REQUEST FOR PROPOSAL (RFP)

FOR

SELECTION OF IS AUDITOR FOR CONDUCT OF COMPREHENSIVE CYBER SECURITY AUDIT

RFP Reference No.	**GEM/2024/B/5198605**
RFP Issuance Date	**24/07/2024**
Last Date of request for Queries/ Clarifications	**29/07/2024 01:00 PM**
Date and time of Pre-Bid Meeting	**30/07/2024 03:00 PM (through web-ex)**
Last Date and time for receipt of bids	**08/08/2024 up to 03:00 PM**
Date and time of opening Technical bids	**08/08/2024 03:30 PM**

Issued by:

IS Audit Cell,
Inspection & Audit Department,
Head Office, No.66 Rajaji Salai, Chennai 600 001
Phone: *25278716 / 12*
Email: *isaudit@indianbank.co.in*
Website: https://www.indianbank.in

This document is the property of Indian Bank and is meant for exclusive purpose of Bidding as per the Specification, Terms, Condition and Scope indicated in it. This document should not be copied, transferred, reproduced, distributed or recorded on any medium, including all forms of electronic medium, without written permission of Indian Bank. The use of contents of this document for any purpose other than stated herein is strictly prohibited and shall amount to copyright violation and thus, shall be punishable under the Indian Law.

INDEX

SCHEDULE [A]: IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION

S. No	Particulars	Timeline
1	**Issuance Date of RFP** (Date of RFP Issuance)	*24/07/2024*
2	**Last Date of request for Queries/ Clarifications** (Last Date of receiving request for queries / clarifications before the Pre-bid Meeting)	*29/07/2024 01:00 PM* Format for seeking clarification is enclosed as Annexure-V Bank's replies/clarifications and modifications, if any, will be published in the Bank's website and GeM portal only.
3	**Pre–bid Meeting Date and Venue Details**	*30/07/2024 at 03:00 pm.* through physical / virtual mode. Bidders willing to participate in pre-bid meeting need to submit their queries (as per format) along with their details to isaudit@indianbank.co.in on or before 29/07/2024 01:00 PM. Details of virtual/ physical pre-bid meeting would be communicated via e-mail to interested bidders separately.
4	**Last Date of Submission** of RFP Response **/ Closing Date in Online mode**	*08/08/2024 at 3.00 pm.*
5	**Technical Bid Opening Date & time**	*08/08/2024 at 3.30 pm*
6	**Date of Online Reverse Auction**	Will be intimated to technically qualified bidders (after elimination bidders, if any, as per GeM rules) through email from GeM after technical evaluation of the bids submitted.
7	**Online Bid Submission Details**	This RFP will follow e-Procurement (e-Tendering) process and the same will be conducted through Government e-Market Place (GeM) portal.
8	**RFP Coordinator**	Ms. S.Krishnaveni, Indian Bank, Chief Manager, HO:Inspection & Audit Department-IS Audit Cell, No. 66, Rajaji Salai, Chennai 600 001.

The RFP document can also be downloaded from: Bank's website: https://www.indianbank.in/tenders and Government e- Market Place (GeM) portal

Further, clarifications, modifications and date of extensions, if any, will be published in the Bank's website and GeM portal only.

Note:

I. Indian Bank, does not take responsibility of any bid/offer damaged/lost in transit/delivered at incorrect address prior to its receipt at the Bank's designated office, wherever applicable.

II. Bank will follow two bidding system. Part-I (Technical Bid) of the bid contains compliance details of the eligibility and terms & conditions set in the RFP document (including annexures) for which proposal/quotation is called for. Bids have to be submitted in **online mode only** through **Government e- Market Place (GeM) portal** along with physical submission of certain documents at designated office as mentioned in Point No. 10 of Schedule [A] (Important Dates and Information on RFP Submission). Further, Bidders must submit their commercial bid as per the format given in the RFP (as per Part-II of Section-V) along with the technical bid on the e-procurement (GeM) portal. The commercial bid submitted on GeM portal at the time of submission of technical bid will be treated as online sealed bid. Subsequently Technical bids submitted by all the bidders will be evaluated and commercial bid of only technically qualified bidders will be opened. Reverse auction will be conducted among the technically qualified bidders after elimination bidders, if any, as per GeM rules.

1. Bidders should enrol/ register themselves on Government e-Market Place (GeM) portal before participating in bidding. All the documents in support of eligibility criteria etc. are also to be scanned and uploaded along with the tender documents. Except as provided in this RFP, any document sent by any other mode will not be accepted.

2. Documents which are to be uploaded online are required to be duly signed by the Authorized Signatory under the seal of the bidder company/ firm in every page. Any correction should be authenticated by the same signatory. If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the bid will be liable for rejection.

3. The price quoted should be unconditional and should not contain any string attached thereto. Bid, which do not confirm to our eligibility criteria and terms & conditions, will be liable for rejection.

III. The RFP document (alongwith addendums, if any) needs to be signed and stamped by the authorised signatory of Bidder and it must be submitted along with the Technical Bid as an evidence of having read and understood the contents of RFP and its addendums (if any).

IV. Time wherever mentioned in this RFP is as per Indian Standard Time. The above dates and timelines are tentative and subject to change without any prior notice or intimation.

This RFP is issued by:

Deputy General Manager,
Indian Bank, HO:Inspection & Audit Department,
No. 66, Rajaji Salai, Chennai 600 001.

SCHEDULE [B] GLOSSARY OF TERMS

i) Following terms are used in the document interchangeably to mean:

1. Bank refers to "Indian Bank (IB)"' including its Branches, Administrative offices, processing centres/HUBS, cells and all other units and establishments etc. (excluding its overseas establishments and Regional Rural Banks).
2. Recipient, Respondent, Consultant, Consultancy firms, Bidder, Applicant means the respondent to the RFP document.
3. RFP means the "Request for Proposal" document.
4. Proposal, Bid means "Response to the RFP Document".
5. Tender means RFP response documents prepared by the Bidder and submitted to "Indian Bank".
6. Selected bidder and the Bank shall be individually referred to as "party" and collectively as "parties". The terms, Successful bidder and the Bank are also referred as Supplier/Service provider/IS Auditor and Purchaser respectively.
7. The term "Bid" & "Quote/ Quotation" bears the same meaning in this RFP.
8. Unless contrary to the context or meaning thereof, Contract or agreement wherever appearing in this RFP shall mean the contract to be executed between the Bank and the successful bidder.
9. Unless the context otherwise requires, reference to one gender includes a reference to the other, words importing the singular include the plural and words denoting natural persons include artificial legal persons and vice versa.

ii) Other Terms and abbreviations**:**

Sl. No.	Terms used in the RFP	Terms and abbreviations
1	GOI	Government of India
2	RBI	Reserve Bank of India
3	IBA	Indian Banks' Association
4	GFR	General Financial Rules
5	POA	Power of Attorney
6	IMPS	Immediate Payment Service
7	NEFT	National Electronic Funds Transfer
8	RTGS	Real Time Gross Settlement
9	CTS	Cheque Truncation System
10	IEM	Independent External Monitor
11	DPIIT	Department for Promotion of Industry and Internal Trade
12	MSE	Micro and Small Enterprises

13	MSME	Micro, Small & Medium Enterprises
14	LLP	Limited Liability Partnership
15	OEM	Original Equipment Manufacturer
16	EMD	Earnest Money Deposit
17	WCS	Weighted Commercial Score
18	WTS	Weighted Technical Score
19	SOW	Scope of Work
20	TCO	Total Cost of Ownership
21	API	Application Programming Interface
22	PBG	Performance Bank Guarantee
23	CASA	Current Account Savings Account
24	ISO	International Organization for Standardization
25	GST	Goods and Services Tax
26	BFSI	Banking, Financial Services and Insurance
27	IS Audit	Information Systems Audit
28	VAPT	Vulnerability Assessment and Penetration Testing
29	ICT	Information and Communication Technology
30	CSCF	Customer Security Controls Framework
31	DC/CDC	Centralised Data Centre
32	DR/NDR	Disaster Recovery / Near Disaster Recovery Centre
33	NIC	National Informatics Centre
34	DFS	Department Financial Services
35	MeitY	Ministry of Electronics and Information Technology

Any term used in this document and not specifically defined herein will have the same meaning as provided in relevant RBI regulations and/ or RBI/IBA guidelines and in case of any dispute the decision of the Bank shall be final and binding.

Confidentiality:

This document is meant for the specific use by the Bidder/s to participate in the current tendering process. This document in its entirety is subject to Copyright Laws. Indian Bank expects the Bidders or any person acting on behalf of the Bidders to strictly adhere to the instructions given in the document and maintain confidentiality of information. ***The Bidder/s do hereby undertake that they shall hold the information received by them under this RFP process or the contract “in trust” and they shall maintain utmost confidentiality of such information. The Bidders have to agree and undertake that (a) They shall maintain and use the information only for the purpose as permitted by the Bank (b) To strictly allow disclosure of such information to its employees, agents and representatives on” need to know” basis only and to ensure confidentiality of such information disclosed to them****. The Bidders will be held responsible for any misuse of information contained in this document or obtained from the Bank during course of RFP process, and liable to be prosecuted by the Bank in the event such breach of confidentiality obligation is brought to the notice of the Bank. By downloading the document, the interested parties are subject to confidentiality clauses.*

SCHEDULE [C] DISCLAIMER

The information in this Request for Proposal (“RFP”) document provided to bidders or applicants whether verbally or in documentary form by or on behalf of Indian Bank, is under the terms and conditions set out in this RFP document and shall also be subject to all other terms and conditions to which such information is generally made available. This RFP document is not an agreement, offer or an invitation by Indian Bank to enter into an agreement/contract in relation to the service but is meant for providing information to the applicants who intend to submit the bids (hereinafter individually and collectively referred to as “Bidder” or “Bidders” respectively). This RFP is designed with the purpose to assist the applicants/ Bidders to formulate their proposal and does not claim to provide all the information that may be required by the applicants/ Bidders.

Each Bidder may conduct its own independent investigation and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP. Indian Bank and its directors, officers, employees, respondents, representatives, agents, and advisors make no representation or warranty and shall incur no liability under any law, statute, rules, or regulations as to the accuracy, reliability or completeness of this RFP. The information contained in the RFP document is selective and is subject to updation, expansion, revision, and amendment. It does not purport to contain all the information that a Bidder may require. Indian Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent.

The Bidders, by accepting this document, agree that any information contained herein may be superseded by any subsequent written information on the same subject made available to the bidders or any of their respective officers/ employees or published in the Bank’s website and/or GeM portal. It is also understood and agreed by the Bidder/s that decision of the Bank regarding selection of the Bidder will be final and binding on all concerned. No correspondence in this regard, verbal or written, will be entertained.

It shall be the duty and responsibility of the Bidders to ensure about their legal, statutory and regulatory eligibility and other competency, capability, expertise requisite for them to participate in this RFP process and to provide all the services and deliverables under the RFP to the Bank.

The applicant shall bear all its costs associated with or relating to the preparation and submission of its proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the Bank or any other costs incurred in connection with or relating to its proposal. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an applicant in preparation or submission of the proposal, regardless of the conduct or outcome of the selection process.

Indian Bank in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Such change will be published on the Bank's Website and GeM Portal and it will become part and parcel of RFP.

Indian Bank reserves the right to reject any or all the bids/proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Indian Bank shall be final, conclusive and binding on all the parties.

SCHEDULE [D] GENERAL INFORMATION

Indian Bank (hereinafter called the “Bank”) is floating Request for Proposal (RFP) for identification of Bidder/s (Service Provider/s) for IS Audit.

Shortlist of Bidders shall be prepared after evaluation of the technical Bids submitted by the bidders participated in this RFP.

Bidders are hereby advised to carefully review and submit all relevant information in the same chronology under the relevant sections only, with their RFP responses.

Details of the objectives, scope of the services, eligibility and qualification criteria, data & documents required (if any) to be submitted along with RFP. Criteria that would be adopted for evaluation of the responses for short listing and other information is contained in the RFP document.

The RFP document can be downloaded from GeM portal or from the Bank’s website www.indianbank.in/tenders.

SCHEDULE [E] OVERVIEW OF INDIAN BANK

Indian Bank, with Corporate Office in Chennai was established as part of the Swadeshi Movement on August 15, 1907.

Along with 13 other banks, the Bank was Nationalized on July 19, 1969. The Bank celebrated its centenary in August 2007. With effect from 1st April 2020, erstwhile Allahabad Bank merged into Indian Bank. The integration of CBS systems of both the banks was completed on 14/02/2021. In the last 117 years, Bank has established a rich legacy by providing quality financial services. It has passed through challenging times, successfully registered turnaround and emerged stronger than before. Given the ever-changing requirements, Bank fine-tuned its strategies and undertook several structural and operational changes and earned a coveted position in the Indian banking industry. Bank's foremost priority has been to serve the people and its nation.

The Bank has been pioneer in developing many digital products and received many awards on digital front.

Bank has been making profit continuously since 2002 and has been self-sustaining in terms of capital adequacy.

VISION:

"Delivering excellence in financial services through customer focus, employee engagement and sustainable growth"

MISSION:

- Bring the best of innovation and technology in our offerings
- Be responsive to the unique needs of every customer through all channels of choice
- To provide value to stake holders
- Empower and engage our employee

As on 31st March 2024, Bank's total Global business reached Rs.12.22 Lakh Cr. consisting of Deposits at Rs.6.88 Lakh Cr. and Advances at Rs.5.34 Lakh Cr.

As on 31st March 2024, Bank has Pan-India network with 22,082 touch points including 5847 Brick & Mortar branches, 4937 ATMs/BNAs, 11,297 Business Correspondents. The Bank has expanded its footprint overseas with branches at Singapore, Colombo and Jaffna, besides a Foreign Currency Banking Unit in Colombo.

Bank had always been a forerunner in offering digital products which provide hassle free, convenient and safe transaction facilities to enhance customer experience, meeting their expectations as the country gears itself for riding on the digital wave. After the amalgamation, the Bank is poised to grow on both business and profitability fronts. The emphasis will be to leverage operational efficiencies, cost synergies and new opportunities in terms of Brand and reach to deliver enhanced customer experience. The focus will be on increasing the CASA share in deposits while looking at diversified growth in credit. Cost optimisation and increasing revenue with focus on fee income, improving recovery and containing NPAs will be levers to improve bottom line.

Technology Environment

Indian Bank has all its branches on Core Banking Solutions, has a range of customer centric and other solutions like full suite of Core Banking Solution, payment systems like IMPS, NEFT, RTGS, SWIFT, CTS, etc., alternate delivery channels viz., ATM, e-Kiosk, Internet Banking, Mobile Banking, e-payment of Taxes, Utility Bill, Ticket, Donation, etc., SMS alerts and Corporate Net Banking. Bank has launched an integrated mobile application having various functionalities with biometric / face id login.

As a part of enhancing customer experience, Bank has also launched an AI-Chatbot ADYA, that is currently available on Bank’s website and Mobile Banking App as an additional interface for answering customer queries and lead generation.

Bank has launched Digital Banking Omni Channel Platform (Mobile Banking/Internet Banking), Digital Lending Platform and Cloud/Containerised Platform.

For further details, please visit Bank’s website www.indianbank.in

SECTION – I

REQUEST FOR PROPOSAL (RFP)

The Bank is interested in selection of IS Auditor for conduct of Comprehensive Cyber Security Audit as advised by Ministry of Finance (MoF) and Ministry of Electronics and Information Technology (MeitY).

Bank will follow two bidding system. Part-I of the bid contains compliance details of the specifications for which quotation is called for. The Bidders should enrol/ register themselves on GeM portal before participating in bidding. **Bids have to be submitted online only through GeM portal**. The Commercial Bid (Part II) will be submitted separately along with the bid document.

Interested eligible bidders may submit their quotation for providing **IS Audit services**, as specified in Part-I as per the following procedure:

1. Bidders should apply through GeM Portal only. All the documents in support of eligibility criteria etc. are also to be scanned and uploaded along with the tender documents. Bid Documents submitted/sent by any other mode will not be accepted.

2. **Part-I** contains compliance details of the specifications for which Bid is called for. No column shall be left blank or altered.

3. **Part-II** – Commercial along with price break up details to be submitted separately along with the bid documentation. After Technical Evaluation, commercial bids of only technically qualified bidders will be opened and reverse auction will be conducted among the technically qualified bidders after elimination of bidders, if any, as per GeM rules. The L1 Bidder will be finalized based upon the price obtained after completion of reverse auction process.

