Terms of Reference

for

Security Audit of DIKSHA Portal, Mobile Application

&

N-VSK Portal

by

CERT-IN Empaneled Agencies

Date: 01/03/2023

V1.0

Issued by

Central Institute of Educational Technology (CIET),
National Council of Educational Research And Training (NCERT),
Sri Aurobindo Marg, New Delhi-110016

To

All CERT-In Empaneled Agencies

Sub:- Terms of Reference for conducting the Security Audit of DIKSHA Portal & Mobile Application, N-VSK Portal by CERT-In empaneled agencies.

1. The National Council of Educational Research and Training (NCERT) is an autonomous organization set up in 1961 by the Government of India to assist and advise the Central and State Governments on policies and programmes for qualitative improvement in school education. Central Institute of Educational Technology (CIET), a constituent unit of NCERT, came into existence in the year 1984 with the merger of Center for Educational Technology (CET) and Department of Teaching Aids(DTA). CIET is a premiere national institute of educational technology. Its major aim is to promote utilization of educational technologies viz. radio,TV, films, Satellite communications and cyber media either separately or in combinations, The institute undertakes activities to widen educational opportunities, promote equity and improve quality of educational processes at school level. The CIET is located at

   Central Institute of Educational Technology (CIET),
   National Council of Educational Research And Training (NCERT),
   Sri Aurobindo Marg, New Delhi-110016
2. DIKSHA is the national platform for school education available for all states and the central government for grades 1 to 12, and was launched in September 2017. DIKSHA can be accessed through a web-portal (https://diksha.gov.in/) and mobile application (android https://play.google.com/store/apps/details?id=in.gov.diksha.app&hl=en_IN&gl=US) and ios: https://apps.apple.com/in/app/diksha/id1587874277. DIKSHA provides access to a large number of curriculum linked e-content through several use cases and solutions such as QR coded Energized Textbooks (ETBs), courses for teachers, quizzes and others. As part of PM eVidya announced under the Atma Nirbhar Bharat programme, DIKSHA is the 'one nation; one digital platform' for school education in India. DIKSHA is being transformed into a platform for diverse and rich curriculum linked e-content requirements of learners and teachers for all states/UTs accessible across digital devices (laptop/mobile/desktop/tablets, TV and radio) in order to have coherence of access and learning experience
3. NEP 2020 caters to a multitude of requirements along with many programs / schemes run by the Centre / State that benefit different facets of education & stakeholders. But running multiple schemes brings in challenges in effective implementation due to lack of:

   i. Visibility to stakeholders - 'Ability to See' what's going on in almost real time

ii. Insights about what's happening - 'Ability to Make Sense' of what's working/what's not
iii. Coordination in driving improvements - 'Ability to Amplify Actions' through timely, coordinated efforts based on data & insights

4. Keeping in view the challenges faced, a comprehensive system through which the relevant stakeholders will be able to observe and monitor the overall information of education is required. The NDEAR compliant VSK (N-VSK) is an institutional avenue that **enables integrated** and **shared 'seeing' for amplifying data-based decision making** to drive action by key stakeholders for the success of their programs. The webportal is available at: https://vsk.ndear.gov.in/
5. Sealed Bids are invited on behalf of CIET - NCERT, Ministry of Education (MoE) from CERT-In Empaneled Agencies for Security audit of DIKSHA portal and mobile application, and N-VSK portal.
6. The proposal bids (Technical and financial in separate sealed covers inside the sealed cover envelope) duly filled in all respect enclosing necessary documents may be addressed to the following, so as to reach on or before **13.03.2023 till 17:00** hrs.:

   The Joint Director,
   Room No. 243, Second Floor, Chacha Nehru Bhawan,
   Central Institute of Educational Technology (CIET),
   National Council of Educational Research And Training (NCERT),
   Sri Aurobindo Marg, New Delhi-110016

   Note: Any bid received through email shall be summarily rejected.

