REQUEST FOR PROPOSAL (RFP)
FOR

INFORMATION SYSTEM AUDIT OF
BANK'S INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) INFRASTRUCTURE

RFP No : **IB:CO:INSP:ISA 5 / 2019-20**

Indian Bank
Information Systems Audit Cell
Inspection Department, Corporate Office
254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600 014
E-mail: isaudit@indianbank.co.in
Website: www.indianbank.in

SCHEDULE OF EVENTS AND BID DETAILS

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion, should the need arise. Changes to the timeframe will be published in the Bank's website.

RFP Reference	**IB:CO:INSP:ISA: 5 / 2019-20**
Porting of RFP in Bank website	13.03.2020
Last Date for submitting queries (only through email)	20.03.2020 ; 17:00 Hrs
Date of pre-response (pre-bid) Meeting	Date/Time & Venue will be intimated in the Bank's website
Last date and Time for submitting bids	09.04.2020 ; 15:00 Hrs
Date and Time of Opening of bid responses	Will be intimated in the Bank's website
Place of Opening RFP responses	Indian Bank Corporate Office, No.254-260, Avvai Shanmugam Salai, Royapettah, Chennai - 600 014
Cost of RFP Document	Rs 5,000/- (Rupees Five thousand only) The cost is Non-refundable.
Bid Security Guarantee	Rs 200,000/- by way of Bank Guarantee (Rupees Two lakhs only)
Address for communication and submission of response	Assistant General Manager Indian Bank Corporate Office, Inspection Department No.254-260,Avvai Shanmugam Salai, Royapettah, Chennai - 600 014
Contact No.	044-28134536 / 28134468
Email	isaudit@indianbank.co.in

In case scheduled dates fall on a public holiday, the same will be extended to the next working day.

All dates mentioned above are tentative dates and the bidder acknowledges that it cannot hold the Bank responsible for breach of any of the dates.

Non-attendance at the pre-bid meeting or bid opening will not be a cause for disqualification of a bidder.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 - BACKGROUND

Indian Bank is a premier Nationalised Bank with over 2887 Branches and having a business of over Rs. 4,50,000 crores. The Bank is a forerunner in absorption of technology and has many firsts to its credit in implementation of IT in banking. The Bank has overseas presence through Branches in Singapore, Colombo & Jaffna and has reciprocal arrangements with various Foreign Banks across the globe.

Allahabad Bank is another premier Nationalised Bank with over 3400 branches and having a business of over Rs 3,90,000 crores.

With effect from 1st April 2020, Allahabad Bank will be amalgamated in to Indian Bank and hence, this is RFP is proposed for the combined entity (hereinafter referred as "Bank").

Both the Banks -

- have implemented Core Banking Solution,
- have issued Debit Cards, Credit Cards and RuPay cards and
- are offering banking services through Multiple Delivery Channels like ATM (onsite/offsite), BNA, Internet Banking, Mobile Banking, RTGS, SFMS, NEFT, Integrated Treasury & Forex, FI, CTS, UPI, AEPS etc. and more than 60% of the transactions are through Digital Channels.
- partnering various e-governance initiatives of Govt of India and State Governments.
- have been certified with ISO27001:2013 standard for Information Systems & Security processes.

1.2 - PURPOSE

This RFP seeks to engage an Information Systems Audit Firm, which has the capability and experience to conduct a comprehensive Information Systems and Security Audit of Bank's IT infrastructure and Communication Technology (ICT) including IT Governance. Bank seeks to have an external examination of the IT security

- To ward off risks in the IT Domain and to appraise the findings thereof to the Management.
- To determine the effectiveness of planning and oversight of IT Activities
- Evaluating adequacy of operating processes and internal controls
- Determine adequacy of enterprise-wide compliance efforts relating to IT Policies and Internal Control Procedures.
- Identifying areas with deficient Internal Controls and recommend corrective action to address deficiencies.

2. SCOPE OF AUDIT

(for the years 2020-21 and 2021-22)

2.1 - Overview of Scope

The overall scope of Information Systems Audit includes the following:

- The Auditors shall understand the current IT Setup / processes involved in the Bank and the industry prevailing standards, Regulatory guidelines etc.