4. Part-I (as per Section-V – Capability and Experience Details) & Part-II (as per Section-V - Commercial bid) to be uploaded online duly signed by the Authorized Signatory under the seal of the bidder in every page. Any correction should be authenticated by the same signatory. If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the quotations will be liable for rejection. The price quoted in the Commercial bid should be unconditional and should not contain any strings attached thereto. The bids which do not conform to our specifications will be liable for rejection and offers with a higher configuration will not attract any special consideration in deciding the vendor.

5. Bank has the right to accept or reject any quotation/cancel the e-tender at its sole discretion, at any point, without assigning any reason thereof. Also, Bank has the discretion for amendment / alteration / extension before the last date of receipt of bid.

6. **MAKE IN INDIA**

This RFP is further governed by Government of India, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion order number P-45021/ 2/2017-B.E.-II dated 15th June 2017 for the Public Procurement (Preference to Make in India), Order 2017, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 28th May 2018, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 29th May 2019, revision order no DPIIT Order No. P-45021/2/2017-PP(BE-II) dated June 04, 2020 and subsequent revision order no. P-45021/2/2017-PP (B.E.-II) dated 16th Sept 2020 & its amendment (if any).

Bank will follow the above orders and guidelines on Public Procurement (Preference to Make in India) and basis of allotment will be done in terms of the same.

7. Bank will also provide benefits to Micro and Small Enterprises (MSEs) as per the guidelines of public procurement policy issued by Government of India. However, the bidder must be the Service provider of the offered Service to avail benefits of MSEs. The bidders to submit the relevant proof of MSE along with declaration for claiming MSE Benefits as per Annexure-III.

8. **RESTRICTION OF BIDDERS FROM COUNTRIES SHARING LAND BORDERS WITH INDIA:**

As per Ministry of Finance, Department of Expenditure, Public Procurement Division's office memorandum F.No.6/18/2019-PPD dated 23.07.2020, regarding insertion of Rule 144 (xi) in the General Financial Rules (GFR) 2017, any bidder from a country which shares a land border with India will be eligible to bid either as a single entity or as a member of a JV / Consortium with others, in any procurement whether of goods, services (including consultancy services and non-consultancy services) or works (including turnkey projects) only if the bidder is registered with the Competent Authority. The Competent Authority for registration will be the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT). Political & Security clearance from the Ministries of External and Home Affairs respectively will be mandatory.

However, above condition shall not apply to bidders from those countries (even if sharing a land border with India) to which the Government of India has extended lines of credit or in which the Government of India is engaged in development projects. Updated lists of countries to which lines of credit have been extended or in which development projects are undertaken are given in the website of the Ministry of External Affairs (MEA).

“The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority”

Definitions pertaining to “Restriction of Bidders from Countries sharing Land Borders with India” Clause Bidder" (including the term 'tenderer', 'consultant' 'vendor' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency, branch or office controlled by such person, participating in a procurement process.

"Bidder from a country which shares a land border with India" means:

a) An entity incorporated, established or registered in such a country; or

b) A subsidiary of an entity incorporated, established or registered in such a country; or

c) An entity substantially controlled through entities incorporated, established or registered in such a country; or

d) An entity whose beneficial owner is situated in such a country; or

e) An Indian (or other) agent of such an entity; or

f) A natural person who is a citizen of such a country; or

g) A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

"Beneficial owner" will be as under:

i. In case of a company or Limited Liability Partnership (LLP), the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has a controlling ownership interest or who exercises control through other means.

   Explanation

   a. "Controlling ownership interest" means ownership of, or entitlement to, more than twenty-five per cent of shares or capital or profits of the company;

   b. "Control" shall include the right to appoint the majority of the directors or to control the management or policy decisions, including by virtue of their shareholding or management rights or share-holders' agreements or voting agreements;

ii. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

iii. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

iv. Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

v. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

"Agent" is a person employed to do any act for another, or to represent another in dealings with third persons.

9. Please note that

(i) The cost of preparing the bids, including visit / visits to the Bank is not reimbursable.

(ii) The Bank is not bound to accept any of the bids submitted and the bank has the right to reject any/all bid/s or cancel the tender at any point without assigning any reason therefor.

(iii) All pages of the Bid document, Clarifications/Amendments, if any, should be signed by the Authorized Signatory under the seal of the bidder company/ firm and to be uploaded with technical bid. A certificate to the effect that the Authorized Signatory has authority to bind the company/ firm should also be attached along with the technical bid.

(iv) The Authority/Bank shall not be liable for any omission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to RFP, Bidding Documents or the Bidding Process, including any error or mistake therein or in any information or data given by the Authority.

(v) Nothing in this RFP shall obligate either Party to enter into any further Agreements.

After technical evaluation, intimation/alert will be given to all qualifying bidders about the date and time of reverse auction for the commercial through GeM portal.

Note: The tender cannot be split.

SECTION-II
INSTRUCTIONS TO BIDDERS

1. Introduction

The Bidder is expected to examine all instructions, forms, terms and specifications given in the Bidding Documents. If any element of doubt arises, the same should be clarified from the Bank in terms of this RFP. Failure to furnish all information required in the Bidding Documents may result in the rejection of its bid and will be at the Bidder's own risk. Bank shall not be responsible for the same.

2. Pre-Bid Meeting

a. A pre-bid meeting is scheduled to be held through physical/Video Conference/ Skype/ Web-ex on ***30/07/2024 at 3.00 pm.*** Bidder's designated representatives (maximum two persons) may attend the pre-bid meeting.

b. The purpose of the meeting will be to clarify the doubts raised by the probable bidders.

c. The Bidder is requested to submit any queries/clarifications to the Bank to the following email id on or before 29/07/2024 01:00 PM**.**

Email id : ***isaudit@indianbank.co.in***

In case the Probable Bidder wants to participate in the Pre-Bid Meeting to be held on the date specified in this bid, they should register themselves with the Bank through email.

3. Replies/clarifications to Pre-Bid Queries

The text of the questions raised (without identifying the source of enquiry) and the responses given, together with amendment to the bid document, if any, will be ported in websites: https://www.indianbank.in and GeM portal and informed vide mail to the bidders who have raised queries.

4. Amendment of bidding documents

1.1 At any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification(s) requested by a prospective Bidder, may modify/ cancel/ extend/ amend the Bidding Document by modification(s) / amendment(s).

1.2 The Bank's replies / clarifications to bidders' queries and amendments if any, will be published in Bank website and in the GeM Portal and will form part of the Bidding document.

1.3 Any bid submitted by a bidder under this RFP process cannot be withdrawn / modified after the last date for submission of the bids unless specifically permitted in writing by the Bank.

5. Technical Bid

The Bidder shall furnish as part of its technical bid, documents establishing the bidder's eligibility to bid and its qualifications to perform the Contract.

The documentary evidence of the Bidder's eligibility to bid and qualifications to perform the Contract if its bid is accepted, shall establish to the Bank's satisfaction that, the Bidder has the financial and technical capability necessary to perform the Contract and that, the Bidder meets the qualification requirements.

Any bid document not accompanied by the above will be rejected.

6. Commercial Bid

1. The Bank will finalize commercials through Online Reverse Auction after evaluation of Part I after giving due notice to the technically qualified bidders.
2. The calling for quote does not confer any right on a bidder for being awarded any purchase order.

7. Clarification of Bids

During evaluation of the bids, the Bank may, at its discretion, seek clarification from the Bidder/s. The request for clarification and the response shall be in writing/ by email, and no change in the substance of the bid shall be sought, offered, or permitted.
The Bidder shall make his/her own interpretation of any and all information provided in the Bidding Document. The Bank shall not be responsible for the accuracy or completeness of such information and/or interpretation. Although certain information is provided in the Bidding Document, bidder shall be responsible for obtaining and verifying all necessary data and information, as required by him. The Bank shall not be bound to accept the lowest tender and reserves the right to accept any or more tenders in part. Decision of Bank in this regard shall be final.

8. Bid Security Declaration

The Bidder shall submit Bid Security Declaration as per the format prescribed in Annexure V confirming that they will not withdraw their bid during the period of bid validity specified in the RFP and they will not fail or refuse to execute the Agreement and furnish the performance security as specified in the RFP.

9. Evaluation Criteria

Bid evaluation methodology that Indian Bank is adopting is detailed hereunder:

9.1 Eligibility Criteria

Bank is looking for CERT-In empanelled auditor other than the auditor who has done the comprehensive audit of the Bank in last 2 years, having resources possessing sufficient domain and technical knowledge in respect of security audit of banking applications including Core Banking and Mobile Banking applications and latest emerging technologies in BFSI Sector like cloud / containerized environment / virtualization / Software Defined Data Network (SDDN), DevOps and automation techniques, etc.

SN	Eligibility Criteria	Proof to be enclosed
1.	The applicant should have been included in the latest panel of Information Systems Auditors maintained by Computer Emergency & Response Team, India [CERT-IN] on the date of submission of Bid with minimum validity upto 31.12.2024	Copies of • Certificate from CERT-IN • Certificate of Incorporation, Certificate of Commencement of Business, Memorandum and Articles of Association and / or Copy of Registered Partnership Deed; • Legal Entity Identifier (LEI) Certificate; • PAN Card AND • GST Certificate • MSE Certificate, if applicable
2.	The applicant should have capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website	Copy of extract from CERT-In website
3.	The applicants or their promoters/ directors/ partners or sister / group concerns ➢ should not be involved in any legal case that may affect the applicant's solvency / existence or in any other way affect the applicant's capability to provide / continue the services to the Bank. ➢ should also not be involved in any litigation / arbitration proceeding. ➢ should not have been involved in any unlawful activity as per the laws of the land. ➢ should not have been blacklisted nor have been technically disqualified on the grounds of non-performance of	Self-Declaration / Certificate of Fair Practices Code in the prescribed format

	contract, by any Government Department / Statutory Body / Regulatory Agency / Public Sector Undertaking / Public Sector Bank / Financial Institution in India. ➢ should not be in the defaulter/barred/caution list published/ displayed at web sites of public/ Autonomous bodies such as RBI/ IBA/ ECGC/SEBI/ICAI, etc.	
4.	Applicant or their subsidiaries/sister concerns ➢ whose Partner/Director is a member of the Bank's Board, ➢ who have undertaken statutory audit of the Bank in the current or previous financial year as on the date of RFP, ➢ who have undertaken / presently undertaking any other assignment of the Bank, which will have potential conflicts of interest with the proposed IS Audit assignment, ➢ who have undertaken / undertaking comprehensive IS Audit / VAPT of the Bank in the last 2 years, shall not be eligible to participate in the RFP.	Self-Declaration in the prescribed format

9.2 General Evaluation Criteria

a) The Bank will examine the bid to determine whether they are complete, whether the documents have been properly signed and whether the bid is generally in order.
b) The bank may waive any minor informality, non-conformity, or irregularity in a bid which does not constitute a material deviation. Material deviation is a substantial deviation which may affect the cost, quantity or quality of the services proposed in the RFP.
c) Prior to the detailed evaluation, the bank will determine the substantial responsiveness of bid documents. For the purposes of these clauses, a substantially responsive quote is one which conforms to all the terms and conditions of the bid documents without material deviations.
d) Bank may seek clarification at the time of evaluation.
e) IS Auditors who have conducted IS audit/VAPT of Indian Bank in the last 2 years will not be considered in line with directions from DFS.

9.3 Technical Evaluation Criteria

Only bids from Bidders meeting the eligibility criteria (as described in the RFP) and submitting complete and responsive bids will proceed to the stage of being fully evaluated and compared.

9.4 Technical Evaluation

The evaluation procedures to be adopted for the bid will be the sole discretion of the Bank and the Bank is not liable to disclose either the criteria or the evaluation report/ reasoning to the bidder(s).

9.5 Commercial evaluation

a) Technical bids submitted by all the bidders will be evaluated and commercial bid of only technically qualified bidders will be opened. Reverse auction will be conducted among the technically qualified bidders after elimination bidders, if any, as per GeM rules.

b) The comparison of prices among the bidders shall be based on the Total Cost of Audit (TCA) quoted covering the entire scope of work as per the Tender documents, inclusive of all applicable taxes and all other cost/charges. Bidder has to quote the Total Cost of Audit (TCA) inclusive of taxes, in the commercial offer as well as at the time of reverse auction.

c) Bidder, whose quote is the least, shall be treated as the successful bidder.

d) The lowest (L1) price arrived at on evaluation of the Commercial Bids or any price lower than the same, as negotiated by the Bank with L1 bidder, will be considered.

e) The finalized prices will be frozen for the period of contract and the Bank, at its discretion may entrust the assignment in full or parts at the same price and terms, as per its requirements.

f) Selection would not amount to any commitment by the Bank to provide any professional assignment during the period of contract. At any one point of time, one or more audit assignment may be entrusted, at the discretion of the Bank, as per its requirement.

9.6 Correction of Error in Commercial Bid:

Bank reserves the right to correct any arithmetical errors furnished in the Commercial Bid. If any such errors are noticed, it will be rectified on the following basis:

(a) Bank may waive off any minor infirmity or non-conformity or irregularity in a bid, which does not constitute a material deviation. Material deviation is a substantial deviation which may affect the cost, quantity or quality of the services proposed in the RFP.

(b) If there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price shall be corrected accordingly.

(c) If there is discrepancy between percentage and amount, the amount calculated on percentage basis will prevail.

(d) If there is discrepancy in the total arrived at (addition, subtraction, multiplication, division and carryover of amount from one page to another), correct total will be arrived by the Bank and the same will prevail over the total furnished by the bidder.

(e) If there is a discrepancy between words and figures, the rate/ amount in words shall prevail, unless the amount expressed in words is related to an arithmetical error in which case, the amount in figures will prevail, subject to the above two provisions.

If the bidder does not accept the correction of errors, the bid will be rejected.

10. Proposal Process Management

Bank reserves the right to

(a) accept or reject any or all proposals received in response to the RFP without assigning any reasons thereof. Bank's decision in this regard will be treated as final. Bids may be accepted or rejected in total or any part or items thereof. No contractual obligation whatsoever shall arise from the RFP process.

(b) reject the bids not submitted in the prescribed format or incomplete in any manner or not containing sufficient information, in the view of the Bank.

(c) verify the validity of bid information and reject any bid where the contents appear to be incorrect, inaccurate or inappropriate at any time during the process of evaluation.

(d) revise the RFP, to request one or more re-submissions or clarifications from one or more Bidders, or to cancel the process in part or whole without assigning any reasons.

(e) alter the requirements, in part or whole, during the RFP process, and without re-issuing the RFP.

(f) modify or relax the eligibility criteria at any time and reserves the right to accept any bid, or to reject a particular bid at its sole discretion without assigning any reason whatsoever.

The evaluation procedures to be adopted for the bid will be the sole discretion of the Bank and the Bank is not liable to disclose either the criteria or the evaluation report / reasoning to the bidder(s).

Bidder/s shall be entirely responsible for its own costs and expenses that are incurred in the RFP process, including presentations, demos and any other meetings.

11. Liabilities of the Bank

This RFP is not an offer by Bank, but an invitation for bidder responses. The calling for quote does not confer any right on the bidder for being awarded any work order.
No contractual obligation on behalf of Bank whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officials of Bank and the bidder.

12. Bid and Proposal Ownership

The Bid submitted and all supporting documentation/ templates are the sole property of Indian Bank and should NOT be redistributed, either in full or in part thereof, without the prior written consent of Bank. Violation of this would be a breach of trust and may, inter-alia cause the Bidder to be irrevocably disqualified. The proposal and all supporting documentation submitted by the Bidder shall become the property of Indian Bank and will not be returned.

13. Bid Pricing Information

By submitting a signed bid, the Bidder certifies that:

(a) The Bidder has arrived at the prices in its bid without agreement with any other bidder of this RFP for the purpose of restricting competition; and

(b) The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP; and

(c) No attempt, to induce any other bidder to submit or not to submit a bid for restricting competition, has occurred.

SECTION – III

Scope of Work

COMPREHENSIVE CYBER SECURITY AUDIT

1. Scope of Comprehensive Audit

Comprehensive Cyber Security Audit should be conducted to cover the Guidelines prescribed by MeitY as detailed hereunder and Audit Report to be submitted as per 282-point audit checklist and 40 point audit summary prescribed by NIC Cyber Security Audit Division. (Annexure X)

1.1 Comprehensive audit should cover the entire application, including the following:

(a) web application (both thick client and thin client);

(b) mobile apps;

(c) APIs (including API whitelisting):

(d) databases;

(e) hosting infrastructure and obsolescence;

(f) cloud hosting platform and network infrastructure; and

(g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

1.2 The scope of the comprehensive audit should include, inter alia, the following:

(a) source code assessment;

(b) application security assessment (both Black Box and Grey Box testing), including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;

(c) network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs);

(d) penetration testing;

(e) network and device configuration review;

(f) application hosting configuration review;

(g) database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication);

(h) user access controls (including privilege access management) and access reconciliation review;

(i) identity and access management controls review;

(j) data protection controls review (Inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches/Data Leaks [CIAD-2021-0004]");

(k) security operations and monitoring review (including maintenance of security logs, correlation and analysis);

(l) review of logs, backup and archival data for access to personal data (including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian Jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); and

(m) review of key management practices (Including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website).