7. The bids will be opened on **14.03.2023 at 11:00 Hrs** at CIET-NCERT, New Delhi in the presence of bidders who may wish to be present in person, either by themselves or through their authorized representatives.
8. To obtain first-hand information on the assignment, Bidders are encouraged to attend a pre-bid meeting. Attending the pre-bid meeting is optional. The Pre-bid Meeting shall be held on **6th March 2023** at 11:00 AM. The link for the VC is https://us02web.zoom.us/j/89218536664?pwd=bVA2ZFJMSzZFUGF2ZkhNQ0J4cENSQT09 Meeting ID: 892 1853 666 Passcode: 505665
9. Prebid queries (if any), shall be sent on or before 6th March 2023, 10:00 AM to the following email address: diksha.pmu@ciet.nic.in as per the format in **Annexure XI**
10. The detailed Terms & Conditions as **Annexure-I**, Scope of Work as **Annexure- II**, Format for submitting Price bid as **Annexure-III** and Bidder Details as **Annexure-IV** and so on, are attached with this document and can be downloaded from CIET website https://ciet.nic.in/

ANNEXURE-I

TERMS & CONDITIONS

The application is currently hosted at Microsoft Azure Cloud (and may soon be migrated to Oracle cloud). The bidders may well acquaint themselves with CERT-IN Standards before applying for this Terms of Reference.

Bids not satisfying the below eligibility criteria / not accompanied by the requisite documentary proofs shall be rejected.

1. **Eligibility Criteria:**

Sr. No	CRITERIA	DOCUMENTARY PROOF TO BE SUBMITTED
1	The bidder must be an empanelled auditor of CERT-In	Copy of Valid Letter of empanelment issued by CERT-IN.
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 letterhead) that they have not been blacklisted by any of the State/Central Government Institution or PSUs. In case, in the past, the name of their Company was blacklisted by any of the Govt. Institution or PSUs, the name of the company or organization must have been removed from the blacklist as on date of submission of the TOR	Undertaking by bidder (Annexure VI)
3	The bidder should be duly registered with the relevant tax authorities such as GST, etc.	Documentary evidence for such registration must be furnished
4	The bidder must have successfully completed minimum three (3) Security Audits of Web Application with minimum 1 Lakh user base or Mobile Application with minimum 1 Lakh downloads of PSUs / Govt. Organizations during the recent three financial years (FY 2022-23, FY 2021-22, FY 2020-21).	Copy of work order along with relevant details and completion certificate must be attached.
5	The bidder should have a minimum annual turnover of Rs.2.50 Crores for the financial years (i.e FY 2021-22, FY 2020-21 and FY 2019-20).	Annexure-VIII Audited Balance Sheet, Profit & Loss

		account for the last 3 financial years to be submitted
6	The Bidder should provide the list of the number of employees having the certifications/qualifications relevant in the domain of cyber security and audit. Some of the preferred & relevant certifications are provided in the list below. 1. CISM 2. COBIT Certificate Holder 3. CHFI 4. GIAC Certificate Holder 5. CRISC 6. SSCP 7. ECSA 8. Offensive Security Certified Professional 9. ECIH 10. CISA 11. CISSP 12. ISO 27001 LA/LI 13. CEHS The bidder should have at least 5 resources covering any six of the above listed certifications.	Undertaking by the bidder (Annexure# V)
7	The bidder should have at least one valid quality assurance accreditation/certification such as SEICMM/ ESCM/ CMMI/ ISO	As per Annexure-IX
8	Bidder has to submit company profile	As per Annexure-IV

2. **Instructions**

The bid shall contain two sealed packs - One with Eligibility related documents and other with Financials and cover envelope super-scribed as, “Bid for security audit of DIKSHA portal and mobile application & N-VSK portal”. All pages of the bid being submitted must be signed with an official seal.

Period of Bid Validity

a. Bids shall remain valid for 90 days from the date of Bid Opening. Any Bid valid for a shorter period than the period specified shall be rejected as non- responsive.
b. The last date for receipt of Bids is 14 March, 2023 till 17:00 Hrs.
c. Bids will be opened on 15 March, 2023 at 11:30 Hrs.

3. **Submission of Bids:**

The completed bids may be submitted in person or alternatively the bids may be sent by registered post/speed post to The Joint Director, Room No. 243, Second Floor, Central Institute of Educational Technology (CIET), National Council of Educational Research And Training (NCERT), Sri Aurobindo Marg, New Delhi-110016 so as to reach by the time and date stipulated for receipt of Bid. Any bids sent by email / fax will not be entertained.

4. **Late Bid:**

Any delay, including postal delay, in the receipt of bid would be treated as late submission of bid and shall be rejected. Bids handed over at the Reception Counter or any other counter or room or to any person, other than the authorized person of CIET-NCERT, shall not be considered.

5. **Language of Bids**

The Bids prepared by the Bidder and documents relating to the bids exchanged by the Bidder and CIET-NCERT, shall be written in the English language, provided that any printed literature furnished by the Bidder may be written in another language so long as the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English version shall govern.

