recommended corrective measures.

16. **Re-audit:** Include a provision for re-audit after CEC implements the security recommendations, if required, without additional charges.

17. **Confidentiality:** The agency must maintain strict confidentiality of CEC's websites information, server configurations, credentials and security-related findings.

18. **Audit coordination:** The audit shall be conducted in coordination with CEC, as the applications are hosted on staging servers at the CEC, New Delhi.

Annexure – 'A'

FINANCIAL BID

S.No.	Particulars	Cost (in Rupees)
1.	Cost for Security Audit a) CEC website b) Web Based Library Management System	
2.	GST (if applicable)	
3.	Any other taxes (if applicable)	
	Total Cost including Tax	

Signature of the Tenderer

Name of the Tenderer

Address & Seal

Telephone no.

Scope of Work for the Security Audit for

CEC Website and Web Based Library Management System

A. CEC Website

The website has been developed in-house by CEC; The Basic information of CEC website is mentioned below.

S.No.	Parameters	Description
1.	Web Application Name & URL	cec.nic.in
2.	Operating System Details (E.g. Windows-2003, Linux, AIX, Solaris, etc.)	Microsoft windows datacenter 2019 (64bit)
3.	Application Server with Version (E.g. IIS 5.0. Apache, Tomcat, etc.)	Apache 2.4.67
4.	Front-end Tool [Server-side Scripts] (E.g. ASP, Asp.NET, JSP, PHP, etc.)	PHP 8.5.6
5	Back-end Database (E.g. MS-SQL Server, PostgreSQL, Oracle, etc.)	MySQL 8.0.46
6.	Authorization No. of roles & types of privileges for the different roles	0
7.	Whether the application contains any content management System (CMS) (If yes then which? (E.g. Joomla/WordPress/Drupal/Liferay etc.)	No
8.	Total No. (Approximate) of Input Forms	1
9.	Total No. of input fields	1
10.	No. of login modules	0
11.	Whether the application is to be audited for Application Security Vulnerabilities for the 1st time?	Yes, 1st time
12.	Any other information, you would like to provide.	No

B. Web Based Library Management System

Web Based Library Management System developed in-house by CEC is successfully running since 2017 on server located at NIC Data Centre. The basic information of Web based Library Management system is mentioned below:

S.No.	Parameters	Description
1.	Web Application Name & URL	cecmedialibrary.nic.in, Web Based Library Management System
2.	Operating System Details (E.g. Windows-2003, Linux, AIX, Solaris, etc.)	Microsoft windows datacenter 2019 (64bit)
3.	Application Server with Version (E.g. IIS 5.0. Apache, Tomcat, etc.)	IIS
4.	Front-end Tool [Server-side Scripts] (E.g. ASP, Asp.NET, JSP, PHP, etc.)	Asp.NET
5	Back-end Database (E.g. MS-SQL Server, PostgreSQL, Oracle, etc.)	SQL Server 2019
6.	Authorization No. of roles & types of privileges for the different roles	7(MCD,PRE,REC,MCDE,MCP,LADMIN,JD)
7.	Whether the application contains any content management System (CMS) (If yes then which? (E.g. Joomla/WordPress/Drupal/Liferay etc.)	No
8.	Total No. (Approximate) of Input Forms	30
9.	Total No. of input fields	275
10.	No. of login modules	1
11.	Whether the application is to be audited for Application Security Vulnerabilities for the 1st time?	No, already audited
12.	Any other information, you would like to provide.	Application successfully running since 2017 on server located at NIC Data Centre, Shastri Park, New Delhi

SCOPE OF WORK FOR SECURITY AUDIT OF CEC WEBSITE AND WEB-BASED LIBRARY MANAGEMENT SYSTEM

1. Scope of Security Audit

1.1. The selected Auditor shall conduct a comprehensive assessment of the vulnerabilities, threats and security risks associated with the above-mentioned web applications through Internet-based Vulnerability Assessment and Penetration Testing (VAPT). The assessment shall include identification of security weaknesses, remedial measures and recommendations for mitigating the identified risks, with the objective of strengthening the overall security of the applications.

1.2. The Security Audit shall be conducted in accordance with applicable industry standards, the Open Worldwide Application Security Project (OWASP) methodology and relevant NIC Security Audit Guidelines.

1.3. Any security vulnerabilities, lapses or weaknesses identified during the audit shall be promptly reported to CEC, along with appropriate recommendations and corrective measures required to address the identified issues and ensure the security of the applications hosted on NIC servers.