2. Scope of the Limited audit

2.1 Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is

(a) modification in application functionality; or

(b) addition/modification of APIs; or

(c) migration to new infrastructure platform or cloud service; or

(d) change in configuration of application hosting, servers, network components and security devices; or

(e) change in access control policy.

2.2 The scope of limited audit should include, inter alia, the following:

(a) In all cases: Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;

(b) In case limited audit is after six months of comprehensive audit: In addition to (a) above, user access controls (including privilege access management) and access reconciliation review; identity and access management controls review;

(c) In case limited audit is done earlier: In addition to (a) and (b) above,

(i) For audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change configuration of application hosting, servers, network components and security devices: Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets, and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs); network and device configuration review; application hosting configuration review; database security assessment (including whether personal data is being encrypted at rest and in motion, or used tokenised form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorised users and are protected with multi factor authentication); data protection controls review (inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration with security monitoring solutions, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); review logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

(ii) For audit on change in access control policy: Review of logs and integration with security monitoring solutions.

3. Compliance Audit

Audit to be followed by compliance audit on monthly basis for Comprehensive Audit as well as Limited Audit to verify and confirm the compliance status reported by the Bank. The non-compliances to be reported with respective remarks from the Bank, Auditor’s comments with reasons for disagreements, if any and PoCs. On full compliance, Final Certification to be submitted.

4. Deliverables

a) The IS Auditor will nominate a Project Manager immediately on acceptance of the order, who will be the single point of contact for the Project. Additionally, escalation contact details to be submitted to the Bank.

b) The Auditor has to undertake IS Audit in a phased manner as described below:
   - (i) Conduct of IS Audit as per scope & submission of preliminary reports of IS Audit findings and discussion on the findings.
   - (ii) Submission of final reports in a format acceptable to the Bank for regulatory compliance.
   - (iii) Limited Audit after 6 months of the comprehensive audit.
   - (iv) Compliance review & certification.

c) IS Audit / VAPT to be scheduled and conducted in such a way that there is no business downtime.

d) Only licensed tools have to be utilized and each audit report shall include the details of tools utilized, version of the tools, license, etc. along with a declaration / confirmation that the tools used
   - are free from any malicious code & malwares,
   - are updated with latest patches released by the OEM and
   - are updated with the latest vulnerabilities notified by Market Intelligence sources.

e) The checklists updated and evidences/PoCs collected during the audit process are to be shared with Bank's Inspection Department for their reference and for submission to Regulatory Authorities, as and when required.

f) Dedicated Single Point of Contact (SPOC) to be available (both onsite / offsite) during the entire contract period for conduct of audit and to clarify on compliance issues / to guide the Bank for closure of vulnerabilities.

5. Indicative size of the proposed Audit coverage

SN	Description	Approx. Count
1.	Internal Applications	100
2.	Public facing web and mobile applications	130
3.	Servers	1000
4.	Databases	50
5.	Network and SOC devices	400
6.	Application Programming Interfaces (Public facing)	250
7.	Application Programming Interfaces (Internal)	350
8.	Cloud / Containerized Platform	20

Note :

The above is an indicative list of infrastructure available with the Bank. Actual count may vary later on. Details and other specifications will be provided at the time of commencement of respective audit.

CONDITIONS OF CONTRACT

1) Period of Validity of Bids

Bids should remain valid for the period of 90 days after the last date for submission of bid prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as non-responsive. Bank may seek extension of bid validity period, if required.

2) Authorization to Bid

Responses submitted by a Bidder to this RFP (including response to capability and experience details and commercial bid) represent a firm offer to contract on the terms and conditions described in the tender document. The proposal must be signed by an official authorized to commit the bidder to the terms and conditions of the proposal. Bidder must clearly identify the full title and authorization of the designated official and provide a statement of bid commitment with the accompanying signature of the official and submit the copy of power of attorney/ authority letter authorizing the signatory to sign the bid.

3) Payment Terms

Payments for the job of Information System Auditor will be milestone payments as under:

SN	Audit Activity	% of fee payable as per price schedule in commercial bid
1.	Submission of Final Cyber Security Audit Reports in a format acceptable to the Bank and Regulatory Authorities	100% of the rate quoted for Comprehensive Cyber Security Audit
2.	Submission of Limited Audit Report in a format acceptable to the Bank and Regulatory Authorities	100% of the rate quoted for Limited Audit
3.	Submission of Compliance Audit Reports on monthly basis for Comprehensive Audit for first 6 months	50% of the rate quoted for Compliance Audit
4.	Submission of Compliance Audit Reports on monthly basis, for remaining period of contract, for Comprehensive Audit as well as Limited Audit & Final Certification on full compliance	50% of the rate quoted for Compliance Audit

4) Change Orders

The Bank may at any time, by a written order given to the bidder, make changes within the general scope of the Contract in any one or more of the following:

a. the place of delivery; and / or

b. the items to be supplied/ Services to be provided by the Supplier;

If any such change causes substantial increase or decrease in the cost of, or the time required for, the Bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule, or both, and the Contract shall accordingly be amended. Any claim by the bidder for adjustment under this clause must be asserted within thirty (30) days from the date of the bidder's receipt of the Bank's change order.

5) Service Level Agreement (SLA)

Within 15 (fifteen) days from the date of Work Order, the successful bidder shall sign the Service Level Agreement, as required in RFP and return it to the Bank.

6) Human Resource Requirements

As and when any assignment is entrusted, successful bidder shall ensure that the Security Audit and IS Audit work is got done by qualified Professionals having requisite expertise.

7) Contract Period

The proposed contract will be for a period of 15 months from the date of execution of contract.

8) Sub-Contracting

The successful bidder will not subcontract or delegate or permit anyone other than the bidders' personnel to perform any of the work, service or other performance required of the supplier under this agreement without the prior written consent of the Bank. Bank at its own discretion may permit or deny the same.

9) Insurance

The successful bidder may be required to take adequate insurance cover against all kinds of risks including fidelity clause for the loss arising from acts of omission/ commission/ dishonesty of its employees and / or agents and would be required to keep the insurance policy alive at all times during the currency of the agreement. Bidder should have cyber insurance policy to cover first party and third-party liability coverage to organisation when cyber risk materializes and / or cyber security controls at organization fails. The coverages established by the cyber insurance shall cover property, theft and network level security.

10) Jurisdiction and Applicable Law

The Contract shall be interpreted in accordance with the laws of India. Any dispute arising out of this contract will be under the jurisdiction of Courts of Law in Chennai. Compliance with labour and tax laws, etc. will be the sole responsibility of the service provider at their cost.

11) Liquidated Damages (LD) and Penalty

- The liquidated damages will be an estimate of the loss or damage that the bank may have suffered due to delay in performance of the obligations by the Service Provider under the terms and conditions of the contract and its amendments and the Service Provider shall be liable to pay the Bank as liquidated damages at the rate of 0.5% of the contract price for delay of every week or part thereof. Once the penalty crosses 10% of the contract price, the Bank reserves the right to cancel the contract or take any other suitable penal action as deemed fit.
- Without any prejudice to the Bank's other rights under the law, the Bank shall recover the liquidate damages, if any, accruing to the Bank, as above, from any amount payable to the Service Provider either as per the Contract, executed between the Bank and the Service Provider pursuant hereto or under any other Agreement/Contract, the Bank may have executed/shall be executing with the Service Providers.

12) Bank’s right to accept or reject any bid or all bids

- The Bank reserves the right to accept or reject any bid / all bids or annul the bidding process at any time prior to awarding the contract, without thereby incurring any liability to the affected Bidder or Bidders.
- Bank reserves the right to modify the terms and conditions of this RFP duly informing the same before due date of submission of bids & publishing the same on Bank Website and GeM portal.

13) Performance Security

a. Within 15 days of issue of Work Order, the successful bidder shall furnish to the Bank the Performance Security equivalent to 5% of the contract value in the form of a Bank Guarantee from a scheduled commercial Bank located in India, valid for 18 months (period of contract + 3 months) with further one month of claim period, in the format enclosed (Annexure-IX). Relaxation if any, extended by GOI/ competent authorities for furnishing PBG shall be passed on to eligible bidders.

b. The performance security submitted by the successful bidder shall be invoked by the Bank as compensation for any loss resulting from the bidder’s failure in completing their obligations or any other claim under the Contract.

c. In case of delay in the execution of assignment entrusted, Bank will seek extension of the Performance bank guarantee.

d. The performance security will be discharged by the Bank and returned to the successful bidder not later than thirty (30) days following the date of completion of the successful performance obligations under the Contract.

e. Failure of the successful bidder to comply with the requirement of signing of contract and providing performance security shall constitute sufficient grounds for annulment of the award, in which event the Bank may call for new bids or offer the contract to L-2 bidder.

14) Limitation of Liability

Successful bidders' aggregate liability under the contract shall be at actual and limited to a maximum of the contract value. For this purpose, contract value at any given point of time, means the aggregate value of the work orders placed by bank on the vendor that gave rise to claim, under this tender.

This limit shall not apply to third party claims for

a. IP Infringement indemnity
b. Bodily injury (including death) and damage to real property and tangible property caused by vendor' or its employee/ agents.

If a third party asserts a claim against bank that a vendor product acquired under the agreement infringes a patent or copy right, vendor should defend the bank against that claim and pay amounts finally awarded by a court against bank or included in a settlement approved by vendor**.**

15) Indemnity Clause

If at the time of the supplying the goods or services or installing the platform/ software in terms of the present contract/ order or subsequently it appears at any point of time that an infringement has occurred of any right claimed by any third party in India or abroad, then in respect of all costs, charges, expenses, losses and other damages, which the Bank may suffer on account of such claim, the supplier shall indemnify the Bank and keep it indemnified on that behalf.

16) Disclaimer

The Bank and/or its officers, employees disown all liabilities or claims arising out of any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of Bank and/or any of its officers, employees.

This RFP is not an agreement by the Authority to the prospective Bidders or any other person. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

The information contained in this RFP document, or any information provided subsequently to Bidder(s) whether verbally or in documentary form by or on behalf of the Bank, is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the Bidder(s) with information to assist in the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary, obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP.

17) Patent Rights

The Supplier shall indemnify the Bank against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods or software or hardware or any part thereof. In the event of any claim asserted by the third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the Goods or any part thereof, the bidder shall act expeditiously to extinguish such claims. If the bidder fails to comply and Bank is required to pay compensation to a third party resulting from such infringement, the bidder shall be responsible for the compensation including all expenses, court costs and lawyer fees. Bank will give notice to the bidder of such claims, if it is made, without delay by fax/e-mail/registered post.

18) Regulatory Requirements

The services to be quoted as per this tender should comply with the requirements under Information Technology (IT) Act 2000 and subsequent amendments and related Government/Reserve Bank India/other Regulatory Authorities' guidelines issued from time to time.

19) Intellectual Property Rights (IPR)

While the successful bidder / OEM shall retain the intellectual property rights for the application software, it is required that successful bidder shall grant user-based annual subscription License to the bank for the bank's exclusive use without limitation on the use of those licenses. The successful bidder shall place the source code of customizations done for the bank in Banks environment (and the procedures necessary to build the source code into executable form) for the application software, and the source code of the application software in escrow with a reputable agency (a bank or established software escrow firm in India) acceptable to the Bank during the contract period.

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No License under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

Bidder warrants that the inputs provided and/or deliverables supplied by them does not and shall not infringe upon any third-party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever.

In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, bidder shall at its choice and expense: [a] procure for Bank the right to continue to use such deliverables; [b] replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables; or [c] if the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse the bank for any amounts paid to bidder for such deliverables, along with the replacement costs incurred by Bank for procuring an equivalent equipment in addition to the penalties levied by Bank. However, Bank shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, the bidder shall be responsible for payment of penalties in case service levels are not met because of inability of the bank to use the proposed product.

The indemnification obligation stated in this clause apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby.

The bidder acknowledges that business logics, workflows, delegation and decision-making processes of Bank are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors.

20) Acceptance of Work Order

Acceptance of work order should be submitted within 4 (four) days of issuance of work order, along with authorization letter by the successful bidder to the Bank. If for any reason L1 bidder backs out after issuance of work order or the work order issued to the L1 bidder does not get executed in part / full, Bank shall blacklist the bidder for a period of one year.

21) Signing of Contract Form and NDA and SLA

Within 15 (fifteen) days of issuance of Work Order, the successful bidder shall sign the contract form (Annexure-VII), Non-Disclosure Agreement (Annexure-VIII) and Service Level Agreement (Annexure-IX) and return it to the Bank.

Background check conducted, KYC details for the resources provided for the project to be submitted to the Bank.

22) Settlement of Disputes

a. If any dispute or difference of any kind whatsoever shall arise between the Bank and the service provider in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

b. If the parties fail to resolve their disputes or difference by such mutual consultation **within a period of 30 days**, then either the Bank or the supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the goods under the contract. Arbitration proceedings shall be conducted in accordance with the following rules of procedure.

The dispute resolution mechanism to be applied shall be as follows:

a) In case of dispute or difference arising between the Bank and the Service Provider relating to any matter arising out of or connected with the agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators one each to be appointed by the Bank and the Service Provider; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator. In case of failure of the two arbitrators appointed by the parties to reach upon a consensus within a period of 30 days from the appointment of the presiding Arbitrator, the Presiding Arbitrator shall be appointed by the Indian Banks' Association, India which shall be final and binding on the parties.

b) If one of the parties fails to appoint its arbitrator within 30 days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Indian Banks' Association shall appoint the Arbitrator. A certified copy of the order of the Indian Banks' Association making such an appointment shall be furnished to each of the parties.

c) Arbitration proceedings shall be held at Chennai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.

d) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.

e) Where the value of the contract is Rs. 10 million and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator shall be appointed by agreement between the parties; failing such agreement, by the appointing authority namely the Indian Banks' Association (IBA).

f) Notwithstanding any reference to arbitration herein,

a. the parties shall continue to perform their respective obligation under the contract unless they otherwise agree; and

b. the Bank shall pay the supplier any monies due to the supplier.

Submitting to arbitration may be considered as an additional remedy and it does not preclude Parties to seek redressal / other legal recourse.

23) Coverage of Successful Bidder under the Employees' Provident Funds and Miscellaneous Provisions Act, 1952

The Successful bidder has to submit necessary details of all the outsourced employees for any type of services engaged either through contractors or directly whenever required by the Bank. If engaged through contractors, list of all the contractors engaged for any/all services and whether the said contractors are covered independently under the EPF & MP Act 1952 is to be submitted on the Bank's request. The agreement of contracts with the contractors, the PF code number of the contractors, if covered, the attendance of the contract employees, the remitted PF challan with the Electronic Challan cum Return (ECR) should be submitted on the Bank's request.

24) Exit Requirements

In the event, the Agreement between the Bank and the Successful bidder comes to an end on account of termination or by the expiry of the term / renewed term or otherwise, the Supplier shall render all reasonable assistance and help to the Bank and to any new vendor engaged by the Bank, for the smooth switch over and continuity of the Services.

25) Termination for Convenience

The Bank, by 90 days' written notice sent to the Successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the bank's convenience, the extent to which the performance of the Successful bidder under the Contract is terminated, and the date upon which such termination becomes effective.

The assignments that are complete before the Service Provider's receipt of notice of termination shall be accepted by the Bank at the Contract terms and prices. For the remaining services, the Bank may elect:

a. to have any portion completed and delivered at the Contract terms and prices; and / or

b. to cancel the remainder and pay to the Service Provider an agreed amount for partially completed assignments.

26) Termination for Default

The Bank, without prejudice to any other remedy for breach of contract, by 90 days' written notice of default sent to the Supplier, may terminate this Contract in whole or in part:

a. if the successful bidder fails to deliver any or all of the Goods and Services within the period(s) specified in the Contract, or within any extension thereof granted by the Purchaser;

b. if the successful bidder fails to perform any other obligation(s) under the Contract.

c. If the successful bidder, in the judgement of the Purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

d. In case of successful Bidders revoking or cancelling their Bid or varying any of the terms in regard thereof without the consent of the Bank in writing.