6. **Bid Prices**

a. The prices shall be quoted in Indian Rupees only.
b. All taxes, duties, levies applicable etc. shall be clearly indicated.
c. Prices quoted must be final and shall remain constant throughout the period of validity of bid and shall not be subject to any upward modifications, whatsoever.

d. Bidders shall indicate their rates in clear/visible figures as well as in words and shall not alter/overwrite/make cutting in the quotation.

7. **Bid Evaluation**
    a. During Eligibility Criteria Evaluation, bidder's details shall be evaluated with reference to the required Eligibility Criteria as mentioned in this document and subsequently the bids of only eligible bidders shall be considered for final evaluation of financial bids.
    b. The price bids shall be evaluated as under:
        i. If there is any discrepancy between words and figures, the amount in words will prevail.
        ii. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and total price shall be corrected.
    c. If the Bidder does not accept the correction of the errors as above, the bid shall be rejected.

8. **Selection Criteria**
    a. The bidder whose evaluated price is found to be lowest (L-1), shall be considered for award of contract for Conducting Security Audit of DIKSHA and N-VSK Web and mobile application .

9. **Work Period**

    The work should be completed within 30 days from the date of issue of the Work Order.

10. **Payment Terms:**
    a. Payment will be released after successful completion of work, submission of final audit report and Security Audit clearance Certificate to CIET - NCERT and receipt of pre-receipted bills in triplicate.
    b. No advance payment shall be made.
    c. No claim on account of any price variation / escalation shall be entertained.
    d. No claim for interest in case of delayed payment will be entertained by the Authority.

11. **CIET-NCERT's right to accept or reject any or all bids**

    CIET-NCERT reserves the right to accept or reject any Bid, and to annul the Bidding process and reject all Bids at any time prior to Award of Contract without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds.

12. **Force Majeure**
    a. "Force Majeure" means an event beyond the control of the Auditor and not involving the Auditor's fault or negligence and not foreseeable. This type of event

may include but not limited to fires, explosions, floods, earthquakes, strikes, wars or revolutions etc.

b. The work execution period may be extended in case of Force Majeure condition. In order to be able to obtain an extension to the contract work period, the Auditor shall promptly notify auditee advising the existence of such an event, not later than one week of such event happening and produce the necessary documents from competent authority indicating the scope of such an event, and its impact on the performance of the contract and establish that such an event is not attributable to any failures on its part.
c. **Laws governing contract: -** The contract shall be governed by the laws of India for time being in force.
d. **Jurisdiction of courts:** The courts of Delhi shall alone have the jurisdiction to decide any dispute arising out of or in respect of the contract.

13. **Arbitration:**

In the event of any dispute arising out of the processing of this TOR or any agreement arising therefrom or any matter connected or concerned with the said agreement in any manner of its implementation or any terms and conditions of the said agreement, the matter shall be referred to Director - Digital Education, DoSEL, Ministry of Education, Government of India who may himself act as sole arbitrator or may nominate an officer of Ministry of Education as sole arbitrator, notwithstanding the fact that such officer has been directly or indirectly associated with the agreement. The bidder/ auditor will not be entitled to raise any objection for the appointment of such an officer of the Ministry of Education as the sole arbitrator. The award of the arbitrator shall be final and binding subject to the provisions of the arbitration and conciliation Act, 1996 and rules made thereunder. The seat of arbitration shall be New Delhi and the language of arbitration shall be in English only.

ANNEXURE-II

Scope of Work for the Security Audit

1. DIKSHA portal is accessible through https://diksha.gov.in/ and mobile application is accessible through https://play.google.com/store/apps/details?id=in.gov.diksha.app&hl=en_IN&gl=US (for android) & https://apps.apple.com/in/app/diksha/id1587874277 (for ios) and web portal for N-VSK is available at https://vsk.ndear.gov.in/ . The webportal is presently hosted on Azure Server and shall be migrated to Oracle Cloud soon. If required, CIET-NCERT will provide a staging server on Azure / Oracle cloud for security audit or may ask for security audit of DIKSHA (portal & mobile app) and N-VSK portal on Production Server as the case may be at the time of allotment of work.
2. The Auditor will have to carry out IT security assessment:
    a. Vulnerability Assessment and Penetration Testing and highlight vulnerabilities, threats and risks that may exist in the above portal and mobile application. Auditor will also suggest corrective actions/ recommendations to mitigate all identified risks, with the objective of enhancing the security of the portal and mobile application.
    b. GIGW (Guidelines for Government Websites) review to check that portal and mobile application adhere to the common minimum standards
3. The auditor agency will coordinate with a technical partner of CIET-NCERT and share recommendations to fix the vulnerabilities found during the Security Audit and have to re-audit the portal and mobile application till all issues are resolved, irrespective of the number of iterations. On completion of the security audit, the security audit agency has to issue a safe-to-host and free-from-vulnerability certificate.
4. The audit should be done per the guidelines or policies of Cert-In, MeitY, Govt of India, and Open Web Application Security Project (OWASP) methodology. Security Agency can refer to the given guidelines at https://www.cert-in.org.in/PDF/guideline_auditee.pdf.
5. During the Security Audit, if any lapse is found, the same shall be reported by the auditor to CIET-NCERT to make the application (portal and mobile app) fully secured.
6. The audit of the application (portal and mobile app) should be conducted in conformity with Government of India audit guidelines. After a successful security audit of the website, the security audit report from the auditor should clearly state that all web pages along with respective linked data files (in pdf / doc / xls etc. formats), all scripts and image files are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said website.