1.4. The audit shall be conducted in conformity with applicable NIC Security Audit Guidelines. Upon successful completion of the audit, the Auditor shall provide a Security Audit Report clearly indicating the security status of all web pages, associated downloadable/linked files (including PDF, DOC), scripts, images and other application components. The report shall identify any vulnerabilities or malicious code that could potentially be exploited to compromise the application or gain unauthorised access to the hosting server, including through privilege escalation.

2. Responsibilities of the Selected Auditor

The selected Auditor shall undertake the Security Audit of the CEC Website and Web-Based Library Management System in the following manner:

2.1. **Verification of Vulnerable Services:** Identify and verify potentially vulnerable services, systems and application components strictly after obtaining prior written permission from CEC.

2.2. **Communication and Coordination:** Inform CEC promptly about any changes in the audit plan, testing location, source of testing, high-risk findings or any technical issues encountered during the audit.

2.3. **Documentation and Reporting:** Maintain proper documentation of all audit activities, testing procedures, observations, findings and recommendations, and submit reports as prescribed in this document.

2.4. **Task-1: Initial Web Security Audit/Assessment:** Conduct a comprehensive Web Application Security Audit, including Vulnerability Assessment and Penetration Testing (VAPT), of both applications and submit a detailed report identifying vulnerabilities, security risks and recommended corrective measures.

2.5. **Task-2: Re-Audit Based on Recommendations:** Conduct a follow-up security audit after CEC has implemented the recommended corrective measures, to verify whether the identified vulnerabilities have been successfully rectified.

2.6. **Issuance of Security Audit Certificate:** Upon successful completion of the audit and satisfactory verification of compliance with applicable NIC requirements, issue the requisite Security Audit Certificate separately for the CEC Website and Web-Based Library Management System, certifying their security status for hosting on NIC servers.

3. Audit Reports

The Auditor shall submit an initial report containing details of vulnerabilities identified in accordance with OWASP methodology, along with recommendations for corrective action, upon completion of Task-1.

After completion of Task-2 and verification of the corrective measures, the Auditor shall submit the final formal IT Security Audit Report.

The audit reports shall contain the following details:

3.1. Identification of the auditee, including address and contact details.

3.2. Dates and locations of the audit conducted under Task-1 and Task-2.

3.3. Terms of reference agreed upon between the auditee and the Auditor, including applicable audit standards, wherever relevant.

3.4. Details of the Audit Plan and methodology adopted.

3.5. References to relevant organisational documents, including applicable policies and procedures, wherever applicable, with document dates or version numbers.

3.6. Details of additional mandatory or voluntary standards and regulations applicable to the auditee.

3.7. Summary of audit findings, including identification tests, tools used and results of the tests performed.

3.8. Analysis of identified vulnerabilities, security weaknesses and other issues of concern.

3.9. Recommendations for corrective actions and mitigation of identified security risks.

3.10. Details of personnel involved in conducting the audit, including identification of trainees, if any. Any information that could not be verified or remains unknown shall be clearly identified as such in the report.

4. Confidentiality

The selected Auditor shall maintain strict confidentiality of all documents, information, technical details, server configurations, access credentials, audit findings and reports relating to the assignment.

The Auditor shall not share, publish, disclose, reproduce or disseminate any such information, either wholly or partially, to any third party without prior written permission from CEC.

All confidential information obtained during the assignment shall be used solely for the purpose of conducting the Security Audit. The Auditor shall ensure that such information is adequately protected throughout the audit process.

5. Deliverables and Audit Reports

The successful bidder shall submit the following deliverables upon completion of the Security Audit of the above-mentioned web applications:

i. A detailed Security Audit Report indicating the overall security status of the applications, identified vulnerabilities, security weaknesses and misconfigurations, along with their respective risk levels and recommended mitigation measures.

ii. Summary and detailed reports of security risks, vulnerabilities and audit findings, including appropriate countermeasures and recommended corrective actions to be undertaken by CEC.

iii. A re-audit report confirming the status of rectification of vulnerabilities identified during the initial audit.

iv. Final Security Audit Certificates, separately for the CEC Website and Web-Based Library Management System, in accordance with applicable NIC Security Audit Guidelines.

v. All reports and certificates shall be submitted in English, in A4-size format, in two (02) printed copies each.

vi. The Auditor shall also provide soft copies of all final reports and certificates in PDF format.

vii. All deliverables shall be submitted in accordance with the terms and conditions of this tender document and shall be subject to acceptance by CEC.

6. Duration / Completion of Contract

The entire assignment, including the initial Security Audit (Task-1), rectification verification and re-audit (Task-2), and submission of final reports and Security Audit Certificates, shall be completed within **three (03) weeks from the date of issuance of the Work Order**, in coordination with CEC.

The Auditor shall submit the initial audit report within the agreed audit schedule to enable CEC to undertake the necessary corrective measures within the stipulated contract period.