'For the purpose of this clause:

"corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution; and

"**fraudulent practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Bank and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

In the event the Bank terminates the Contract in whole or in part, the Bank may procure the Goods or Services similar to those undelivered, upon such terms and in such manner as it deems appropriate, and the Supplier shall be liable to the Bank for any excess costs paid/ to be paid by the Bank for such similar Goods or Services. However, the Supplier shall continue performance of the Contract to the extent not terminated.

27) Force Majeure

The Successful bidder shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure. For purposes of this clause, “Force Majeure” means an event beyond reasonable control of the Successful bidder and not involving the Successful bidder’s fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes. Delay by sub suppliers of vendor to Vendor will not be considered as cause of force Majeure.

If a Force Majeure situation arises, the Successful bidder shall promptly notify the Bank in writing of such condition and the cause thereof but in any case, not later than 10 (Ten) days from the moment of their beginning. Unless otherwise directed by the Bank in writing, the Successful bidder shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

If the impossibility of complete or partial performance of an obligation lasts for more than 6 (six) months, either party hereto reserves the right to terminate the contract totally or partially upon giving prior written notice of 30 (thirty) days to the other party of the intention to terminate without any liability other than reimbursement on the terms provided in the agreement for the services received or complete transition / handover to the in-coming Vendor / Service Provider**.**

28) Confidentiality

The supplier will be exposed to internal business information of the Bank, affiliates, and / or business partners by virtue of the contracted activities. The Bidder / their employees shall treat all data & information collected from the Bank during the project in strict confidence. The Bank is expected to do the same in respect of Bidder provided data / information. ***After termination of the contract also the successful bidder / supplier shall not divulge any data/ information collected from the Bank during the project.***

The supplier will have to enter into a Non-Disclosure agreement (Annexure-XII) with the Bank to safeguard the confidentiality of the Bank’s business information, legacy applications and data.

The successful bidder and its employees either during the term or after the expiration of the contract shall not disclose any proprietary or confidential information relating to the project, the services, the contract, or the business or operations without the prior written consent of the Bank.

The successful Bidder and its employees shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location. The successful Bidder shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank data and sensitive application software. The successful Bidder shall also ensure that all permitted subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location.

The successful bidder will be permitted to retain all information and documents as may be required for legal purposes, provided that such retained information remains subject to confidentiality obligations for the entire retention period.

29) Negligence

If the successful bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given in writing by the Bank in connection with the work or contravenes the provisions of other Terms, in such eventuality, the Bank may after giving notice in writing to the successful bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the successful bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the successful bidder.

30) Amalgamation

If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the obligations of the successful bidder under this RFP. In such case, decision of the new entity will be binding on the successful bidder.

31) Inspections and Tests

The Bank or its representative(s), RBI or any of the Statutory bodies, shall have the right to visit and /or inspect any of the Bidder’s premises to ensure that services provided to the Bank is secured. The Bank shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

Any charges payable to the Purchaser's representative designated for inspection shall be borne by the Purchaser.

Should any inspected or tested services fail to conform to the requirements, the Bank may reject the services, and the Service Provider shall undertake the services again to meet specification requirements at no additional cost to the Bank.

The Bank's right to inspect, test and, where necessary, reject the services after the delivery shall in no way be limited or waived by reason of the services having previously been inspected, tested and passed by the Bank.

The supplier shall provide unrestricted access to its premises and records being maintained with regard to the job being performed as per its contract with the Bank, to the authorized personnel of the Bank/ its auditors (internal and external)/ any statutory/ regulatory authority/ authorized personnel from RBI to carry out any kind of process of audit including that of its operations and records related to services provided to the Bank, in the presence of representatives of the supplier, at any point of time giving advance notice. RBI or persons authorized by it shall access the records of Bank and the supplier related to this agreement and cause inspection.

32) Use of Contract Documents and Information

The successful bidder shall not, without the Purchaser’s prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Purchaser in connection therewith, to any person other than a person employed/authorized by the successful bidder in the performance of the Contract. Disclosure to any such employed/authorized person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

The successful bidder shall not, without the Purchaser’s prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.

33) Delivery Schedule

SN	Audit Activity	Timeline
1.	Conduct of Comprehensive Cyber Security Audit as per scope & submission of preliminary reports of IS Audit findings and discussion on the findings	To be completed within 1 months of execution of contract
2.	Submission of final reports in a format acceptable to the Bank for regulatory compliance	To be completed within 2 months of execution of contract
3.	Conduct of Limited Review and submission of preliminary / final report	To be commenced after 6 months of final audit report and to be completed within 1 month.
4.	Conduct of Compliance review & submission of Certification for Compliance	To be conducted by 10th of each calendar month for 12 months following the month of Final Comprehensive Report or till compliance of all the observations of Final Report and Limited Review Report, whichever is earlier.

34) Working Days

Bank's Working Days will be considered as Working Days for the purpose of this contract. However, wherever required, IS Audit / VAPT to be scheduled and conducted in such a way that there is minimum disturbance to business.

35) Implementation of Services

The successful bidder shall provide all the services specified hereunder in accordance with the highest standards of professional competence and integrity. If the Bank finds that any of the staff of the successful bidder assigned to work at the Bank's site is not responsive, then the successful bidder will be notified accordingly and the successful bidder shall be under obligation to resolve the issue expeditiously to the satisfaction of the Bank.

36) Termination for Insolvency

If the successful bidder becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the successful bidder is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over in part of its undertaking or assets, or if the successful bidder takes or suffers any other analogous action in consequence of a debt; then the Bank may at any time terminate the contract by giving a notice to the successful bidder.

If the contract is terminated by the Bank in terms of this clause, termination will be without compensation to the successful bidder provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Bank.

In case the termination occurs before implementation of the project/ delivery of services in full, in terms of this clause, the Bank is entitled to make its claim to the extent of the amount already paid by the Bank to the successful bidder.

37) Taxes and Duties

The successful bidder shall be liable to pay all taxes that shall be levied against it, in accordance with the laws applicable from time to time in India.

38) Compliance with Policy

The successful bidder shall have to comply with Indian Bank's policies like IT policy, Information Security policy, Cyber Security Policy, Digital Personal Data Protection Policy etc. in key concern areas relevant to the RFP, details of which shall be shared with the successful bidder.

39) Other Terms and Conditions

- The relationship between the Bank and Successful Bidder/s is on principal-to-principal basis. Nothing contained herein shall be deemed to create any association, partnership, joint venture or relationship or principal and agent or master and servant or employer and employee between the Bank and Successful Bidder/s hereto or any affiliates or subsidiaries thereof or to provide any party with the right, power or authority, whether express or implied to create any such duty or obligation on behalf of the other party.

- Successful bidder/Service Provider shall be the principal employer of the employees, agents, contractors, subcontractors etc., engaged by the successful bidder/Service Provider and shall be vicariously liable for all the acts, deeds, matters or things, of such persons whether the same is within the scope of power or outside the scope of power, vested under the contract. No right of any employment in the Bank shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc., by the successful bidder/Service Provider, for any assignment under the contract. All remuneration, claims, wages dues etc., of such employees, agents, contractors, subcontractors etc., of the successful bidder/Service Provider shall be paid by the successful bidder/Service Provider alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the successful bidder’s/Service Provider’s employees, agents, contractors, subcontractors etc. The Successful Bidder/Service Provider shall agree to hold the Bank, its successors, assigns and administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the Bank through the action of Successful Bidder/Service Provider’s employees, agents, contractors, subcontractors etc.

40) GENERAL TERMS AND CONDITIONS

40.1 Rejection of Bids

The Bank reserves the right to reject the Bid if,

i. Bidder does not meet any of the pre-bid eligibility criteria mentioned above including non-payment of the bid cost.

ii. The bid is incomplete as per the RFP requirements.

iii. Any condition stated by the bidder is not acceptable to the Bank.

iv. If the RFP and any of the terms and conditions stipulated in the document are not accepted by the authorized representatives of the bidder.

v. Required information not submitted as per the format given.

vi. Any information submitted by the bidder is found to be untrue/fake/false.

vii. The bidder does not provide, within the time specified by the bank, the supplemental information / clarification sought by the bank for evaluation of bid.

The Bank shall be under no obligation to accept any offer received in response to this RFP and shall be entitled to reject any or all offers without assigning any reason whatsoever. The Bank may abort entire process at any stage without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for Bank's action.

In order to promote consistency among the Proposals and to minimize potential misunderstandings regarding how Proposals will be interpreted by the Bank, the format in which Bidders will specify the fundamental aspects of their Proposals has been broadly outlined in this RFP.

Any clarifications to the RFP should be sought by email as per the dates mentioned in **"Schedule [A] Important Dates"**. Bank will hold a pre-bid meeting, to answer all the questions / queries received by email which would also be uploaded on bank's website and GeM portal.

Proposals received by the Bank after the specified time and date shall not be eligible for consideration and shall be summarily rejected.

In case of any change in timeline, the same shall be updated on the Bank's website and shall be applicable uniformly to all bidders.

40.2 Representation and Warranties

The Bidder represents and warrants as of the date hereof, which representations and warranties shall survive the term and termination hereof, the following:

i. That the representations made by the Bidder in its Bid are and shall continue to remain true and fulfil all the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the RFP and unless the Bank specifies to the contrary, the Bidder shall be bound by all the terms of the RFP.

ii. That all the representations and warranties as have been made by the Bidder with respect to its Bid and Contract, are true and correct, and shall continue to remain true and correct through the term of this Contract.

iii. That the execution of the Services herein is and shall be in accordance and in compliance with all applicable laws.

iv. That there are –

(a) no legal proceedings pending or threatened against Bidder or any sub Bidder/third party or its team which adversely affect/may affect performance under this Contract; and

(b) no inquiries or investigations have been threatened, commenced or pending against Bidder or any sub-Bidder / third part or its team members by any statutory or regulatory or investigative agencies.

v. That the Bidder is validly constituted and has the corporate power to execute, deliver and perform the terms and provisions of this Contract and has taken all necessary corporate action to authorize the execution, delivery and performance by it of the Contract.

vi. That all conditions precedent under the Contract has been complied by the bidder.

vii. That neither the execution and delivery by the Bidder of the Contract nor the Bidder's compliance with or performance of the terms and provisions of the Contract:

a) will contravene, any provision of any applicable law or any order, writ, injunction or decree of any court or government authority binding on the Bidder,
b) will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Bidder is a Party or by which it or any of its property or assets is bound or to which it may be subject, or
c) Will violate any provision of the Memorandum or Articles of Association of the Bidder.

viii. That the Bidder certifies that all registrations, recordings, filings and notarizations of the bid documents/ agreements/ contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the Bidder which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been/ shall be made.

ix. That the Bidder confirms that there has not and shall not occur any execution, amendment or modification of any agreement/contract without the prior written consent of the Bank, which may directly or indirectly have a bearing on the Contract or the project.

x. That the Bidder owns or has good, legal or beneficial title, or other interest inthe property, assets and revenues of the Bidder on which it grants or purports to grant or create any interest pursuant to the Contract, in each case free and clear of any encumbrance and further confirms that such interests created or expressed to be created are valid and enforceable.

xi. That the Bidder owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all Intellectual Property Rights, which are required or desirable for the project and the Bidder does not, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. None of the Intellectual Property or Intellectual Property Rights owned or enjoyed by the Bidder or which the Bidder is licensed to use, which are material in the context of the Bidder's business and operations are being infringed nor, so far as the Bidder is aware, is there any infringement or threatened infringement of those Intellectual Property or Intellectual Property Rights licensed or provided to the Bidder by any person. All Intellectual Property Rights (owned by the Bidder or which the Bidder is licensed to use) are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required by the bidder to maintain the same in full force and effect have been taken thereon and shall keep the Bank indemnified in relation thereto.

xii. Any intellectual property arising during the course of the execution under the contract related to tools/ systems/ product/ process, developed with the consultation of the bidder will be intellectual property of the Bank.

40.3 Relationship of Parties

i. Nothing in the Contract shall constitute any fiduciary relationship between the Bank and Bidder/Bidder's Team or any relationship of employer – employee, principal and agent, or partnership, between Indian Bank and Bidder and /or its employees.

ii. No Party has any authority to bind the other Party in any manner whatsoever, except as agreed under the terms of the Contract.

iii. Indian Bank has no obligation to the successful Bidder, except as agreed under the terms of the Contract.

iv. All employees/personnel/ representatives/agents etc., engaged by the Successful Bidder for performing its obligations under the Contract/RFP shall be in sole employment of the Successful Bidder and the Successful Bidder shall be solely responsible for their salaries, wages, statutory payments etc. Under no circumstances, shall Indian Bank be liable for any payment or claim or compensation (including but not limited to any compensation on account of any injury / death / termination) of any nature to the employees/personnel/representatives/agent etc. of the Successful Bidder.

v. The Successful Bidder shall disclose to Indian Bank in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Successful Bidder or its team/agents/representatives/personnel etc.) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

vi. The Successful Bidder shall not make or permit to be made a public announcement or media release about any aspect of the Bid/ Contract unless Indian Bank first gives the Successful Bidder its prior written consent.

40.4 No Right to Set Off

In case the Successful Bidder has any other business relationship with the Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available under the agreement to the said Bidder for any payments receivable under and in accordance with that business.

40.5 Publicity

Any publicity by the Bidder in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

40.6 Conflict of Interest

The Bidder shall disclose to the Bank in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder's team) in the course of performing the services / appointment as soon as practical after it becomes aware of that conflict.

40.7 Solicitation of Employees

The selected Bidder, during the term of the contract shall not without the express written consent of the Bank, directly or indirectly:
a) recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services in relation to the contract; or
b) induce any person who shall have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.

40.8 Notices and Other Communication

If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be sent personally or by certified or registered post with acknowledgement due or overnight courier or email duly transmitted, addressed to the other party at the addresses, email given in the contract.

Notices shall be deemed given upon receipt, except that notices sent by registered post in a correctly addressed envelope shall be deemed to be delivered within 5 working days (excluding Sundays and public holidays) after the date of mailing dispatch and in case the communication is made by email, on business date immediately after the date of successful email (that is, the sender has a hard copy of the page evidencing that the email sent to correct email address).

Any Party may change the address, email address and fax number to which notices are to be sent to it, by providing written notice to the other Party in one of the manners provided in this section.

40.9 Substitution of Team Members

The BID should also contain resource planning proposed to be deployed for the project which includes inter-alia, the number of personnel, skill profile of each personnel, duration of employment etc.

During the assignment, the substitution of key staff identified for the assignment shall not be allowed unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the Bidder can do so only with the concurrence of the Bank by providing alternate staff of same level of qualifications and expertise. If the Bank is not satisfied with the substitution, the Bank reserves the right to terminate the contract and recover whatever payments has been made by the Bank to the Bidder during the course of this assignment besides claiming an amount, equal to 10% of the contract value as liquidated damages. The Bank reserves the right to insist the Bidder to replace any team member with another (with the qualifications and expertise as required by the Bank) during the course of assignment. The Bidder will have to undertake that no such substitution would delay the project timelines.

40.10 Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this RFP shall not be affected or impaired.

SECTION - IV

INSTRUCTIONS TO BIDDERS FOR ONLINE TENDER THROUGH GeM PORTAL

1.1. SUBMISSION OF BIDS THROUGH GeM PORTAL

The Bid documents, to be uploaded as part of online bid submission, are as follows:

a. Eligibility Criteria, along with all supporting documents required.

b. All Annexures as per this tender on Bidder's letter head with authorizing person's signature and Bidder seal on all pages.

c. All supporting documents in support of Capability and Experience Details.

d. Relevant brochures

f. Compliance to Capability and Experience as per Technical Bid.

g. Any other information sought by the Bank with relevant to this tender.

*(*Please refer checklist under Annexure of this tender for more details)*

Bidder should upload all the copies of relevant documents without fail in support of their bid and as per the instructions given in tender documents. If the files to be uploaded are in PDF format, ensure to upload it in "Searchable" PDF Format. After filling data in predefined forms bidders need to click on final submission link to submit their encrypted bid.

Please take care to scan documents so that total size of documents to be uploaded remains minimum. Unless specified in this RFP, **every document submitted online to the Bank shall be in PDF Format. The Scanned Documents shall be OCR enabled for facilitating "search" on the scanned document.** Utmost care may be taken to name the files/documents to be uploaded on e-tendering portal.

1.2. BID RELATED INFORMATION

Bidders must ensure that all documents uploaded on e-tendering portal as files or zipped folders, contain valid files and are not corrupt or damaged due to any processing at bidder PC system like zipping etc. It shall be the responsibility of bidder themselves for proper extractability of uploaded zipped files.

Any error/virus creeping into files/folder from client end PC system cannot be monitored by e-tender software/server and will be bidder's responsibility only.