- The Auditors shall give reasonable assurance to the Top Management explicitly in their audit report, with regard to
  - completeness, effectiveness of the various Policies / procedures / guidelines defined by the Bank from time to time as per guidelines from the regulatory authorities.
  - compliance of all applicable guidelines / recommendations / directions laid down by regulatory authorities like RBI, NPCI, UIDAI, CSITE etc. and ISMS control requirements of ISO/IEC 27001.
  - compliance to various Policies / procedures / guidelines defined by the Bank from time to time.

- IS Audit shall cover the entire gamut of computerized functioning including core banking, e-Delivery Channels, robustness of different functions, such as application systems and subsystems, architecture, infrastructure, network, Logical access control, input, processing and output controls, procedures, data integrity/efficiency, Change Management and effectiveness in implementation of Bank's IT Security Policy & Procedures. This shall include any other new addition/ upgradation in hardware, software, business applications, new deliverables, change in architecture/ Migration during the contract period at Data Centre, DR site, Near-DR, Head Office & Corporate Office Divisions.

- IS Audit shall cover evaluation of the level of compliance on adherence to maintenance of Integrity, Confidentiality, Reliability, Availability and Dependability of information resources, System effectiveness and efficiency, Safeguarding of IT assets, Identification of potential IT risks, timely triggers for IT related risks, adoption of Risk based approach in all areas and Risk Mitigation measures.

- Audit of IT Governance shall cover evaluation of the Bank's strategic and operational alignment with its enterprise's business strategy, ensuring that IT is supporting the Bank's overall goals while measuring IT delivery performance and transparently reporting the results.

2.2 - Audit Period

The proposed I S audit assignments will be for a period of two years. Award of IS Audit assignment will be initially for a period of one year. On satisfactory performance and completion of first year assignment, the same may be extended for another one year.
Bank reserves the right to call for additional information from the IS Auditor at the time of annual review.
The entire process of audit shall be completed within the respective calendar quarter/half year/year, as per the timeline stipulated by the Bank, having regard to the Regulatory and other requirements of the Bank.

2. 3. Scope of Audit

Scope / functional areas to be covered during the proposed audit process have been divided into three verticals as under :

VERTICAL – I - Annual Audit:

a) IT General security Control / Process audit in following locations/Offices:

- Data Center
- Near Disaster Recovery Site
- Disaster Recovery Site
- Information Technology Department / Network Operations /inhouse development
- Digital Banking Department and all e-banking channels (web based and mobile based)
- Payment Gateway
- CTS grids
- ATM Switch /ATM Service Centre / Card Issue
- Credit Card Department
- Call Center
- NEFT / RTGS Cell
- International Division / SWIFT
- Treasury Branch
- Registration authority (RA)
- CPPC/CDPC/FI/MIS/AML/eAudit/HRM Department
- IT Security Operations
- Information System Security Department
- Other departments of Corporate Office / Head Office at Chennai or any other bank's office at any place, where critical application/IT infrastructure is installed or to be installed by the Bank from time to time
- Premises/activities of all third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements, escrow agreements, etc. both at their Primary Site and DR Site
- Minimum of one Specialised branch under each category (like Service Branch, Overseas Branch, MSME, Ind-Retail Branch (IRB), CMS Hub etc.)
- Minimum 10 CBS branches (along with onsite and offsite ATMs / Bunch Note Accepters (BNAs) / including systems rendering various types of services like Passbook printing, Cheque acceptance etc.)

b) Application Security Audit of all applications running in the bank, including new / modified and third party applications, during the period of contract.

c) Source code review of 10 applications as per secure coding practices and as per the requirement of regulatory bodies like RBI CSITE, NPCI, UIDAI, etc.
d) Review of the DR drills conducted by the bank during the contract period.
e) Review of compliance of RBI CSITE advisories & circulars and any other Regulatory guidelines issued during the contract period.
f) Quality Assurance Audit on the functioning of IS Audit functions of the Bank.
g) Review of mitigation status of all the previous audit observations.
h) Submission of Audit Reports with Risk Analysis and asset-wise Recommendations for Risk Mitigation.
i) Two days intensive training to Indian Bank Inspection (Audit) Team.
j) Cost of additional 50 Mandays is to be included in the contract for the purpose of conducting special audits, as and when required by Regulatory Authorities or any other specific audit assignments, as may be required by the Bank from time to time, **in addition to the scope of work covered above**. The bidders have to take up specialised audits as per the requirement of the bank whenever needed, as per the discretion of the bank.