7. **Audit Environment:** The current cloud environment is on Azure (migration is being planned to Oracle Cloud). Supply / installation of auditing / testing tools, if any, for the audit purpose will be liability of the auditor.
8. **Responsibilities of Selected Auditor:** The Selected Auditor will conduct security Audit for the DIKSHA Portal and mobile application and N-VSK portal as under:
    a. Submit the audit plan
    b. Verify possible vulnerable services, only with explicit written permission from CIET NCERT and as per CERT-IN guidelines.
    c. Notify the auditee whenever there is any change in auditing plan / source test venue / high risk findings or any occurrence of testing problem.
    d. Responsible for documentation and reporting requirements for the audit.
        i. Task-1: Web Security Audit/Assessment.
        ii. Task-2: Re-audit the application and including review of observation in report of Task-1.
    e. On successful security audit, furnish certificate/safe to host certificate for the portal and mobile application as per MeitY - Government of India norms stating that the portal / mobile application is safe and free from any cyber vulnerabilities and suitable for hosting in Government cloud / NIC server.
9. **Audit report**

    The Auditor shall submit a report indicating the vulnerabilities as per OWASP and recommendations for action after completion of Task-1. The final formal IT security Audit Report should be submitted by the Auditor after the completion of all the tasks of Audit. The reports should contain:

    a. Identification of auditee (address & contact information).
    b. Dates and locations(s) of audit (Task-1 and Task-2)
    c. Terms of reference (as agreed between the auditee and auditor), including the standard for audit, if any.
    d. Audit Plan.
    e. Explicit reference to key auditee organization documents (by date or version) including policy and procedure documents, if any.
    f. Additional mandatory or voluntary standards or regulations applicable to the auditee.
    g. Summary of audit findings including identification tests, tools used, and results of tests performed.
    h. Analysis of vulnerabilities and issues of concern.
    i. Recommendations for action.

10. **Responsibility of CIET-NCERT**

    a. The auditor will submit the vulnerability report to CIET- NCERT, who will be responsible for removing any vulnerabilities through its technical partner (DIC - Digital India Corporation). After removing the vulnerabilities, as per the recommendations made by the auditor, CIET-NCERT will send confirmation to the auditor stating that the vulnerabilities have been rectified/ closed and applications are ready for re-assessment.
    b. The next round of audit shall be conducted by the auditor after receiving confirmation for removal / closure of vulnerabilities by CIET-NCERT through its technical partner.
    c. CIET-NCERT will refrain from carrying out any unusual or major changes during auditing / testing. If found necessary for privileged testing, the auditee can provide necessary access to the Auditor as mentioned in the clause 'Audit Environment' above after approval of Competent Authority,

11. **Confidentiality**

    All documents, information and reports relating to the assignment would be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner, by the Auditor. The auditor (including members of the audit team) will sign Non-Disclosure Agreement to this effect with CIET-NCERT.

12. **Non - Disclosure Agreement**

    a. The participating bidders shall have to submit signed NDA without any deviations on Company's Letterhead by authorized Signatory from vendor side as per prescribed format at Annexure-X while submitting a technical bid on the tender due date.
    b. After placement of order, the successful bidder shall have to submit mutually accepted/agreed NDA on Non-Judicial stamp paper of value Rs. 100/- in two (2) originals. The agreement will be executed by authorized representatives from Vendor Side & CIET, NCERT

13. **Technical Details of the applications are as follows:**

    a. Technical Details of DIKSHA Portal

S. No	Parameters/Information about the Website	Description
1	Web Portal Name & URL	**DIKSHA** DIKSHA Portal: https://diksha.gov.in/