1.3. OTHER INSTRUCTIONS

For further instructions like system requirements and manuals, the bidder should visit GeM portal or banks Website.

SECTION-V

PART I – Capability and Experience Details

Date:

The Deputy General Manager
Indian Bank
Head Office, I floor,
Inspection & Audit Department,
No.66 Rajaji Salai, Chennai – 600001

Dear Sirs,

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: Your RFP No. GEM/2024/B/5198605 dated 24/07/2024

******

Referring to your above RFP, we submit the compliance details of the specifications given below:

S. No	**Details**	
1.	Name of the Audit Organization	
2.	Registered Office / Head Office	
3.	Constitution	
4.	Year of Incorporation	
5.	Date of empanelment with CERT-In with expiry date	

6.	Partner/Director Details					
SN	**Name**	**Address**	**Professional Qualification**	**Validity of Certification**	**Experience in brief**	**Role in IS Audit (Task / Module)**

7.	Employee Details					
SN	**Name**	**Designation**	**Professional Qualification**	**Validity of Certification**	**Years of IS Audit experience**	**Role in IS Audit (Task / Module)**

8.	Experience Details							
S.No.	**Name & Address of Organization for whom services rendered**	**Nature of Work**	**Date of Work Order**	**Project Details**				**Contact details for reference**
				Period (No. of Months)	**Start Date**	**Date of Completion/ expected completion**	**Team size**	

9.	Financial Details for last 3 years			
Financial Year (Apr-Mar)	***Turnover***	***Turnover from IS Audit activities***	***Net Profit or Loss***	***Net worth***
2023-24				
2022-23				
2021-22				

We confirm that we are empanelled with CERT-In since ______ and the validity of the empanelment is ________________. We undertake to submit the Certificate of Renewal from CERT-IN immediately after the expiry of validity. We understand that Bank may terminate the contract in case our Organization ceases to be on CERT-IN Empanelled list or fail to submit documentary evidence for renewal of empanelment within 3 months of expiry.

We confirm that we have permanent office in Chennai at ________and/or permanent officials in Chennai at _________,

We also confirm that our Audit Organization is having the capability and willingness to deploy competent resources to carry out assignments entrusted by the Bank in Chennai, Mumbai and / or any other location, as specified by the Bank, at short notice and to ensure timely completion of the assignments, at our cost.

We confirm that dedicated Single Point of Contact (SPOC) will be available (both onsite / offsite) during the entire contract period for conduct of audit and to clarify on compliance issues / to guide the Bank for closure of vulnerabilities.

We comply with all requirements, specifications, terms and conditions mentioned in the Bid Document and are submitting proof of the same along with bid.

We agree for the time frame for completion of activities as per your above bid.

We agree to the terms of payment mentioned in your bid.

We submit that we shall abide by your terms and conditions governing the quotation.

We submit that the details given above are true to the best of our knowledge.

For

Office Seal
Place:
Date:

(Authorised Signatory)
Name:
Designation:
Mobile No:
Business Address:

Telephone No:
E-mail ID:

PART – II

Commercial Bid

(Price bid along with Breakup to be submitted with Technical Bid in a separate envelope)

Date:

The Deputy General Manager
Indian Bank
Head Office, I floor,
Inspection & Audit Department,
No.66 Rajaji Salai, Chennai – 600001

Dear Sirs,

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: Your RFP No. GEM/2024/B/5198605 dated 24/07/2024

We submit hereunder the price breakup details for **Comprehensive Cyber Security Audit,** as per the specifications.

PRICE SCHEDULE:

(a)	(b)	(c)	(d)	(e)	(f=d+e)
Sl. No	**Brief description of the services**	**Ref in Scope**	**Base Amount Rs.**	**GST Rs.**	**Total Price incl. taxes Rs.**
1	Conduct of Comprehensive Cyber Security Audit (CSA) and submission of Final Audit Report as per the scope in RFP	(1)			
2	Conduct of Limited Audit and submission of Final Report as per the scope in RFP	(2)			
3	Conduct of Compliance Audit for Comprehensive Audit as well as Limited Audit on monthly basis during the period of contract and submission of Final Certification on full compliance	(3)			
	Total Cost of Audit (TCA)				

PRICE STATEMENT:

Bank will not provide any reimbursement for travelling, lodging/boarding, local conveyance or any other related expenses.

Bank reserves the right to re-negotiate the price for any of the line items furnished above, in case the rates offered are arbitrary and not as per market prices.

Number of instances indicated in the RFP are indicative only and the actual work done may be more or less than the count indicated in the RFP based on actual requirement of the Bank.

Total Cost of Audit (TCA) for the entire contract period, inclusive of all duties, levies, freight, insurance, warranty, etc. and all applicable taxes, is Rs.………………………. (in figures) Rupees ……………………… (in words)

We submit that we shall abide by the details given above and the conditions given in your above tender.

For

Office Seal (Authorised Signatory)
Place: Name:
Date: Designation:
Mobile No:
Business Address:
Telephone No:
E-mail ID:

(LIST OF ANNEXURES)

ANNEXURE-I

Declaration / Fair Practices Code Undertaking

(*To be submitted on the letter head of the bidder signed by* Director/Partner)

To Date:

The Deputy General Manager
Indian Bank
Head Office, I floor,
Inspection & Audit Department,
No.66 Rajaji Salai, Chennai – 600001

Dear Sir,

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: Your RFP No. GEM/2024/B/5198605 dated 24/07/2024

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to conduct **Comprehensive Cyber Security Audit**, in conformity with the said Bidding Documents.

We, hereby declare/undertake as under:

We, __________________________ (The applicant) or our promoters or sister concerns or our group companies /LLPs / firms/ organizations/ agencies are not involved in any legal case that may affect our solvency / existence or in any other way affect our capability to provide / continue the services to the Bank.

We are not involved in any dispute / litigation / arbitration proceeding relating to performance of any contract undertaken by us.

We have not been blacklisted nor have been technically disqualified on the grounds of non-performance of contract, by any Commercial Banks/ Financial Institution/ Public Sector Organisation/ any Government agency / Statutory or Regulatory Body/ Ministry or Department of Government of India or State Governments and we undertake to inform the Bank immediately about any such blacklisting / disqualification, if arise in future.

The Name of our company/LLP/firm or its promoter/partner etc. are not in any of the defaulter/barred/caution list published/ displayed at web sites of public/ Autonomous bodies such as RBI/ IBA/ ECGC/SEBI/ICAI.

We further declare and confirm that our company/LLP/firm or its sister concern has not been involved in any unlawful activity as per the laws of the land.

None of the Partners/ Directors of the firm/LLP / company is a member of the Bank’s board.

We/our sister concerns have not undertaken statutory audit of the Bank presently or in the previous financial year.

We/our sister concerns have not undertaking / presently undertaking any other assignment of the Bank, which will be have potential conflicts of interest with the proposed IS Audit assignment/s of the Bank.

We undertake that, in competing for and, if we are selected, in executing the Agreements, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

We declare that we have neither entered into nor are party to (whether by conduct or by acquiescence) any restrictive trade practice or sub-contracting arrangement or collective arrangement with any other person or entity including the other Applicants for the audit, in connection with the preparation and/or submission of our responses.

We undertake, if our bid is accepted, to deliver the services in accordance with the delivery schedule specified in the Schedule of Requirements.

If our bid is accepted, we will obtain a Performance Bank Guarantee from a Scheduled Commercial Bank located in India, for the sum stipulated in the RFP, for due performance of the Contract, in the form prescribed by the Bank.

We agree to abide by this for the bid validity period specified and it shall remain binding upon us and may be accepted at any time before the expiration of that period. We agree to extend the Bid Validity Period, if required.

We also confirm that we shall abide by the conditions, clauses, terms and conditions mentioned in the RFP document.

Until a formal contract is prepared and executed, this bid, together with your notification of award, shall constitute a binding Contract between us.

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

We also understand that the Bank may accept the offer either in part or in full. If the Bank rejects the offer in full or in part, the Bank may do so without assigning any reasons thereof. Bank at all times will have absolute right in its decision and submission of offer does not confer any right with regard to participation in further process.

We further acknowledge that we cannot hold the Bank responsible for any breach of dates in the course of this RFP process.

We understand that the finalized prices will be frozen for the period of contract and that the Bank, at its discretion may entrust the assignment in full or parts at the same price and terms as per its requirements.

We also understand that the Bank reserves the right to call for RFP from audit organizations with similar terms and / or revised terms at its own discretion to include additional audit organisations.

We confirm that we are having resources with sufficient domain and technical knowledge in respect of Security Audit of banking applications including Core Banking and Mobile Banking applications and latest emerging technologies in BFSI Sector like cloud / containerized environment / virtualization / Software Defined Data Network (SDDN), DevOps and automation techniques, etc.

We confirm that Background Verification of our employees and Documentation Verification for their qualifications / validity of their professional certifications, has been conducted prior to their employment with us. We note to provide documentary evidence of the qualifications or professional certifications obtained by the personnel, as and when required by the Bank.

We note to provide the details of renewed certifications, whenever any professional qualification obtained by the Personnel lapses.

We also note to inform the bank promptly in writing, if any of the Key Personnel involved in the audit of the Bank leave the organisation.

As and when any assignment is entrusted, we shall ensure that the Security Audit and IS Audit work is got done by qualified Professionals having requisite expertise.

We note to certify that the personnel who are going to conduct the audit are on our rolls and we note to mention the length of their service with us.

We undertake not to deploy any professional, who was in the services of the Bank prior to the date of accepting any audit assignment from the Bank.

In respect of past Work Experience declared by us, we confirm that the audit assignments have been undertaken by deploying qualified professionals who are permanent employees of our Audit Organization without subcontracting the assignment.

We declare that we have disclosed all material information, facts and circumstances to the Bank. We further confirm that the information furnished in the proposal, annexures, formats, etc. is correct.

We undertake to intimate the Bank immediately about any change/development in our organisation relating to the requirements of this RFP, including but not limited to change in constitution, professional certifications and availability of professional resources.

We also undertake to inform Head Office Inspection & Audit Department of the Bank, before undertaking any other assignment/service to the Bank (other than those covered in this RFP) during the validity of the contract period.

We acknowledge and understand that Bank may make its own inquiries for verification and in the event that any of the information furnished in the proposal is found to be false/incorrect or the Bank discovers anything contrary to our above declarations, Bank is empowered to forthwith disqualify us from further participation in the process. We also understand that the Bank may debar us from participating in future tenders and report the matter to regulatory authorities.

We understand that we are bound by the confidentiality agreement / NDA to be signed by our organization, in case we are empanelled and we shall ensure removal of any data/ information of the bank from our systems / hard discs / mails after the completion of the audit period and provide confirmation immediately after removal of the same. During the period of empanelment, we shall not share any confidential information through personal email IDs / cloud storage.

It is hereby confirmed that I/We are entitled to act on behalf of our company/LLP/ firm and authorized to sign this document as well as such other documents, which may be subsequently called for in connection with this RFP.

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

ANNEXURE-II

Declaration for MSE Benefits

(*To be submitted on the letter head of the bidder signed by* Director/Company Secretary)

To Date:
The Deputy General Manager
Indian Bank
Head Office, I floor,
Inspection & Audit Department,
No.66 Rajaji Salai, Chennai – 600001

Dear Sir,

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: Your RFP No. GEM/2024/B/5198605 dated 24/07/2024

Dear Sir,

This has reference to our bid submitted in response to your Request for Proposal (RFP) Ref. No. RFP No. GEM/2024/B/5198605 dated 24/07/2024 floated for Comprehensive IS Audit of Bank's ICT Infrastructure. We have carefully gone through the contents of the above referred RFP and hereby undertake and confirm that, as per the Govt. Of India guidelines, we are eligible to avail the MSE benefits in response to your RFP floated, as referred above.

In case, at any later stage, it is found or established that, the above undertaking is not true then the Bank may take any suitable actions against us viz. Legal action, Cancelation of Notification of Award/Work Order/contract (if issued any), Blacklisting & debarment from future tender/s etc.

Yours Sincerely

For M/s ______________________

Signature
Name:
Designation: Director/Company Secretary
Place:
Date:
Seal & Stamp

ANNEXURE-III

Declaration On Procurement from a Bidder of a Country which shares a land border with India

(THE BIDDER SHOULD GIVE THE FOLLOWING UNDERTAKING / CERTIFICATE ON ITS LETTERHEAD)

To Date:
The Deputy General Manager
Indian Bank
Head Office, I floor,
Inspection & Audit Department,
No.66 Rajaji Salai, Chennai – 600001

Dear Sir,

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: Your RFP No. GEM/2024/B/5198605 dated 24/07/2024

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India; I certify that **<< name of the firm>>** is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. *[Evidence of valid registration by the Competent Authority shall be attached, wherever applicable.]*

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

ANNEXURE-IV

BID SECURITY DECLARATION FORM

To Date:
The Deputy General Manager
Indian Bank
Head Office, I floor,
Inspection & Audit Department,
No.66 Rajaji Salai, Chennai – 600001

Dear Sir,

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: Your RFP No. GEM/2024/B/5198605 dated 24/07/2024

We declare that, we will not withdraw our bid during the period of bid validity specified in this RFP and we will not fail or refuse to execute the Agreement and furnish the performance security as specified in the RFP.

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

ANNEXURE-V

Pre-Bid Query Format

(to be sent in MS-Excel format to isaudit@indianbank.co.in)

Sub: Request for Proposal for Comprehensive Cyber Security Audit

Ref: RFP No. GEM/2024/B/5198605 dated 24/07/2024

Bidder's Name:

S.No	Page No	Para No.	Description	Query details

Whether interested in participating in Pre-bid meeting; if so, details of participants :

S.No	Name	Designation	Section	Contact No. / Email id

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

ANNEXURE–VI

Contract Form
(To be submitted on Non - Judicial Stamp Paper)

THIS AGREEMENT is made the ....day of.................................202.. between Indian Bank, having its *Corporate Office, 254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600014* (hereinafter "the Bank") which term shall unless repugnant to the context or meaning thereof shall mean its successors and assigns) of the one part and ………………………………… (Name of IS Auditor) having its Registered Office at ………………………………………………… (City and Country of IS Auditor) (hereinafter called "the IS Auditor") which term shall unless repugnant to the context or meaning thereof shall mean its successors and permitted assigns) of the other part:

WHEREAS the Bank invited bids vide RFP No. …………………………. for conduct of Comprehensive Information System Audit of Indian Bank's Information and Communication Technology infrastructure and has accepted a bid by the IS Auditor for the provision of those services for a sum of .... (Contract Price in Words and Figures) (hereinafter called "the Contract Price") for a period of 15 months.

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:
   (a) the RFP including Addendum/s & corrigendum/s (if any);
   (b) the Bid Form and the Price Schedule submitted by the Bidder;
   (c) the Conditions of Contract;
   (d) the Purchaser's Notification of Award/Work Order;
   (e) the Service Level Agreement.

3. In consideration of the payments to be made by the Bank to the IS Auditor as hereinafter mentioned, the IS Auditor hereby covenants with the Bank to provide the services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Bank hereby covenants to pay the IS Auditor in consideration of the provision of the services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

5. Total Cost of Audit (TCA) for the entire contract period, inclusive of all duties, levies, freight, insurance, warranty, etc. and all applicable taxes, is Rs.……………………….. (in figures) Rupees ……………………… (in words)

6. The above price is all inclusive of incidental costs such as travel, lodging/boarding, local conveyance or any other related expenses incurred during the project.

7. Bank reserves the right to re-negotiate the price for any of the line items furnished above, in case the rates offered are arbitrary and not as per market prices.

8. Number of instances indicated in the RFP are indicative only and the actual work done may be more or less than the count indicated in the RFP based on actual requirement of the Bank.

9. The entire process of audit and submission of final report covering all areas as per Scope / RFP will be completed within 3 months of execution of contract.

10. The Compliance Audit Reports after completion of compliance verification shall be submitted by 10th of every month during the contract period.

11. **IN WITNESS** whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the

said .... (For Indian Bank)

in the presence of: ....

Signed, Sealed and Delivered by the

said .... (For the supplier)

in the presence of:......................................

ANNEXURE-VII

SERVICE LEVEL AGREEMENT

THIS Service Level Agreement is made the ....day of.................................202.. between ………………………………… (Name of IS Auditor) having its Registered Office at …………………………………………………. (City and Country of IS Auditor) (hereinafter called “the IS Auditor”) which term shall unless repugnant to the context or meaning thereof shall mean its successors and assigns) of the one part and Indian Bank, having its *Corporate Office, 254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600014* (hereinafter “the Bank”) which term shall unless repugnant to the context or meaning thereof shall mean its successors and permitted assigns) of the other part:

The IS auditor and INDIAN BANK are hereinafter collectively referred to as the “Parties” and individually as the “IS Auditor” and “Bank” respectively.