Cost for taking up additional assignments, as and when entrusted by the Bank, may also be indicated separately in the prescribed format, which will be considered for commercial evaluation. However, cost for the same will be paid on actual basis based on the number of assignments completed / mandays utilised. Such assignments will be entrusted on ad-hoc basis, as and when required by the Bank, either in test or in production environment and specific scope of audit for each assignment will be communicated, as and when entrusted.

(Detailed list of setups will be provided at the time of commencement of Audit and setups added during the contract period will be provided on quarterly basis)

VERTICAL – II – VAPT

a) Vulnerability Assessment/ Penetration Testing (VAPT) of Bank's entire ICT infrastructure including Hardware/Servers, Operating System, Database, internal/external/mobile Applications, APIs, Network and Security Devices and Web application security audit / Penetration Testing of all the internal / external facing applications, including third party applications **on half-yearly basis**.
b) VAPT of all critical and external facing / mobile applications and servers, which are interfacing with Bank's internal information, including Bank's website/intranet, **on quarterly basis.**

Cost for taking up additional assignments, as and when entrusted by the Bank, may also be indicated separately in the prescribed format, which will be considered for commercial evaluation. However, cost for the same will be paid on actual basis based on the number of assignments completed / mandays utilised. Such assignments will be entrusted on ad-hoc basis, as and when required by the Bank, either in test or in production environment and specific scope of audit for each assignment will be communicated, as and when entrusted.

(Detailed list of setups will be provided at the time of commencement of Audit and setups added during the contract period will be provided on quarterly basis)

VERTICAL- III – Concurrent Audit

Continuous and Concurrent IS Audit of CO:ITD, DBD and ISSD, including CDC, DR site and NDR, by qualified Auditors who shall be stationed at the CBS Project Office of the Bank.

Scope of the concurrent I S Audit shall cover :

- CO:ITD/DBD – Change management process, Patch Management, Backend updations, Parameter changes, Single sided transactions, Abnormal/Exceptional transaction monitoring process, GL creation/modification, User Management, Log analysis, Remote login, issues pending with vendor, Review of online ticketing, Global process like NPA tracking, updation of Interest Rate, Service charges, TDS, etc.
- Networking – Analysis of Network reports, Analysis of total downtime and business downtime of network due to factors like, power, network equipments, etc.
- Data Centre, Disaster Recovery site and Near Disaster Recovery site– Environmental, Physical / Logical Access controls, Incident Management, Event Management, Change Request Management and Storage and space utilization of various servers, Physical and logical access control, Backup processes, Database Management, DBA activities including parameterisation, Downtime, Synchronisation between DC, DR and Near DR etc.
- Security Operations Centre and ISSD – Applications / tools like BIGFIX, Antivirus / Anti Spyware updation, Rules and policies relating to Firewalls, Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS), Biometric access control, Security Information and Event Management (SIEM) solution, Privileged Identity Management Solution (PIM), Vulnerability Assessment Solution (VAS), Database Access Monitoring Solution (DAM), etc.

The above list is not exhaustive and the Scope of concurrent audit shall cover all the IT related activities of CO:ITD, DBD, ISSD and DC/NDR site on monthly basis and DR site on yearly basis.

Interim IS Audit report for each month has to be submitted to General Manager (I&C) and DH of concerned Department by 10th succeeding month and Final Audit report has to be submitted by 15th of succeeding month with observations /comments on the adequacy of various Information System processes of the Bank.

Cost for taking up additional assignments, as and when entrusted by the Bank, may also be indicated separately in the prescribed format, which will be considered for commercial evaluation. However, cost for the same will be paid on actual basis based on the number of assignments completed / mandays utilised. Such assignments will be entrusted on ad-hoc basis, as and when required by the Bank, either in test or in production environment and specific scope of audit for each assignment will be communicated, as and when entrusted.

2.4. Detailed Scope of Audit

VERTICAL – I - Annual Audit

i) I S audit to cover entire range of computerized functioning including eDelivery Channels & functional areas with special reference to the following, to give assurance with regard to Confidentiality, Integrity and Availability:

- Core Banking (BANCS@24)
- Trade Finance (Exim Bills)
- Financial Inclusion Project
- E-Banking channels including Internet Banking, Mobile Banking, Telebanking applications (Indpay, UPI, etc) and
- Payment systems architecture
- ATM – Switch, Application, Network Security, Interface, Audit Trails, Transmission Security, Authorization Process
- ATM Process - Operational controls, Reconciliation/Functional/Managerial activities, Card Issue, Card / PIN Management cum Security Review, Debit Card Management System, RACS with reference to ATM Cash Management
- E-commerce, Point of Sale (POS), e-Branch-kiosk etc.
- Networking and Aggregation Points
- Treasury operations / SWIFT
- Credit Card Centre
- Anti Money Laundering
- Integrated Call Centre
- M I S
- C M S
- RTGS / NEFT / SFMS
- A S B A
- I T M S
- L O S
- E W S
- Human Resource Management Systems – SAP / Pension / Payroll / P F
- Risk Management – RAM /CAM/ CORE , etc
- Service Branch (in-house clearing software, Cheque Truncation System and other applications)
- Overseas Branches
- Fraud Risk Management Systems (FRMS)
- Corporate Messaging system
- Utility Bills Payment / IMPS / Aadhaar Enabled Payment System (AEPS) / Unified Payment Interface (UPI)
- Interfaces like Micro ATMs, Aadhaar Pay App, CIBIL etc
- Bank's website
- Intranet
- eAudit
- Registration Authority - Digital certificate
- Cyber Roam / Websense Application
- Active Directory Management
- Big Fix Application
- Bio metric authentication systems
- Bank's Enterprise wide Security project (including SOC)
- All other Web Applications and In-house application packages

Note: Any new addition/ up gradation in hardware, software, business applications, new deliverables, change in architecture/Migration during the contract period at various areas of operations involving information systems will also be covered in the audit.

ii) I S audit of Bank's website, intranet, web applications facing internet, in-house applications accessed by Bank's internal as well as external systems, mobile applications, cyber-roam facility provided to staff members, to access the internet.

iii) I S Audit of the Information Systems – Standard applications and legacy applications (either integrated with Core Banking Solution or working as stand-alone) such as Credit Card Centre, Treasury Branch – Credence Treasury Domestic / Forex, Anti Money Laundering, Integrated Call Centre, M I S, RTGS/NEFT, H R M S–SAP, Risk Management – RAM /CAM/ CORE, Fraud Risk Management System, Financial Inclusion application, Corporate messaging system and Active Directory Management, In-house applications and all other aspects of IT environment in the Bank and all IT and IT enabled services as guided by Regulatory bodies like RBI, NPCI, UIDAI etc.

iv) I S Audit / Review of the overall security aspects of the entire Internet Banking / Mobile Banking / Tele-banking ATM Switch / POS Terminal / Payment systems architecture with recommendation for improving the security, if any.

v) I S Audit of Enterprise Network infrastructure/systems/Aggregation Points including Network architecture review, NMS (Network Monitoring system) with thrust on Penetration Testing & Administrative Process.

vi) I S audit of Bank's Enterprise wide Security project including SOC, Intrusion Detection/Prevention System (IDPS), Anti-Virus Management etc to ensure its effectiveness and efficiency in Cyber Security Preparedness.

vii) Audit / Review of the Automated tools deployed by Security Operation Center / CO: ISSD including, Security Information and Event Management (SIEM), Privileged Identity Management Solution (PIM), Vulnerability Assessment Solution (VAS), Database Access Management (DAM), with regard to their implementation, integration, maintenance, effective utilization etc

viii) Audit of capacity management and adequacy of performance tuning of Bank's Information and Communication Technology infrastructure

ix) Audit of processes / procedures involved in Backup, End Of Day (EOD), Start Of Day (SOD) operations, etc., generation of reports, its distribution to branches, availability, consistency, data integrity, completeness of data

x) Security testing of applications running in the bank as on the date of RFP (including CBS) and those newly developed during the audit period.

xi) Code review of applications developed in-house (minimum of 50% in each half year), as per bank's secure coding practices.

xii) Functionality and IS Audit of the ATM Service Centre with regard to reconciliation and settlement within and outside the Bank.

xiii) Systems audit of the Unified payments Interface (UPI) and Indpay mobile application with PCI-DSS / PA DSS testing / Application Security Testing etc., as per NPCI guidelines.

xiv) Audit of Cheque Truncation system/Grid infrastructure including Hardware, Operating System, Database, Application, Network including people and process

xv) Audit of Registration Authority, issue/maintenance/retiring of digital signatures to individuals/servers

xvi) IS Audit of SWIFT operations as per the Swift guidance document, including time synchronization.

xvii) IS Audit of Treasury Branch covering the efficacy and efficiency of the software used, parameter settings, access control, authorisation etc. in safeguarding the IT assets through proper controls & procedures.