2	Operating system details (i.e. windows - 2003, Linux, AIX, Solaris etc.,)	Ubuntu 16.04, 18.04 and 20.04
3	Application Server with Version (i.e. IIS 5.0. Apache, Tomcat, etc.)	NGINX, NodeJS
4	Front end Tool [Server-side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.)	NodeJS and Angular
5	Back end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	Multiple databases are used, Neo4J, ElasticSearch, Cassandra, Redis
6	Authorization No. of roles & types of privileges for the different roles	Multiple no. of Role (15 to 30)
7	Whether the site contains any content management module (CMS) (If yes then which?)	No, but has modules / building blocks for contributing and consuming content
8	No of input forms	About 50+ forms
9	No. (Approximate) of input Fields	200 - 300
10	No. of login modules	login module is available to support direct registration via email, phone, google account and state SSO logins
11	Involvement of any payment system,crypto, digital signature, gateway	no
12	Number of Web Services, if any	400+ APIs
13	Total no. of Static Pages	100
14	Total no. of dynamic pages	200

b. **Technical Details of the DIKSHA mobile application**

S.No	Technical Parameter	Information
1	Application URL	DIKSHA - for School Education (for android : https://play.google.com/store/apps/details?id=in.gov.diksha.app&hl=en_IN&gl=US For iOS:

		https://apps.apple.com/in/app/diksha/id1587874277
2	Mobile Application Platform	Android and iOS
3	About the Mobile Application:	DIKSHA Mobile app
4	Service/API used	100+
5	Any third-party software app relies on	PDF viewers and few more similar applications
6	Role Management/Access control system	Yes
7	No. of Pages/screens in the application	50 - 75
8	No. of pages/screens taking user inputs	20 - 25
9	Use of any special client side technologies (Ajax, Java Applets, Flash, Smart cards etc.) in the Application	Ionic and cordova
10	Number of privilege levels present in the application.	Multiple
11	Involvement of payment system, crypto, digital signature, gateway in the application	no
12	Back-end Database (E.g. MS-SQL Server, PostgreSQL, Oracle, etc.)	Multiple
13	No. of Servers	This is hosted in the cloud and has about 400+ servers

c. **Technical Details of N-VSK Web Portal:**

S. No	**Parameters/Information about the Website**	**Description**

1	Web Portal Name & URL	NVSK Portal: https://vsk.ndear.gov.in/
2	Operating system details (i.e. windows - 2003, Linux, AIX, Solaris etc.,)	Linux VMs
3	Application Server with Version (i.e. IIS 5.0. Apache, Tomcat, etc.)	Nginx
4	Front end Tool [Server-side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.)	Angular
5	Back end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	PostgreSQL
6	Authorization No. of roles & types of privileges for the different roles	3 roles
7	Whether the site contains any content management module (CMS) (If yes then which?)	no
8	No of input forms	0
9	No. (Approximate) of input Fields	0
10	No. of login modules	1
11	Involvement of any payment system, crypto, digital signature, gateway	no
12	Number of Web Services, if any	5
13	Total no. of Static Pages	1
14	Total no. of dynamic pages	20

14. **Deliverables and Audit Reports:**

The successful bidder will be required to submit the following documents in printed format (2 copies each) after the audit of above-mentioned web application:

i. A detailed report with security status and discovered vulnerabilities, weakness and misconfigurations with associated risk levels and recommended actions for risk mitigations.

ii. Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by CIET-NCERT.

iii. The final security audit certificate for and should be in compliance with the Government of India standards.
iv. All deliverables shall be in English language and in A4 size format.
v. The auditor will be required to submit the deliverables as per terms and conditions of this document.

ANNEXURE-III

(On Company Letterhead)

To

The Joint Director,
Central Institute of Educational Technology (CIET),
National Council of Educational Research And Training (NCERT),
Sri Aurobindo Marg, New Delhi-110016

Subject: Financial Bid for conducting Security Audit of DIKSHA Portal, Mobile Application (Android & iOS) and N-VSK Web Portal

I/We hereby submit the financial bid for conducting security audit of DIKSHA Portal and mobile application as per the tender document: -

#	***Description of Work***	***Amount (Rs.)***
1	Security Audit of DIKSHA Website (https://diksha.gov.in/)	
2	Security Audit of DIKSHA mobile application (android : https://play.google.com/store/apps/details?id=in.gov.diksha.app&hl=en_IN&gl=US & iOS https://apps.apple.com/in/app/diksha/id1587874277)	
3	Security Audit of N-VSK Web Portal: (https://vsk.ndear.gov.in/#/dashboard)	
4	Taxes (specify)(_____%)	
5	**Grand Total**	
	Rupees in words (Rupees……..... ……. ..... …… ……. ……)	

Note:

1. The Financial Bid shall contain ***nothing else but Prices*** only.
2. The L 1 shall be decided based on the Grand Total Amount at S.No. 5 above.