WHEREAS the Bank invited bids vide RFP No. …………………………. for conduct of Comprehensive Cyber Security Audit and has accepted a bid by the IS Auditor for the provision of those services for a sum of .... (Contract Price in Words and Figures) (hereinafter called “the Contract Price”).

Indian Bank has issued work order ref: ………… dated ………...The work order and the related agreements are valid up to 15 months from the date of execution of contract or compliance of all the deliverables of the RFP, whichever is later.

Bank reserves the right to call for additional information from the IS Auditor at the time of annual review.

NOW THEREFORE THE PARTIES HERETO AGREE AS FOLLOWS:

1. **Scope of Comprehensive Audit**

Comprehensive Cyber Security Audit should be conducted to cover the Guidelines prescribed by MeitY as detailed hereunder and Audit Report to be submitted as per 282 point audit checklist and 40 point audit summary prescribed by NIC Cyber Security Audit Division.

1.1 Comprehensive audit should cover the entire application, including the following:

(a) web application (both thick client and thin client);

(b) mobile apps;

(c) APIs (including API whitelisting):

(d) databases;

(e) hosting infrastructure and obsolescence;

(f) cloud hosting platform and network infrastructure; and

(g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

1.2 The scope of the comprehensive audit should include, inter alia, the following:

(a) source code assessment;

(b) application security assessment (both Black Box and Grey Box testing), including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;

(c) network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs);

(d) penetration testing;

(e) network and device configuration review;

(f) application hosting configuration review;

(g) database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication);

(h) user access controls (including privilege access management) and access reconciliation review;

(i) identity and access management controls review;

(j) data protection controls review (Inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches/Data Leaks [CIAD-2021-0004]");

(k) security operations and monitoring review (including maintenance of security logs, correlation and analysis);

(l) review of logs, backup and archival data for access to personal data (including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian Jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); and

(m) review of key management practices (Including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website).

2. Scope of the Limited audit

2.1 Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is

(a) modification in application functionality; or

(b) addition/modification of APIs; or

(c) migration to new infrastructure platform or cloud service; or

(d) change in configuration of application hosting, servers, network components and security devices; or

(e) change in access control policy.

2.2 The scope of limited audit should include, inter alia, the following:

(a) In all cases: Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;

(b) In case limited audit is after six months of comprehensive audit: In addition to (a) above, user access controls (including privilege access management) and access reconciliation review; identity and access management controls review;

(c) In case limited audit is done earlier: In addition to (a) and (b) above,

(i) For audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change configuration of application hosting, servers, network components and security devices: Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets, and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs); network and device configuration review; application hosting configuration review; database security assessment (including whether personal data is being encrypted at rest and in motion, or used tokenised form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorised users and are protected with multi factor authentication); data protection controls review (inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration with security monitoring solutions, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); review logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

(ii) For audit on change in access control policy: Review of logs and integration with security monitoring solutions.

3. Compliance Audit

Audit to be followed by compliance audit on monthly basis to verify and confirm the compliance status reported by the Bank. The non-compliances to be reported with respective remarks from the Bank, Auditor's comments with reasons for disagreements, if any and PoCs.

4. Deliverables

1. The IS Auditor will nominate a Project Manager immediately on acceptance of the order, who will be the single point of contact for the Project. Additionally, escalation contact details to be submitted to the Bank.
2. The Auditor has to undertake IS Audit in a phased manner as described below:
   (v) Conduct of Comprehensive Cyber Security Audit (CSA) as per scope & submission of preliminary reports of IS Audit findings and discussion on the findings.
   (vi) Submission of final CSA reports in a format acceptable to the Bank for regulatory compliance.
   (vii) Conduct of Limited Audit after 6 months of the Final Comprehensive Audit Report.
   (viii) Conduct of Compliance review & submission of Certification for Compliance.
3. IS Audit / VAPT to be scheduled and conducted in such a way that there is no business downtime.
4. Only licensed tools have to be utilized and each audit report shall include the details of tools utilized, version of the tools, license, etc. along with a declaration / confirmation that the tools used
   - are free from any malicious code & malwares,
   - are updated with latest patches released by the OEM and
   - are updated with the latest vulnerabilities notified by Market Intelligence sources.
5. The checklists updated and evidences/PoCs collected during the audit process are to be shared with Bank's Inspection Department for their reference and for submission to Regulatory Authorities, as and when required.
6. Dedicated Single Point of Contact (SPOC) to be available (both onsite / offsite) during the entire contract period for conduct of audit and to clarify on compliance issues / to guide the Bank for closure of vulnerabilities.

5. Jurisdiction

Any dispute arising out of this order will be governed under Indian Law and shall be subject to the jurisdiction of Courts of Law in Chennai, Tamil Nadu.

6. Other Terms and Conditions

The terms and conditions specified in the work order dated ……… shall be treated as part and parcel of this Agreement.

Further, the IS Auditor agrees on the following

01) Visit by RBI or any other Regulatory Authority viz., recognize the right of the RBI or any other Regulatory Authority to conduct inspection of service provider of the Bank and its books and accounts by one or more of its officers or employees.
02) Submission of EPF paid details of the outsourced employees to Bank.
03) The workers employed by the IS Auditor are provided adequate salary as per Minimum Wages Act, medical and PPF facilities etc. as applicable.
04) Contingency Plans, Testing thereof to maintain Business Continuity (BCP)

05) Bank will periodically review the financial and operational conditions of the IS Auditor to assess their ability to continue to meet their outsourcing activities.

Whatever not specifically mentioned herein, is subject to the terms and conditions of the Work order cited above.

7. Liquidated Damages and Penalty:

The liquidated damages will be an estimate of the loss or damage that the bank may have suffered due to delay in performance of the obligations by the IS Auditor under the terms and conditions of the contract and its amendments and the IS Auditor shall be liable to pay the Bank as liquidated damages at the rate of 0.5% of the contract price for delay of every week or part thereof. Once the penalty crosses 10% of the contract price, the Bank reserves the right to cancel the contract or take any other suitable penal action as deemed fit.

Without any prejudice to the Bank's other rights under the law, the Bank shall recover the liquidate damages, if any, accruing to the Bank, as above, from any amount payable to the Service Provider either as per the Contract, executed between the Bank and the Service Provider pursuant hereto or under any other Agreement/Contract, the Bank may have executed/shall be executing with the Service Providers.

8. Severability:

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this agreement shall not be affected or impaired.

WITNESS:

In witness whereof, the Parties have caused this agreement to be signed by their duly authorised representatives as of the date first written above.

For INDIAN BANK For M/s

Name: ________ Name:

Designation: _________ Designation:

Witness: Witness:

ANNEXURE-VIII

Non-Disclosure Agreement

THIS AGREEMENT made and entered into at …………………on this the ……day of………202… between **INDIAN BANK**, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act 1970, having its Corporate Office at 254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600 014, hereinafter called the "**BANK**" which term shall wherever the context so require includes its successors and assigns

AND

M/s……………………………. Limited a company registered under the Companies Act having its registered office at………………………………… hereinafter called the "IS Auditor" which term shall wherever the context so require includes its successors and assigns, **WITNESSETH**:

WHEREAS

The Bank is inter-alia engaged in the business of banking and intends to engage IS Auditor for conduct of Information System Audit of Bank's Information and Communication Technology Infrastructure.

M/s……………………………. Limited has been engaged in the business of providing IS Audit services.

The parties have entered into agreement dated ________________ for providing IS Audit services (herein after referred to as "purpose")" and have established business relationship between themselves. In course of the said purpose, it is anticipated that each party may disclose or deliver to the other certain or some of its trade secrets or confidential or proprietary information. The parties have agreed that disclosure and use of such confidential information shall be made and on the terms and conditions of this agreement.

NOW THERFORE THIS AGREEMENT WITNESSETH and it is hereby agreed by and between the parties hereto as follows:

1. Confidential information

Confidential Information means all information disclosed/ furnished by either party to another party in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof and all electronic material or records, tenders and other written, printed or tangible thereof and include all information or material that has or could have commercial value or other utility in the business in which disclosing party is engaged.

Receiving party may use the information solely for and in connection with the Purpose.

2. Use of Confidential Information

Each party agrees not to use the other's confidential information for any purpose other than for the specific purpose. Any other use of such confidential information by any party shall be made only upon the prior written consent from the authorized representative of the other party or pursuant to subsequent agreement between the Parties hereto.

The receiving party shall not commercially use or disclose for commercial purpose any confidential information or any materials derived there from, to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to access to and knowledge of the confidential information solely for the purpose authorized above. Whenever, it is expedient under the contract, the Receiving Party may disclose confidential information to consultants/third party only if the consultant/ third party has executed non-disclosure agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these and such consultant should also be liable to the original disclosing party for any unauthorized use or disclosure. The Receiving party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing party's confidential information in violation of the terms of this Agreement.

Neither party shall make news release, public announcements, give interviews, issue or publish advertisements or Agreement, the contents/provisions thereof, other information relating to this agreement, the purpose, the Confidential information or other matter of this agreement, without the prior written approval of the other party.

Upon written request by the Bank, the IS Auditor shall:

(i) cease using the Confidential information,

(ii) return the Confidential Information and all copies, notes or extracts thereof to the Bank within seven (7) business days of receipt of request and

(iii) confirm in writing that the Receiving Party has complied with the obligations set forth in this paragraph."

3. Exemptions

The obligations imposed upon either party herein shall not apply to information, technical data or know how whether or not designated as confidential, that is:

- already known to the Receiving party at the time of the disclosure without an obligation of confidentiality
- or becomes publicly known through no unauthorized act of the Receiving party
- rightfully received from a third party without restriction and without breach of this agreement

- independently developed by the Receiving party without use of the other party's confidential information and is so documented.
- disclosed without similar restrictions to a third party by the Party owning the confidential information
- approved for release by written authorization of the disclosing party; or
- required to be disclosed pursuant to any applicable laws or regulations or any order of a court or a governmental body; provided, however that the Receiving party shall first have given notice to the Disclosing Party and made a reasonable effort to obtain a protective order requiring that the confidential information and / or documents so disclosed used only for the purposes for which the order was issued.

4. Term

This agreement shall be effective from the date of the execution of this agreement and shall continue till expiration or termination of this agreement due to cessation of the business relationship between the parties. Upon expiration or termination as contemplated herein the Receiving party shall immediately cease any or all disclosures or uses of confidential information and at the request of the disclosing party, the receiving party shall promptly return or destroy all written, graphic or other tangible forms of the confidential information and all copies, abstracts, extracts, samples, note or modules thereof.

Notwithstanding the above, the obligations of the receiving party in respect of disclosure and confidentiality shall continue to be binding and applicable without limit until such information enters the public domain.

5. Title and Proprietary rights

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No License under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

6.Return of confidential information

Upon written demand of the disclosing party, the receiving party shall (i) cease using the confidential information (ii) return the confidential information and all copies, abstracts, extracts, samples, note or modules thereof to the disclosing party within seven (7) days after receipt of notice and (iii) upon request of the disclosing party, certify in writing that the receiving party has complied with the obligations set forth in this paragraph.

7. Remedies

The receiving party acknowledges that if the receiving party fails to comply with any of its obligations hereunder, the disclosing party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The receiving party agrees that, in addition to all other remedies provided at law or in equity, the disclosing party shall be entitled to injunctive relief hereunder.

8. Entire agreement

This agreement constitutes the entire agreement between the parties relating to the matter discussed herein and supersedes any and all prior oral discussion and/or written correspondence or agreements between the parties. This agreement may be amended or modified only with the mutual written consent of the parties. Neither this agreement nor any rights, benefits and obligations granted hereunder shall be assignable or otherwise transferable.

9. Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this agreement shall not be affected or impaired.

10. Dispute resolution mechanism

In the event of any controversy or dispute regarding the interpretation of any part of this agreement or any matter connected with, arising out of, or incidental to the arrangement incorporated in this agreement, the matter shall be referred to arbitration and the award passed in such arbitration shall be binding on the parties. The arbitral proceeding shall be governed by the provisions of Arbitration and Reconciliation Act 1996 and the place of arbitration shall be Chennai.
Submitting to arbitration may be considered as an additional remedy and it does not preclude the parties to seek redressal / other legal recourse.

11. Jurisdiction

Any disputearising out of this order will be under the jurisdiction of Courts of Law in Chennai.

12. Indemnity clause

“The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party etc., officers, employees, agents or consultants.”

13. Governing laws

The provisions of this agreement shall be governed by the laws of India.
In witness whereof, the parties hereto have set their hands through their authorised signatories

BANK ……………………….…………

M/s ……………………….…………

ANNEXURE-IX
Performance Security Format

Bank Guarantee No. Date:

To: INDIAN BANK,
Chennai,
INDIA:

WHEREAS .... (Name of Supplier) hereinafter called “the Supplier”) has undertaken, in pursuance of Contract No................. dated .... to conduct Comprehensive Cyber Security Audit (hereinafter called “the Contract”).

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier’s performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to issue a Guarantee in your favor on the request of the Supplier:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total sum of Rs.................................. .... (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the IS Auditor to be in default under the Contract and without any demur, cavil or protest, any sum or sums within the limit of .... (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the ....day of...................20__

Signature of Authorized Official with Seal

....
Date...202…
Address: ....
....

NOTE:

1. Supplier should ensure that seal and code no of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank Guarantee issued by a scheduled commercial Banks located in India and shall be on a Non-Judicial Stamp Paper of requisite value.

ANNEXURE-X
Audit Report Format

I. CSA Status Report wrt Vulnerabilities checked for : ___<Mention Application/Project Name>____ Date: ___________________________________

					Identified Vulnerabilities		
			Vulnerabilities Checked for	Refer 282-Pointer Checklist	H	M	L
Application	VAPT	7	Hosting Environment Security	Refer Controls under section F.1			
			Security Monitoring of Hosting Environment	Refer controls under section F.2			
			Security Assurance on Third Party Cloud Service Provider (CSP)	Refer Controls under Section F.3			
			Backup and System Resilience	Refer Controls under Section F.4			
			Hosting System Decommissioning / Migration	Refer Controls under Section F.5			
			Automated and Manual Code testing	Refer Controls under A.4			
			Conduct Penetration Testing	Refer Controls under D.1			
	APIs	1	Application and API Hosting Security Configurations, Data Transmission and Encryption and Application Functionality Security Assessment	Refer Controls under B.2			
	Apps	2	Application Security Testing	Refer Controls under B.1			
			Aadhaar Authentication Application / API related security controls	Refer to Aadhaar related controls			
	Source Code	6	Planning and Information Gathering	Refer controls under Section A.1			
			Secure Application Development / Coding practices	Refer controls under Section A.2			
			Version Management and Release Management	Refer controls under Section A.3			
			Automated Source Code Scanning	Refer controls under Section A.4			
			Manual Code Analysis	Refer controls under Section A.4			
			Aadhaar Authentication Application / API related security controls	Refer to Aadhaar related controls			
	Aadhaar	4	HSM Vault	Check if HSM is used for Aadhaar Authentication			

			ADV	Check if ADV is used for Aadhaar Authentication			
			PID Block	Check if PID Block is being signed appropriately by the entity for Aadhaar Authentication			
			License key hardcoded	Check if License Key is hardcoded in the source code			
	Database	4	Access control, Authentication and Monitoring	Refer controls under Section G.1			
			Database Encryption	Refer controls under Section G.2			
			Database Updates and Patch Management Review	Refer controls under Section G.3			
			Database Activity Monitoring	Refer controls under Section G.4			
	Log Retention	2	Timelines Defined	Refer controls under Section E.3			
			Data retained as per timeline/regulatory	Refer controls under Section E.3			
	Log Review	2	SOC SIEM Implemented	Refer controls under Section E.3			
			Continuous Monitoring	Refer controls under Section E.3			
Network	VAPT	4	Network Security Architecture Review	Refer controls under Section C.1			
			Network Security Patches	Refer controls under Section C.2			
			Network Monitoring	Refer controls under Section C.3			
			Conduct Penetration Testing	Refer Controls under D.1			
	Configuration	3	Device Configuration Review	Refer controls under Section E.1			
			Network Redundancy	Refer controls under Section E.2			
			Logging and Monitoring	Refer controls under Section E.3			
	Access Control	5	User Access Management Policy and Controls	Refer controls under Section H.1			
			Privileged user controls and Segregation of Duties / Roles	Refer controls under Section H.2			
			User Credentials Management	Refer controls under Section H.3			
			IAM Policy, Procedure and Access controls	Refer controls under Section I.1			
			IAM Security Controls and Authentication Mechanism	Refer controls under Section I.2			
	Total	**40**	Total Score				

II. CSA Audit Checklist : ___<Mention Application/Project Name>____ Date: _______________________________

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
1	**ISOG**	**Information Security Organisation and Governance Check for information security organisation structure, governance framework and information security policies applicable for the audit entity / organisation.** **For any outsourced function or managed services operations by external agency, check for the third party / vendor governance, management and information security compliances.**			
2	**ISOG.1**	**Information Security Organisation**	**To determine whether the audit entity / organisation have a CISO function that oversees information security governance and compliances.**		
3	ISOG.1.1	1. Check whether the auditee organisation has appointed a dedicated CISO / Information Security Officers to oversee and enforce information security practices within the organisation.			
4	ISOG.1.2	2. Where applicable, check whether auditee organization has an independent Data Privacy Officer (DPO) to oversee and enforce data protection and privacy compliance requirements in accordance with country's data protection act and/or sectoral regulatory mandates.			
5	**ISOG.2**	**Information Security Organisation**	**To determine whether the CISO function have independent reporting to entity's Board of Directors / CEO.**		

6	ISOG.2.1	1. Check for the documented and approved information security organisation structure. Wherever applicable, also check for the information privacy organization structure and processes.			
7	**ISOG.3**	**Information Security Governance**	**To determine whether the audit entity / organisation follow established information security practices in reference to ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework, ISO27701 (PIMS) and other industry leading standards.**		
8	ISOG.3.1	1. Check for the information security and privacy certification of the audit entity / auditee organisation. Check valid ISO27001 certification at deployment location			
9	ISOG.3.2	Incorporation/Adherence to Meity and Cert-In guidelines			

10	**ISOG.4**	**Information Security Governance**	**To determine whether the audit entity / organisation performs periodic (annual / half yearly / quarterly, as applicable) review of information security risks and compliances of its ICT applications and infrastructure in accordance with the leading industry standards as mentioned in ISOG.3** **To determine whether there is an established third party information security policy and whether the third party information security risks and compliances were documented and reviewed by auditee organization's CISO / Security Officer / Board. (Where applicable, for external suppliers / vendors / outsourced managed services operations that manage or maintain the ICT applications and/or infrastructure)**		
11	ISOG.4.1	1. Check for adequacy of governance review process and periodicity of reviews.			