xviii) Audit of FI application software Solution, infrastructure and database with particular reference to the process of issue of cards, authentication, and authorization of Micro

ATM devices and process flow/handling of issuer/acquirer transactions and interfacing with UIDAI/NPCI including visit to atleast one village covered under FI.

xix) Audit of IT Governance evaluating the Bank's strategic and operational alignment with its enterprise's business strategy, ensuring that IT is supporting the Bank's overall goals while measuring IT delivery performance and transparently reporting the results.

xx) Audit of Business Continuity Planning (BCP) Policy, Processes / Procedures / Testing relating to various IT setup of the Bank

xxi) Audit of minimum 10 CBS branches (along with onsite and offsite ATMs / BNAs relating to the identified Branch) with focus on critical areas like operating system security, anti-malware controls, maker-checker controls, segregation of duties, rotation of personnel, physical, logical, environmental and network security, review of critical reports (viz. exception reports, etc)/audit trails, BCP policy and testing, User access controls, etc.

xxii) I S Audit and Process Audit of Third party IT environments / service providers / outsourced activities to verify / satisfy about safety & security of information assets of the bank in the hands of third party vendors. IS Audit shall cover all assets belonging to Bank, whether it be data, hardware, software, connectivity, facilities, policies, processes & procedures, HR in so far as it relates to the services provided to Bank, service delivery, processes and procedures followed for procurement and deployment of IS assets for and on behalf of Bank. IS Audit shall audit the services of all service providers to ensure that they adhere to the contracted levels of service set out in the Service Level Agreements entered into / to be entered into with the Bank. IS Audit shall audit the compliances by the service providers to various regulatory and statutory requirements to ensure that Bank is not unduly exposed to any risk on account of acts of commission / omission by them.

xxiii) Product Audit shall include but not limited to, Functionality, Security (Logical access, input/processing/output controls, authorisation controls, Change management, interfaces, etc.), Reporting, log trail, Online Help & Troubleshooting, Controls for fraud/forgery, error handling, emergency / crisis handling, users' feedback mechanism, adherence to Accounting procedures / guidelines/ mandates issued by RBI and other Regulatory bodies.

xxiv) IT General security Control / Process audit shall include the following but not limited to: Audit of various functionalities in the application, Review of controls, Adequacy, generation & availability of Reports for financial, regulatory, statutory, MIS & statistical purposes, Review of Analysis of incidents happened during the contract period and adherence to Operational/Statutory guidelines issued by Regulatory Authorities.

xxv) Review of the DR drills conducted by the bank during the contract period.

xxvi) Review of mitigation status of all the previous audit observations.

xxvii) Two days intensive training to Indian Bank Inspection (Audit) Team. This will provide skills and knowledge on various aspects of IS Audit, IS Security, Threats, attacks & vulnerabilities and technology for protection of Information Assets. It will also discuss configuration and management of security technologies, system hardening, authentication measures, backup processes and others as applicable in banking environment.

VERTICAL – II - VAPT

i) VAPT should be comprehensive, including but not limited to the following: Network Scanning, Port Scanning, System/service identification and scanning, Vulnerability scanning, Malware scanning, Spoofing, Application security testing, OS fingerprinting, Service fingerprinting, Access control mapping, Authorization testing, DoS/DDoS Attacks, Lockout testing, Password cracking, and Cookie security, Functional validations, Network architecture review, Security device configuration review, Network device configuration review, Database security assessment, Web site security assessment, Man in the Middle attack, Man in the browser attack and any other assessments/attacks.

ii) Scan non-production environments actively to identify and address potential problems and after corrective actions have been taken, to ensure that vulnerabilities were actually eliminated.

iii) Penetration Testing should include targeted testing, external testing, internal testing, grey box and black box testing, wherever applicable. The PT functional areas to be taken care of shall include the following, but not limited to: Analysis security vulnerabilities, Investigate Multi Threat Surface, Commercial- Grade Exploits, Vulnerability Assessment Validation, Port Assessing/ Scanning, Configuration and Services, Perimeter Defence Network Penetration Test (internal and external), Host & device Testing, Application Penetration Testing, Client-Side Testing of End Users and Endpoint, Identity Discovery & Password Cracking, Database and Cloud penetration Testing. Latest exploits trend, if any should be brought under assessment during the task is in progress.