3. Bidders are requested to ensure that after quoting the prices this Annexure is duly signed with company seal. **Financial bids submitted without sign / company seal will not be accepted / considered**.

Date_____

Signature: _____
Name: _____
Designation: _____
Company Seal

ANNEXURE - IV

S.No.	Particulars	Information
1	Name of the Bidder	
2	Full address of the Bidder	
3	Authorized Signatory's Name	
4	CERT-In Registration Number (copy of self-attested valid CERT-In empanelment certificate to be submitted)	
5	Detailed office address of the bidder with Office Telephone Number, Fax Number, Mobile Number and Email along with name of the contact person	
6	Status of Applicant (Proprietorship Firm/Partnership Firm/Private Limited/Society/ (attach documentary evidence)	
7	GST Registration No. (copy to be enclosed)	
8	Copy of work order and completion certificate of successfully completed minimum three (3) Security Audits of Web Application with minimum 1 Lakh user base or Mobile Application with minimum 1 Lakh downloads of PSUs / Govt. Organizations during the recent three financial years (FY 2022-23, FY 2021-22, FY 2020-21).	As per Annexure-VII

Signature of the Authorized Signatory

Name:

Designation :

Name of the Bidding Entity :

ANNEXURE-V

Format to submit the no of the employees having Certifications/Qualifications relevant to the Security audit/testing domain

Sr. No	Certification	No of Employees currently working with the Agency

Certification by the Authorized Signatory -

I, the undersigned, certify that to the best of my knowledge and belief, this list reflects correct information and that the wilful misstatement described herein may lead to disqualification or dismissal of the agency.

Name and Designation of Signatory:

Seal & Signature of Authorized Person Name of Firm:

Address

ANNEXURE-VI

Self declaration for non-black listing format.The certificate below is to be provided by the Bidder.

<To be printed on Company letterhead>

Self-declaration for non-black listing

We confirm that our company as on date of submission of the proposal is not blacklisted or banned by any ministry/department/attached offices/subordinate offices under Government of India and any State government, autonomous bodies (established by Central/State govt), any Central/State PSUs in India for corrupt, fraudulent or any other unethical business practices.

Sincerely,

(Signature)

(Name & Signature of Key Managerial Personnel

ANNEXURE-VII

Bidder's Experience

(Use separate sheets for each Project and attach appropriate evidence. Ensure that the number of projects presented is with specific reference to the Evaluation Criteria of this bid document.)

Sr. No	Particulars	Details to be filled by the Bidder
1	Name of the Project	
2	Project location	
3	Name of the Company	
4	Company's address, contact person name & phone number	
5	The Company/project size (no. of users at Clients end at the time of audit services)	
6	Project Scope / Services delivered	
7	List of Audit tools used	
8	Security Standards used	
9	Value of the work done in INR	
10	Date of award or signing the contract	
11	Date of commencement of work	
12	Date of Completion	

Name and Designation of Signatory: Seal & Signature of Authorized Person Name of Firm:
Address

ANNEXURE-VIII

Bidders financial performance

	2021-22	**2020-21**	**2019-20**
Annual Turnover (in INR crores)			
Profit Before Tax (in INR crores)			
Net Worth (in INR crores)			

Note : Audited Balance Sheet, Profit & Loss account for the last 3 financial years to be submitted

Name and Designation of Signatory:

Seal & Signature of Authorized Person

Name of Firm:

Address

ANNEXURE-IX

Certifications acquired by the bidder

Sr. no	Name of the Certification	Date of acquiring	Valid till	Copy attached Yes/No

Name and Designation of Signatory:

Seal & Signature of Authorized Person

Name of Firm:

Address

ANNEXURE-X

MODEL NON-DISCLOSURE AGREEMENT

(Between CERT-In empanelled Auditor & Auditee)

THIS NON-DISCLOSURE AGREEMENT is made on this …….. day (date) of …… (Year) By and between In case of Central Government Ministry/ Departments #/State Government Departments President of India/Governor of (name of state) acting through ……. (Name, Designation) of …….. (Name of Ministry/ Department) address …… hereinafter referred to as "Auditee"which expression shall unless repugnant to the context or meaning thereof ,include its successors and assigns)of the first part.