12	ISOG.4.2	3. Review the action taken by management of audit entity to address the risks and non-compliances / open observations / open vulnerabilities. Check last Application Security Audit, VAPT status as per the adopted Security Audit Policy. Check for the past audit reports and vulnerabilities reported by internal auditors and/or CERT-In auditors. Check for past 1 year audit reports. Review the frequency and completeness of network vulnerability assessments, DC/DR, existence of network segmentation to isolate critical assets and enhance overall network security. Determine the implementation of encryption protocols to secure sensitive data transmitted over the network.			
13	ISOG.4.3	1. Understand the 3rd party / vendor / supplier ecosystem of the audit organizations and identify the critical ICT infrastructure (e.g. application development and upgrade, Data Center support / operations, security infrastructure configurations and administration etc.)			
14	ISOG.4.4	2. Check for the 3rd party information security policy. Check for 3rd party information security risks and compliances documentation / reports for open / critical risks and issues.			
15	ISOG.4.5	Check processes and procedures for monitoring adherence to established information security requirements for each type of supplier and level of access, including third-party reviews and product validation/certification by recognized authority. Check for standardized process and lifecycle for managing supplier relationships (such as NDA signing) with each of the supplier			
16	**A**	**Source Code Assessment (SAST)**	**Source code assessment should be performed for all in-scope applications (including web applications and mobile applications) and API's**		

17	**A.1**	**Planning and Information Gathering**	**To determine whether application deployment and security architecture is documented and depicts at minimum the following:** - **Servers** - **Applications (incl. web & mobile apps)** - **API's** - **IP schema details** - **interfaces with database(s)** - **PII data flow**		
18	A.1.1	1. Identify the application testing scope and plan the testing methodology.			
19	A.1.2	2. Guidance for certain minimum checks include the following:			
20	A.1.2.1	a) Deployment architecture documented plan depicting (Servers, applications, APIs, IP Schema details and interfaces that access the database) should be made available.			
21	A.1.2.2	b) Inspect the page source for sensitive PII info. Manually explore the site and Review the web Contents			
22	A.1.2.3	c) Check whether only web Interface or both Mobile and Web Interface is available			
23	A.1.2.4	d) Check for last Audit compliance status			
24	A.1.2.5	e) Spider/crawl for missed or hidden content. Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store			
25	A.1.2.6	f) Check the caches of major search engines for publicly accessible sites			
26	A.1.2.7	g) Check for differences in content based on User Agent (e.g. mobile sites, access as a search engine crawler)			
27	A.1.2.8	h) Perform Web Application Fingerprinting			
28	A.1.2.9	i) Identify technologies used and Identify user roles			

29	A.1.2.10	j) Identify application entry points and Identify client-side code			
30	A.1.2.11	k) Identify multiple versions/channels (e.g. web, mobile web, mobile app, web services)			
31	A.1.2.12	l) Identify co-hosted and related applications			
32	A.1.2.13	m) Identify all hostnames and ports			
33	A.1.2.14	n) Identify third-party hosted content			
34	A.1.2.15	o) Perform Reconnaissance via Google Dorks Search			
35	A.1.2.16	p) Script output of web folder for assessment of clean data			
36	A.1.2.17	q) Check and examine the permission of read & write folder			
37	**A.2**	**Secure Application Development / Coding practices**	**To determine whether secure application development practice / process exists in the auditee organisation.**		
38	A.2.1	1. Inquire with application owner and application developer to understand the application development methodology.			
39	A.2.2	2. Check for DevSecOps (CI/CD pipeline based Security operations) processes and/or security checkpoints/tollgate process for application development. Check whether Code review (Source Code Analysis) Process is part of the development process or not.			
40	A.2.3	3. Validate code adherence to established coding standards, industry guidelines and assessment frequency during SAST assessments and check whether developers are trained on secure coding practices.			
41	A.2.4	4. Check whether there is separate development / staging environment and production environment.			

42	**A.3**	**Version Management and Release Management**	**Review the application code version and the major/minor changes committed in the version management tool (e.g. SVN, BitBucket, Gitlab etc.).**		
43	A.3.1	1. Check for major and minor code releases committed in the version management tool and the change description.			
44	A.3.2	2. Check for the release management process and approvals workflow. Check if approvals are provided by Change Advisory Board (CAB) or authorized personnel from senior management in change of application security. Check for approval records. Check if source code handling is limited to authorized users only.			

45	**A.4**	**Automated Source Code Scanning & Manual Code Analysis**	**Perform automated source code scan using a reliable open-source or proprietary scanning tool such as Fortify, SonarQube, Checkmarx etc. and assess for vulnerabilities (in accordance with OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis).** Perform manual code review to identify the following vulnerabilities in the source code- sensitive information disclosure (including hard-coding of PII data, PII tokens, authentication tokens, security keys, encryption keys, passwords / user credentials, etc.)		
46	A.4.1	1. Utilize the SAST tool to identify and prioritize high risk vulnerabilities (refer OWASP testing guide and CERT-In guidelines).			
47	A.4.2	2. Verify that the SAST tools are configured to check for compliance with coding standards and security policies.			
48	A.4.3	3. Review the results of automated scans to ensure comprehensive coverage of the codebase.			
49	**B**	**Application Security Assessment (both Black Box and Grey Box)**	**Assessment should be performed as per OWASP Testing Guide and CERT-In Guidelines for Secure Application Design, Implementation and Analysis**		

50	**B.1**	**Application Security Testing**	**Perform application security testing using reliable open-source or proprietary application security tools such as OWASP ZAP, Acunetix, Burp Suite etc. and assess for vulnerabilities** **(in accordance with OWASP Testing Guide and CERT-In guidelines for secure application design, implementation and analysis).**		
51	B.1.1	1. Check for application authentication, authorization session management, etc.			
52	B.1.2	2. Examine error messages for application sensitive information disclosure or internal server leakage details			

53	**B.2**	**Application and API Hosting Security Configurations, Data Transmission and Encryption and Application Functionality Security Assessment**	**Review the application security configurations including secure data transmission (TLS, SSL) and encryption configurations to protect sensitive information / data to determine that latest / secure encryption protocols have been deployed.** **Review the application access and authentication configurations / parameters and test whether user authentications can be bypassed or leveraged for admin/privileged users.** **Review the application features, functionality and test for potential misuse of application business logic and denial of service.** **Review the application/ API whitelisting and secure API linkages to determine whether access to applications and API's is limited to authorized users and systems only.**		
54	B.2.1	1. Check for the following authentication configurations:			
55	B.2.1.1	a) Check for user enumeration			
56	B.2.1.2	b) Check for authentication bypass			

57	B.2.1.3	c) Check for brute force protection			
58	B.2.1.4	d) Check password security controls such as quality rules, autocomplete on password forms/input, change process, reset and/or recovery, password is salted hashed (e.g. SHA256, SHA512)			
59	B.2.1.5	e) Check remember me functionality			
60	B.2.1.6	i) Check integrity and security of CAPTCHA			
61	B.2.1.7	j) Check multi factor authentication			
62	B.2.1.8	k) Check for logout functionality presence			
63	B.2.1.9	l) Check for cache management on HTTP (e.g. Pragma, Expires, Max-age)			
64	B.2.1.10	m) Check for default logins			
65	B.2.1.11	n) Check for user-accessible authentication history			
66	B.2.1.12	o) Check for out of channel notification of account lockouts and successful password changes			
67	B.2.1.13	p) Check for consistent authentication across applications with shared authentication schema / SSO			
68	B.2.1.14	r) Check whether Salt is generated at client side or server side			
69	B.2.1.15	s) Check for clipboard data stealing attack			
70	B.2.2	2. Check for the following Session Management configurations:			
71	B.2.2.1	a) Establish how session management is handled in the application (e.g. tokens in cookies, token in URL)			
72	B.2.2.2	b) Check session tokens for cookie flags (HTTP Only and secure)			
73	B.2.2.3	c) Check session cookie scope (path and domain)			
74	B.2.2.4	d) Check session cookie duration (expires and max-age)			
75	B.2.2.5	e) Check session termination after a maximum lifetime			
76	B.2.2.6	f) Check session termination after relative timeout			
77	B.2.2.7	g) Check session termination after logout			
78	B.2.2.8	h) Check to see if users can have multiple simultaneous sessions			

79	B.2.2.9	i) Check session cookies for randomness			
80	B.2.2.10	j) Confirm that new session tokens are issued on login, role change and logout			
81	B.2.2.11	k) Check for consistent session management across applications with shared session management			
82	B.2.2.12	l) Check for session puzzling			
83	B.2.2.13	m) Check for CSRF and clickjacking			
84	B.2.3	3. Check for the following data validation configurations:			
85	B.2.3.1	a) Check for Reflected, Stored, DOM based Cross Site Scripting and Cross Site Flashing			
86	B.2.3.2	b) Check for Injections related vulnerabilities such as HTML injection, SQL Injection, LDAP injection, ORM Injection, XML, XXE, SSI Injection, IMAP/SMTP injection, code, command injection, host header injection etc.			
87	B.2.3.3	c) Check for Front end web interface (as per OWASP top 10)			
88	B.2.3.4	d) Check for Overflow (Stack, Heap and Integer)			
89	B.2.3.5	e) Check for Format String			
90	B.2.3.6	f) Check for incubated vulnerabilities			
91	B.2.3.7	g) Check for HTTP Splitting/Smuggling			
92	B.2.3.8	h) Check for HTTP Verb Tampering			
93	B.2.3.9	i) Check for Open Redirection			
94	B.2.3.10	j) Check for Local File, Remote File Inclusion			
95	B.2.3.11	k) Compare client-side and server-side validation rules			
96	B.2.3.12	l) Check for NoSQL injection			
97	B.2.3.13	m) Check for HTTP parameter pollution			
98	B.2.3.14	n) Check for auto-binding			
99	B.2.3.15	o) Check for Mass Assignment			
100	B.2.3.16	p) Check for NULL/Invalid Session Cookie			
101	B.2.3.17	q) Check for Server-side request forgery			
102	B.2.3.18	r) Check for maximum character limit in Input box / Field			

103	B.2.4	4. Check for authorization vulnerabilities			
104	B.2.4.1	a) Check for path traversal			
105	B.2.4.2	b) Check for bypassing authorization schema			
106	B.2.4.3	c) Check for vertical Access control problems (a.k.a. Privilege Escalation)			
107	B.2.4.4	d) Check for horizontal Access control problems (between two users at the same privilege level)			
108	B.2.4.5	e) Check for missing authorization			
109	B.2.5	5. Check for application configurations to prevent denial of service attacks			
110	B.2.5.1	a) Check for anti-automation			
111	B.2.5.2	b) Check for account lockout			
112	B.2.5.3	c) Check for HTTP protocol DoS			
113	B.2.5.4	d) Check for SQL wildcard DoS			
114	B.2.5.5	e) Check for OTP Flooding			
115	B.2.5.6	f) Check for Captcha used cannot be replayed after getting validated			
116	B.2.6	6. Check for business logic misuse			
117	B.2.6.1	a) Check for feature misuse			
118	B.2.6.2	b) Check for lack of non-repudiation			
119	B.2.6.3	c) Check for trust relationships			
120	B.2.6.4	d) Check for integrity of data			
121	B.2.6.5	e) Check segregation of duties			
122	B.2.6.6	f) Check for business logic flaw for complete application workflow			
123	B.2.6.7	g) Check for proper input validation			
124	B.2.6.8	h) Check for concurrent user login misuse			
125	B.2.6.9	i) Check for application session timeout			
126	B.2.6.10	j) Check that acceptable file types are whitelisted			
127	B.2.6.11	k) Check that file size limits, upload frequency and total file counts are defined and are enforced			
128	B.2.6.12	l) Check that file contents match the defined file type			

129	B.2.6.13	m) Check that all file uploads have Anti-Virus scanning in- place.			
130	B.2.6.14	n) Check that unsafe filenames are sanitized			
131	B.2.6.15	o) Check that uploaded files are not directly accessible within the web root			
132	B.2.6.16	p) Check that uploaded files are not served on the same hostname/port			
133	B.2.6.16	q) Check that files and other media are integrated with the authentication and authorization schemas			
134	B.2.6.17	r) Open file upload may be avoided			
135	B.2.7	7. Check for Application API whitelisting			
136	B.2.7.1	a) Check for API Security (as per OWASP top 10 and any directions related to application security as issued by UIDAI)			
137	B.2.7.2	b) Check how external APIs consumed are handled properly			
138	B.2.7.3	c) Check how APIs released are handled			
139	B.2.7.4	d) For thick client based applications, check if application is running on an untrusted system, ensure that thick client should always connect to the backend through an API that can enforce appropriate access control and restrictions. Also, check that Direct connections should never be made from a thick client to the backend database.			
140	B.2.7.5	e) For mobile apps, check for mobile app secure API linkages			
141	B.2.7.6	f) For HTML5 based apps, check for web messaging, web storage SQL injection, CORS implementation (refer CERT-In guidance) and offline web application misuse.			
142	B.3	Assess whether the application is transmitting the information in an encrypted format based on leading encryption standard such as TLS 1.3. Check that deprecated / obsolete encryption protocols / TLS protocols are not configured.			
143	B.4	Check if there are potential man-in-the-middle attack related vulnerabilities in application data transmission.			

144	B.5	Check for the following cryptography and secure transmission configurations:			
145	B.5.1	1. Check for randomness functions			
146	B.5.2	2. Check SSL/TLS Version, Algorithms, Key length, weak ciphers			
147	B.5.3	3. Check for Digital Certificate Validity (Duration, Signature and CN)			
148	B.5.4	4. Check credentials only delivered over HTTPS			
149	B.5.5	5. Check that the login form is delivered over HTTPS			
150	B.5.6	6. Check session tokens only delivered over HTTPS			
151	B.5.7	7. Check if HTTP Strict Transport Security (HSTS) in use			
152	B.5.8	8. Check how Sensitive/PII Data at rest is stored			
153	B.5.9	9. Check how Sensitive/PII Data in transit (like Aadhaar Card, PAN, Credit/Debit Card Number, Password etc.) is handled and stored (check that deprecated encryption protocols is not used)			
154	B.5.10	10. Check how Sensitive/PII Data in use (i.e. Back-end data) is handled			
155	B.6	Security of Sensitive Data			
156	B.6.1	1. Check if sensitive data at rest and in transit encryption is done properly			
157	B.6.2	2. Check for wrong algorithms usage depending on context			
158	B.6.3	3. Check for weak algorithms usage			
159	B.6.4	4. Check for proper use of salting			

160	**C**	**Network Vulnerability Assessment**	**(including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs)**		

161	**C.1**	**Network Security Architecture Review**	**Review the network security architecture design and determine the following: - Whether application, databases and underlying infrastructure is protected for external network attacks (i.e. through use of** **Zero Trust Network Architecture, Firewalls,** **IPS/IDS, Anti-DDoS)** - **Whether the network segmentation and network zoning is implemented to protect the application hosting environment.** - **Whether critical databases hosting sensitive / PII data is not exposed over internet.**		
162	C.1.1	1. Verify that authorization, security controls and access controls are in place, protecting and restricting network access to authorized personnel only.			