iv) Web Application VA/PT Website/ Web-application assessment should be done by following industry standards and as per the open web application security project (OWASP) methodology including but not limited to the following: Cross-Site Scripting (XSS), Injections, Broken authentication and session management, Insecure direct object references, Security misconfigurations, Insecure cryptographic storage, Sensitive data exposure , Failure to restrict URL access, Cross site request forgery, Using known vulnerable components, Insecure Deserialization, XML External Entities and any other attacks, which makes Websites and Web Applications Vulnerable.

v) Mobile application assessment should be done by following industry standards and as per the open web application security project (OWASP) methodology including but not limited to the following: Improper Platform Usage, Insecure Data Storage, Insecure Communication, Insecure Authentication, Insufficient Cryptography, Insecure Authorization, Client Code Quality, Code Tampering, Reverse Engineering, Extraneous Functionality and any other attacks, which makes Mobile Applications vulnerable.

vi) For Existing applications, audit to be followed by compliance audit and for test applications, audit to be followed by compliance audit and after go-live of the product/application, re-audit is to be conducted in the LIVE environment.

vii) Audit should cover

- DC, NDR and DR of the Bank as well as of the vendor, wherever applicable.
- Departments in Corporate Office / Head Office or any other bank's office at any place, where application/IT infrastructure is installed or may be installed.
- Review of mitigation status of all the previous audit observations.

VERTICAL – III - Concurrent Audit

The scope of Concurrent Audit shall include

a) Review of the responsibilities of the business process owners and assess whether these are appropriate to support the policies and goals of the Bank.

b) Assessment of whether the business process owners have the skills, experience and resources necessary to fulfil this role.

c) Review of the information received by the business process owners and to assess whether it is appropriate to enable them to discharge their responsibilities and to monitor compliance with the policies. Information that may be considered appropriate include –

i) Reports of attempted access to the systems supporting business processes and follow-up action taken.

ii) Reports of changes to user access rights, including new users and those whose access rights have been removed.

iii) Reports of the results of business continuity tests and follow-up action taken.

iv) Reports on the results of feasibility studies and tendering processes for systems acquisition.

v) Reports of the results of user acceptance testing of new systems or changes to the existing systems.

vi) Reports on performance against agreed service levels.

vii) Statistics on the availability, number of failures, number of system changes requested and implemented etc.

viii) Status of system changes in progress.

ix) Reports of changes to corporate data dictionary entries.

x) Reports on input control/ process control features.

d) Assessment of the system which produces the above information and its reliability, integrity and potential for management override.

e) Review of the procedures to monitor the external factors, which are relevant to the organization.

f) Review to verify whether all material issues are under active consideration at the appropriate level to avoid the potential material adverse effects of such issues.

g) Compliance to ISMS control requirements of ISO/IEC 27001 as per Information Systems Security Policy of the Bank.

h) Review of mitigation status of previous audit observations.

2.5. Conduct of Audit

2.5.1. Project Management:

The Bank and 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. However, for escalation purpose, details of other persons will also be given.

2.5.2. Conduct of Audit:

The Auditor has to undertake IS Audit in a phased manner as described below:

Phase I	Conduct of IS Audit as per scope, evaluation & submission of preliminary reports of IS Audit findings and discussion on the findings
Phase II	Submission of final reports
Phase III	Compliance review & certification

The activities covered under each Phase are appended below:

PHASE I

a) **Conduct of Information Systems Audit as per the SCOPE OF IS AUDIT**

- The Bank will call upon the audit organisation, on placement of the order, to carry out demonstration and/ or walkthrough, and/or presentation and demonstration of all or specific aspects of the IS Audit at the Bank"s desired location or, for a walkthrough, at a mutually agreed location. All the expenses for the above will be borne by the concerned vendor
- Audit schedule to be provided 7 working days prior to the start of audit along with the name of the auditors who will be conducting the audit. Resumes of the auditors assigned above for the project to be provided to the Bank beforehand and they should be deputed to the assignment only after Bank"s Consent.
- Commencement of IS Audit of IT Setups / offices as per the scope of Audit.
- Execute Vulnerability Assessment/External Attack Penetration testing of the entire network including Internet Banking, Wireless network etc. as per the scope of Audit on the written permission of the Bank and in the presence of Bank"s Officials,
- Analysis of the findings and Guidance for Resolution of the same
- The auditors will be required to use only licensed version of tools, free from any malwares, with prior permission of the Bank, strictly in **"non-destructive"** mode only.