In case of Autonomous Societies/ Not-for-profit companies/ Public sector Undertakings/Private sector ……. (Name of Company/ Society) incorporated /registered under the Companies Act,1956/2013/ the societies registration Act,1860 having its registered/corporate office at …… (hereinafter referred to as "Auditee" which expression shall unless repugnant to the context or meaning thereof, includes its successors, administrators and permitted assigns) of the first part .

And

Name incorporated/registered under the…….. Name of the Act having its registered/corporate office at ……(herein referred to as "Auditor" which expression shall unless repugnant to the context or meaning thereof ,includes its successors, assigns,administrators,liquidators and receivers) of the second part

WHEREAS

A. Auditor is a services organization empanelled by the Indian Computer Emergency Response Team (hereinafter CERT-IN) under Department of Electronics & IT, for auditing, including vulnerability assessment and penetration testing of computer systems , networks, computer resources & applications of various agencies or departments of the Government, critical infrastructure organizations and those in other sectors of Indian economy vide communication No……dated…….

B. Auditor as an empanelled Information Security Auditing organization has agreed to fully comply the "Guidelines for CERT-In Empanelled Information Security Auditing Organizations

Terms & conditions of empanelment and Policy guidelines for handling audit related data" while conducting audits.

C. Auditee is also aware of the aforesaid Guidelines along with guidelines for Auditee Organizations published by CERT-In.

D .Both Auditor and Auditee have given their irrevocable consent to fully comply the aforesaid Guidelines and any amendments thereof without any reservations.

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. Definitions. :

(a) The term "Confidential Information" shall include, without limitation, all information and materials, furnished by either Party to the other in connection with Auditee products and services including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic media, and including all proprietary information, customer & prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, business or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flowcharts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to Auditee products and services. Results of any information security audits, tests, analysis, extracts or usages carried out by the Auditor in connection with the Auditee's products and/or services, IT infrastructure, etc. shall also be considered Confidential Information

(b) The term "Auditee products" shall include all such products, goods, services, deliverables, which are subject to audit by the empanelled auditor under the Agreement.

2. Protection of Confidential Information. With respect to any Confidential Information disclosed to it or to which it has access, Auditor affirms that it shall:

(a) Use the Confidential Information as necessary only in connection with scope of audit and in accordance with the terms and conditions contained herein;

(b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its other clients;

(c) Not to make or retain copy of any details of products and/or services, prototypes, business or marketing plans, Client lists, Proposals developed by or originating from Auditee or any of the prospective clients of Auditee.

(d) Not to make or retain copy of any details of results of any information security audits, tests, analysis, extracts or usages carried out by the Auditor in connection with the Auditee's products and/or services, IT infrastructure, etc. without the express written consent of Auditee.

(e) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the auditee ; and

(f) Return to theauditee, or destroy, at auditee's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately on (i) expiration or termination of this agreement, or (ii) the request of Auditee therefor. X

(g) Not to send Auditee's audit information or data and/or any such Confidential Information at any time outside India for the purpose of storage, processing, analysis or handling without the express written consent of the Auditee.

(h) The auditor shall use only the best possible secure methodology to avoid confidentiality breach, while handling audit related data for the purpose of storage, processing, transit or analysis including sharing of information with auditee.

(i) Not to engage or appoint any non-resident/foreigner to undertake any activity related to Information Security Audit. In case of information security audits for Government/ critical sector organization, only the man power declared to CERT-In shall be deployed to carry out such audit related activities.

(j) Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between the Auditor and the Auditee or the nature of services to be provided by Auditor to the Auditee.

(k) Make sure that all the employees and/or consultants engaged to undertake any audit on its behalf have signed the mandatory non-disclosure agreement.

3. Onus. Auditor shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.

4. Permitted disclosure of audit related information:

The auditor may share audit information with CERT-In or similar Government entities mandated under the law as and when called upon to do so by such agencies with prior written information to the auditee.

5. Exceptions. The Confidentiality obligations as enumerated in Article 2 of this Agreement shall not apply in following cases:

(a) Which is independently developed by Auditor or lawfully received from another source free of restriction and without breach of this Agreement; or

(b) After it has become generally available to the public without breach of this Agreement by Auditor; or

(c) Which at the time of disclosure to Auditor was known to such party free of restriction and evidenced by documents in the possession of such party; or

(d) Which Auditee agrees in writing is free of such restrictions.