163	**C.2**	**Network Security Patches**	Review network asset inventory to determine whether inventory is updated and reviewed periodically. Review the patch management process to determine that critical security patches are implemented on vulnerable network equipment. Review the Network devices for their end of life and security operations support.		
164	C.2.1	1. Check the existence of an up-to-date inventory detailing computers, network components, software, and authorized asset details including users, IPs, AMCs, patch management, antivirus, and software licenses.			
165	C.2.2	2. Confirm the presence of a centralized platform for patch updates / deployment, ensuring centralized visibility of all assets.			
166	C.2.3	3. Inquire whether asset versions and corresponding end-of- life/support details are documented, up-to-date in the inventory and periodically reviewed.			
167	C.2.4	4. Check that security patches and updates are implemented periodically (as per their release) and tested before deployment.			
168	C.2.5	5. Check that latest security patches have been installed.			
169	C.2.6	6. Check that there are no end-of-life / obsolete network devices that are vulnerable to security threats.			

170	**C.3**	**Network Monitoring**	**Review the Network operations and monitoring process to determine whether the network traffic is monitored for unauthorized access and usage.**		
171	C.3.1	1. Check the adequacy of network monitoring tools and technologies to detect and respond to potential network security incidents.			
172	C.3.2	2. Check the network performance and network security incident logs.			
173	**C.4**	**Auditing Business Continuity and Disaster Recovery (BCP/DR)**			
174	C.4.1	1. Has the organization performed a comprehensive asset inventory and assigned business owners to all assets?			
175	C.4.2	2. Has the Project specific Business Impact Analysis (BIA) performed as a part of their BCP/DR plans?			
176	C.4.3	3. Have all the organization’s personnel been trained in their role in the BCP/DR process? . Are all BCP/DR plans tested and kept up-to-date on a regular basis?			
177	C.4.5	5. Is the organization regularly backing up their information systems onsite and offsite in light of their BCP/DR plans?			
178	**D**	**Penetration Testing**			

179	**D.1**	**Penetration Testing Scope and Coverage**	**Review the network penetration testing policy to determine the periodicity and coverage of network penetration tests.** **Review the past penetration testing reports to determine whether penetration tests covered the critical assets and network segments. Review whether automated and manual penetration testing was performed.**		
180	D.1.1	1. Check for the existence of a comprehensive network penetration testing policy and assess the regularity and comprehensiveness of penetration tests.			
181	D.1.2	2. Check the scope of penetration tests covers critical assets and network segments and assess if both automated and manual testing were conducted.			
182	**E**	**Network and Device Configuration Review**			
183	**E.1**	**Device Configuration Review**	**Perform configuration review of network and security devices in accordance with industry standards and security guidelines such CIS benchmark, NIST, etc.**		
184	E.1.1	1. Check the access controls, encryption protocols, and authentication mechanisms for robust network security.			
185	E.1.2	2. Check the firewall rules, intrusion prevention systems, anti-malware and proper network segmentation.			
186	E.1.3	3. Check the VPN configuration and user accesses			

187	E.1.4	4. Check the wireless network configurations, remote management configurations and verify the use of strong, unique passwords and the absence of default credentials.			
188	E.1.5	5. Verify that only necessary services, protocols, and ports are allowed.			
189	E.1.6	6. Assess the use of role-based access controls (RBAC) for administrative access.			
190	E.1.7	7. Check network devices are running the latest firmware or software versions.			
191	E.1.8	8. Review SNMP configurations and ensure they use secure versions (e.g., SNMPv3). Implement strong community strings and restrict access to SNMP management.			
192	E.1.10	10. Verify syslog configurations for logging critical events.			
193	E.1.11	11. Verify network segmentation to contain and minimize the impact of potential breaches. Ensure that VLANs are appropriately configured and isolated.			
194	E.1.12	13. Check port security, Quality of Service (QoS) and Network Time Protocol (NTP) synchronization.			
195	**E.2**	**Network Redundancy**	**Review the network redundancy for single point of failures.** **Review whether the network redundancy tests were performed by organization to check the failover mechanism**		
196	E.2.1	1. Check the implementation of redundancy, failover mechanisms, and secure routing.			

197	**E.3**	**Logging and Monitoring**	**Review whether network logs are maintained and monitored by network operations team. Check for log retention and archival policy**		
198	E.3.1	1. Check for NOC reports			
199	E.3.2	2. Check for log retention and archival policy			
200	E.3.3	3. Review the configuration of Security Information and Event Management (SIEM) tools. Assess the performance and scalability of SIEM solutions to handle the volume of logs generated.			
201	E.3.4	5. Does Devices being used in reverse proxy mode such as WAF,LB have enabled requisite header format for web hosting. Ensure that Sensitive PII data is masked/hashed/encrypted.			
202	**F**	**Application Hosting Configuration Review**			

203	**F.1**	**Hosting Environment Security**	**Review the hosting system security configurations for Applications and critical databases to determine the following: - Adherence to secure hosting standards, encompassing secure protocols, encryption, hosting platform/system access controls, authentication mechanisms, and proper segmentation for hosted applications and databases.** **- Application and Database hosting servers are segregated and access is established through zero trust mechanism.** **- Servers hosting critical databases is access controlled, is not accessible on internet.** **- Hosting systems are integrated with SOC/SIEM solutions and monitored for access and changes.**		
204	F.1.1	1. Check adherence to secure hosting standards, encompassing secure protocols, encryption, hosting platform/system access controls, authentication mechanisms, and proper segmentation for hosted applications.			

205	F.1.2	2. Check that Application and Database hosting servers are segregated and access is established through zero trust mechanism.			
206	F.1.3	3. Check that server hosting critical database / PII information is not accessible on internet. Check that user access to critical database / PII data / underlying servers is restricted to authorized users only. Privilege access is restricted and monitored.			
207	F.1.4	4. Check that Application Server and Critical Database Servers hosting PII information are integrated for security monitoring with SOC / SIEM solution. Check that access and transaction logs are secured and retained.			
208	F.1.5	5. Check that server hosting application and critical database is updated for latest security patches. Check that server hosting application, critical database, middleware and load- balancer etc. is hardened and benchmarked against security standards such as CIS.			
209	**F.2**	**Security Monitoring of Hosting Environment**	**Review whether hosting systems are integrated with SOC/SIEM solutions and monitored for access and changes.** **Review whether effective security monitoring,** **and application isolation in case of virtualization is configured**		
210	F.2.1	1. Check the effectiveness of intrusion detection, monitoring, and logging mechanisms in the hosting environment.			

211	F.2.2	2. Check that hosting servers have antivirus/anti-malware and data loss protection software are installed and security threat signatures/definitions are updated.			
212	F.2.3	3. Check the security monitoring of hosted applications, databases and associated user access to servers / Operation System.			
213	F.2.4	4. Check the use of containerization or virtualization for secure application isolation.			
214	**F.3**	**Security Assurance on Third Party Cloud Service Provider (CSP)**	**In-case of applications and / or critical databases hosted on external / third party cloud service provider (CSP), review the hosting environment security assurance reports based on SOC2 Type 2 Examination issued to auditee organization by CSP, to determine the following:** **- Independent auditor opinion** **- management assertions / statement on CSP security control environment - security control deficiencies** **- user entity controls applicable for security governance and management by user organization / auditee organization**		

215	F.3.1	1. Check the CSP hosting environment SOC2 Type2 report for detailed security controls and their effectiveness status. Enquire with auditee management on controls that are ineffective or qualified by CSP's auditors in the SOC2 Type2 report and assess the compensating controls.			
216	**F.4**	**Backup and System Resilience**	**Review the data backup and archival process.** **Review whether backup testing was performed and its effectiveness**		
217	F.4.1	1. Check the data backup and archival policy and procedures and Check the backup testing reports			
218	**F.5**	**Hosting System Decommissioning / Migration**	**Review the hosting system decommissioning / migration process.** **Determine how the data is securely erased (for decommissioning) / transferred during system migration.**		
219	F.5.1	1. Check for proper disposal and decommissioning processes for deprecated hosting resources / end-of-life servers.			
220	F.5.2	2. Confirm the use of encryption for data in transit (TLS/SSL) and data at rest (disk encryption). Assess the strength of encryption algorithms and key management practices.			
221	F.5.3	4. Review Identity and Access Management (IAM) configurations for users, groups, and roles.			
222	F.5.4	5. Assess access controls and permissions and ensure the use of multi-factor authentication (MFA)..			
223	F.5.5	7. Verify the security configurations of servers and workstations.			

224	F.5.6	8. Assess antivirus/antimalware solutions and their update status and Confirm secure configurations for endpoint protection.			
225	**G**	**Database Security Assessment**	**(including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication)**		
226	**G.1**	**Access control, Authentication and Monitoring**	**Review the access management and monitoring controls, including multi-factor authentication (MFA) mechanism for secure access to critical database.**		
227	G.1.1	1. Check for access controls, encryption, monitoring mechanisms for database security and confirm secure configuration settings, including proper authentication methods and multi-factor authentication.			
228	**G2**	**Database Encryption**	**Review if the PII data information in database is encrypted.**		
229	G.2.1	1. Check the data base encryption configuration for protecting PII data.			

230	**G.3**	**Database Updates and Patch Management Review**	**Review the patch management process and update of security patches on database servers.**		
231	G.3.1	1. Check for regular reviews and updates of the database management system software. Check timely implementation of patches and updates for the database.			
232	**G4**	**Database Activity Monitoring**	**Review whether Database Activity Monitoring (DAM) tool is implemented to monitor user and privilege access to databases. Review the DAM rules to determine whether logics have been implemented to prevent privilege** access escalation attacks.		
233	G.4.1	1. Check for DAM implementation and its rule sets.			
234	**H**	**User Access Controls**	**including (privilege access management) and access reconciliation review**		
235	**H.1**	**User Access Management Policy and Controls**	**Review user access controls, access management policies and mechanism that are implemented for access to applications, databases, hosting environment (operating system), active directory / LDAP, network devices and security equipment.**		

236	H.1.1	1. Check existence and effectiveness of documented user access control policies, user authentication mechanisms and adherence to strong password policies.			
237	H.1.2	2. Check for periodic user access reviews performed by management. Verify if user access were revoked in timely manner for terminated or inactive users.			
238	**H.2**	**Privileged user controls and Segregation of Duties / Roles**	**Review whether the privileged accounts are protected and segregation of duties has been defined.**		
239	H.2.1	1. Check for role-based access controls, use of multi-factor authentication and verify proper segregation of duties and implementation of least privilege principles.			
240	H.2.2	2. Check the implementation of account lockout mechanisms and privileged access controls.			
241	**H.3**	**User Credentials Management**	**Review the management and storage of users credentials.**		
242	H.3.1	1. Check for secure storage, transmission, and recovery of user credentials. Check the password management policy and how it is enforced in system. Check whether user credentials are not stored in clear text.			
243	**I**	**Identity and Access Management (IAM) Controls Review**			

244	**I.1**	**IAM Policy, Procedure and Access controls**	**Review the existence and effectiveness of IAM policy and procedures.** **Review whether IAM, PIM/PAM tool is integrated for applications, databases and other hosting system components. Review whether workflow is defined for IAM tool for user access approval.**		
245	I.1.1	1. Check for integration and use of IAM/PIM/PAM tool for user access management.			
246	I.1.2	2. Check for privileged access management controls, regular policy updates and check documentation, communication, and monitoring of IAM policies and activities.			
247	**I.2**	**IAM Security Controls and Authentication Mechanism**	**Review the authentication mechanism and third-party access controls on IAM tool.**		
248	I.2.1	1. Check for the use of Single Sign-On (SSO) and multi-factor authentication and evaluate encryption methods for IAM data and credentials.			
249	I.2.2	2. Check for IAM controls for third-party access, cloud applications, and integrations.			
250	**J**	**Data Protection Controls Review**	**(inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including “Preventing Data Breaches / Data Leaks [CIAD-2021-0004]”)**		

251	**J.1**	**Data Protection Policies**	**Review the Data Protection Policies and Procedures in place to identify and protect PII / Critical Data in the auditee organization.** **Review if PII Data Flow is documented.** **Review if the Data Protection Impact Assessment (DPIA) has been performed by auditee organization.**		
252	J.1.1	1. Check for Data Protection Policies and Procedures.			
253	J.1.2	2. Check where data flow and data classification has been performed to identify and protect critical / PII data.			
254	J.1.3	3. Check whether data protection impact assessment (DPIA) has been performed to assess the impact to organisation in event of data loss / leakage.			
255	J.1.4	4. Evaluate mechanisms for obtaining user consent for data storage and usage. (as per DPDP Act 2023)			
256	J.1.5	5. Organizations must ensure that individuals provide informed consent for the processing of their personal data. This means individuals should be aware of the purposes for which their data is being processed			
257	**J.2**	**DLP Tools Implementation**	**Review whether DLP tool has been implemented for all critical data assets and systems.**		
258	J.2.1	1. Check for comprehensive coverage of DLP tool implementation. . Check the DLP reports and incidents reports for efficacy of DLP rules.			

259	**J.3**	**Data Storage and Encryption Review**	**Review the data encryption implementation for data at rest (in database) and data in motion (network)**		
260	J.3.1	1. Check for encrypted storage and transmission of critical / personal data / PII data. . Check the encryption and security measures for data transferred to third parties.			
261	J.3.2	3. Ensure that encryption standards used for data storage align with industry best practices and legal requirements. Utilize strong encryption algorithms for both data in transit and data at rest.			
262	J.3.3	5. Review and enforce access controls to restrict unauthorized access to personal data.			
263	J.3.4	6. Implement the principle of least privilege, ensuring individuals have access only to the data necessary for their role.			
264	J.3.5	7. Confirm that personal data is stored in locations compliant with data protection laws. Be aware of restrictions on cross- border data transfers and ensure compliance with those regulations.			
265	J.3.6	8. Review and document data retention policies.			
266	J.3.7	9. Implement procedures for the secure disposal/archival of personal data that is no longer needed.			
267	J.3.8	10. Ensure that Sensitive PII data is masked/hashed/encrypted.			
268	**K**	**Security Operations and Monitoring Review**	**including maintenance of security logs, correlation and analysis**		
269	**K.1**	**Security Operations and Monitoring Policy**	**Review Security Operations Center (SOC) policy and procedures**		

270	K.1.1	1. Check for existence and effectiveness of security operations, monitoring policy, vulnerability management process, and incident response plans.			
271	K.1.2	2. Check if SOC monitors network and endpoint security controls, including privileged user monitoring and check for conduct of incident reports and periodic security drills.			
272	**K.2**	**SOC monitoring for Incidents**	**Review SOC/SIEM coverage for devices integration, log correlations and security incident alert notifications.**		
273	K.2.1	1. Check for SOC/ SIEM utilization for log management and analysis. Check the SOC/ SIEM correlation rules and check if they adequately cover the security requirements.			
274	K.2.2	2. Check for the device coverage and number of devices integrated with the SIEM solution.			
275	**K.3**	**Security Monitoring, Orchestration, and Analytics**	**Review SOC effectiveness and efficiency to detect threats, patterns & anomalies using automation, orchestration, and threat intelligence**		
276	K.3.1	1. Check for the effectiveness of the security operations center (SOC) and use of security automation, orchestration tools, access controls, sensitive data monitoring, and documentation of procedures.			
277	K.3.2	2. Check for integration and availability of threat feeds in SOC. Check if SOC team performs security analytics for anomaly detection.			

278	**L**	**Review of logs, backup and archival data for access to personal data**	**(including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law)**		
279	**L.1**	**Log management and backup policies**	**Review the application transaction and security log management process**		
280	L.1.1	1. Check for existence and effectiveness of application transaction and security logs.			
281	**L.2**	**Log Backup, Retention and Archival**	**Review the log backup/retention and archival process**		
282	L.2.1	1. Check for backup and retention policies and archival procedures.			