b) **Detailing the Security Gaps**

- Document the security gaps i.e. vulnerability, security flaws, loopholes, etc. observed during the course of review of CBS & other IT infrastructure of the Bank as per the scope of Audit.
- Document recommendations for addressing these security gaps and categorize the identified security gaps based on their criticality, resource/effort requirement to address them.
- Chart a roadmap for the Bank to address these Security gaps and ensure compliance.

c) **Addressing the Security Gaps**

- Guide in Fixing/addressing the Security flaws, gaps, loopholes, shortfalls Vulnerabilities in deployment of applications/systems which can be fixed immediately. If recommendations for risk mitigation /removal could not be implemented as suggested, alternate solutions to be provided.
- Recommend fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure.
- Suggest changes/modifications in the Security Policies and Security Architecture including Network and Applications of the Bank to address the same.

d) ***Submission* of Preliminary Draft Report of IS Audit Findings:-**

- Auditor has to submit a preliminary draft report of the IS Audit findings as per the report format mutually agreed with the Bank.

e) ***Review* & Acceptance of Preliminary Report**

- Auditor is required to discuss the preliminary report findings / observations / recommendations /suggestions with the Bank prior to finalization and acceptance of the same by the Bank.

PHASE II

Final Reports of IS Audit Findings

- Subject to the acceptance of the preliminary report by the Bank, the auditor has to submit the Final report and Certificate for Completion of IS Audit as per the scope of IS Audit.
- Final reports of the IS Audit findings has to be submitted in the following parts :
  - Executive summary
  - Detailed findings / Checklists along with Risk Analysis, duly mapped with the scope of work defined above, for each site, service, system and critical devices.
  - In Depth Analysis of findings /Corrective measures and suggestions
- Acceptance of Final Report by the Bank.

PHASE III

a) *Compliance* Review

- An exercise to review the compliance with the IS audit findings and recommendations will be undertaken by the IS Auditor preferably within **180/90/30 days** in respect of Vertical I/II/III respectively from the date of completion of Phase II. However, the final date for the start of compliance audit will be intimated by the Bank. This exercise would encompass evaluation of the general/overall level of compliance undertaken by the Bank against the shortcomings reported in the IS Audit reports.

b) ***Certification* for Compliance & Final Sign Off**

- On completion of the compliance review process and before final sign off, the vendor will provide the Bank an ISA compliance certificate including Certificate as per RBI guidelines for Internet Banking.

2.6. Deliverables

The deliverables are as under

- The Auditors shall understand the current IT Setup / processes involved in the Bank and the industry prevailing standards, Regulatory guidelines etc.
- Submission of Audit Plan, procedures and methodology for each component of I S audit, Vulnerability Assessment and Penetration Testing of Bank's I C T infrastructure in locations/offices housing various applications as per the scope of audit mentioned in para 1 within two weeks of signing of acceptance of purchase order.
- The audit report should be mapped with the scope of work defined above, for each site, service, system, devices, etc.
- The audit of the web applications shall be in line with compliance to OWASP and/or any other globally accepted Application Security Framework.
- The application security audit report shall contain 'best practices on secure coding' as this will help the application developers of the bank to adhere to the best security practices.
- In case of VAPT, 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 and are updated with latest patches released by the OEM and the latest vulnerabilities notified by Market Intelligence sources. Necessary licenses for tools, required to conduct the Vulnerability Assessment /Penetration Testing/Code Scan/Code Review etc. shall be available with the audit firm.
- Auditors to discuss immediately with the auditee the vulnerabilities/risks identified along with their recommendations/suggestions/ways for mitigating them.
- Auditors shall provide the draft report and discuss with the respective teams/departments before providing the final audit report. The interim report shall provide details of gaps observed, vulnerabilities found and solutions / recommendations (emergency quick fix solutions as well as long term solutions based on industry standards) to address the same with supporting Security/administrator Handbooks. The report shall also include risk categorization and the details of test conducted along with methodology, screen dumps, test cases, etc.
- Auditors to guide the auditee department in rectification of vulnerabilities/ risks identified if any.

- Compliance audit to be conducted to verify rectification of vulnerabilities not only for the observations of the current audit, but also of the previous audit to enable the closure of issues.

- Compliance audit of Servers, web-application and source code is to be conducted along with retesting until full remediation which may involve multiple iterations.

- The reports submitted on Vulnerability assessment and Penetration Testing observations should be for each IP Address/URL and should mention the details of the application audited, physical location, details of the auditee and the nomenclature should be as required by the bank. After full remediation, the hash generated in the live environment shall be made a part of the audit report to preserver integrity/version control of the application.