(e) Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;

6. Remedies. Auditor acknowledges that any actual or threatened disclosure or use of the Confidential Information by Auditor would be a breach of this agreement and may cause immediate and irreparable harm to Auditee or to its clients; Auditor affirms that damages from such disclosure or use by it may be impossible to measure accurately; and injury sustained by Auditee / its clients may be impossible to calculate and compensate fully. Therefore, Auditor acknowledges that in the event of such a breach, Auditee shall be entitled to specific performance by Auditor of its obligations contained in this Agreement. In addition Auditor shall compensate the Auditee for the loss or damages caused to the auditee actual and liquidated damages which may be demanded by Auditee. Liquidated damages not to exceed the Contract value. Moreover, Auditee shall be entitled to recover all costs of litigation including reasonable attorneys' fees which it or they may incur in connection with defending its interests and enforcement of contractual rights arising due to a breach of this agreement by Auditor. All rights and remedies hereunder are cumulative and in addition to any other rights or remedies under any applicable law, at equity, or under this Agreement, subject only to any limitations stated herein.

7. Need to Know. Auditor shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees and/or consultants of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the

Auditee. No information relating to auditee shall be hosted or taken outside the country in any circumstances.

8. Intellectual Property Rights Protection. No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.

9. No Conflict. The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

10. Authority. The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.

11. Governing Law. This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the jurisdiction of Courts and/or Forums situated at < Name of the city>

12. Entire Agreement. This Agreement constitutes the entire understanding and agreement between the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

13. Amendments. No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.

14. Binding Agreement. This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

15. Severability. It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

16. Waiver. Waiver by either party of a breach of any provision of this Agreement, shall not be deemed to be waiver of any preceding or succeeding breach of the same or any other provision hereof.

17. Survival. Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after expiration or termination of this Agreement.

18. Non-solicitation. During the term of this Agreement and thereafter for a further period of two (2) years Auditor shall not solicit or attempt to solicit Auditee's employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct business similar to Auditee with any employee and/or consultant of the Auditee who has knowledge of the Confidential Information, without the prior written consent of Auditee.

19. This Agreement is governed by and shall be construed in accordance with the laws of India. In the event of dispute arises between the parties in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, the parties shall attempt to resolve the dispute in good faith by senior level negotiations. In case, any such difference or dispute is not amicably resolved within forty five (45) days of such referral for negotiations, it shall be resolved through arbitration process, wherein both the parties will appoint one arbitrator each and the third one will be appointed by the two arbitrators in accordance with the Arbitration and Conciliation Act, 1996. The venue of arbitration in India shall be (please choose the venue of dispute resolution as the city) or where the services are provided. The proceedings of arbitration shall be conducted in English language and the arbitration award shall be substantiated in writing and binding on the parties. The arbitration proceedings shall be completed within a period of one hundred and eighty (180) days from the date of reference of the dispute to arbitration.

20. Term. This Agreement shall come into force on the date of its signing by both the parties and shall be valid up to …… year.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

In case of auditee being Central Government Ministry/ Departments

For & on behalf of President of India

(Name and designation of authorized signatory)

……

<Name of Central Govt. Ministry/Department>

Or

In case of auditee being State Government Department

For & on behalf of Governor of …….

< State name>

……..

(Name and designation of authorized signatory)

<Name of State Department>

Or

In case of Autonomous Societies/Not-for-profit-company/Public sector undertaking /Private Sector # for <Name of organization> , <Name and designation of authorized signatory> duly authorized by rules & regulations / of <Name of society>/ vide resolution no. …. Dated ……. Of Board of Directors of .....<Name of organization>.

(AUDITEE) (AUDITOR)

WITNESSES:

1.

2

Annexure XI Format for Pre-Bid Query Submission

#	Page No	Section No	Section Name	Statement as per RFP	Query by Bidder

1. The bidders should mention only the page number. Ex. '21' as page number and not 'Page 21.
2. Section No. – Example– '4' and not 'Section 4'
3. Section Name – Example – Scope of Work (Should be exactly the same as provided in the RFP)

Note–

a. The queries are to be submitted in the format provided above only. The bidders should ensure that they enter correct details in the format. In case of any inappropriate details being mentioned the purchaser shall not be responsible for the same and such queries may be discarded from providing any response.
b. The bidders to ensure that no cell merging (in excel) is done by them while preparing the query.
c. The bidders ensure that each of the query submitted by them is unique and no duplicate query is submitted by them as a result of copy-paste. It is expected from the bidder to carry out its own due- diligence before submitting the queries.
d. Bidders are expected to do a thorough check of the queries and ensure the completeness of the queries and spelling checks etc. before submitting the same to the purchaser