- Auditors to ensure submission of all audit reports as required in the format acceptable to the Bank. Reasonable assurance for each of the areas mentioned in the scope of audit shall be provided by the Security Auditor explicitly in their reports. Audit report shall be provided to the bank with one report for an asset and the results of the audit of multiple assets shall not be clubbed together. Auditor report shall include Risk Analysis and relevant recommendations to mitigate the risk including references to circulars/documentation. Audit evidences collected and working notes to be submitted as appendix along with the final audit report.

- The entire process of audit and submission of interim report of all areas as per scope/RFP to be completed within three months from the date acceptance of purchase order for Vertical I and II. The final reports after completion of compliance audit pertaining to IS Audit, Vulnerability Assessment and Penetration testing shall be within two months of submission of ATR by the Bank. In respect of quarterly / half yearly audit, the same shall be completed within the first month of each calender / half year. For vertical III, the interim/final audit report for each month is to be submitted within $10^{th}/15^{th}$ of the succeeding month respectively. For adhoc assignments, the audit report is to be submitted within reasonable time as stipulated by the Bank from time to time.

- Presentation to the Top Management of the finding of the Report and to provide assurance to the Top Management of the following:
  - Completeness, effectiveness of the various Policies / procedures / guidelines defined by the Bank from time to time as per guidelines from the regulatory authorities.
  - Compliance to various Policies / procedures / guidelines defined by the Bank from time to time.

- Compliance of guidelines / recommendation / directions laid down by regulatory authorities.

➢ Other deliverables as given in RFP document and its amendment/s.

Bank will, on an ongoing basis, review the performance of the Security Auditor and ensure appropriate action is taken in case any deficiencies were noted therein. For example, system(s)/application(s)/infrastructure that were subjected to audit, ceteris paribus, if found to have been compromised (including instances of near-miss) at a later date, apparently due to vulnerabilities that were not observed/highlighted on timely basis in the audit will qualify as a deficiency in discharge of function by the Security Auditor.

2.7. IS Audit Report :

2.7.1. Audit Report should be submitted separately for monthly/quarterly/half yearly/annual audit assignments and individually for assignments entrusted on adhoc basis.
2.7.2. Broadly the Audit Report should contain observations/recommendations keeping the undernoted points in view:-

➢ Gaps, Deficiencies, Vulnerabilities observed in audit. **Specific observations shall be given for each site, service, application, server, system, devices, etc.** indicating name and address.
➢ Risks associated with gaps, deficiencies, vulnerabilities observed.
➢ Analysis of vulnerabilities and issues of concern.
➢ Recommendations for corrective action.
➢ Category of Risk : Critical/Very High/ High/Medium/ Low.
➢ Summary of audit findings including identification tests, tools used and results of test performed during IS Audit.
➢ Report on audit covering compliance status of the previous IS Audit.
➢ All observations will be thoroughly discussed with process owners before finalization of report.
➢ IS Audit report should be submitted in the following order:
  - Location
  - Domain/Module
  - Hardware
  - Operating Systems
  - Application
➢ Detailed report of network audit including VAPT with recommendations and suggestions.
➢ Detailed report of VAPT of Internet Banking
➢ Audit report shall incorporate a certificate that the report covers every area specified in the scope of BID

2.7.2. As indicated earlier the ISA Reports have to be submitted in two stages Preliminary draft report has to be submitted at the end of Phase I & Final Report during Phase II. Both the sets of reports would comprise of the following sub reports :

2.7.2.i) Executive Summary

An executive summary should form part of the Final Report.

2.7.2.ii) Detailed Findings/Checklists with Risk Analysis

- Detailed findings of the IS Auditor will be brought out in this report, covering in detail all aspects viz.
  - Identification of laws/gaps /vulnerabilities in the systems (specific to equipment/resources indicating name and IP address of the equipment with Office and Department name)
  - Identification of threat sources
  - Identification of Risk
  - Identification of inherent weaknesses
  - Servers/Resources affected with IP Addresses etc.
- Report should classify the observations into Critical /Non Critical category and assess the category of Risk Implication as Very High / High / Medium / Low Risk based on the impact.
- The various checklist formats, designed and used for conducting the IS Audit as per the scope, should also be included in the report separately for Servers (different for different OS), DBMS, Network equipment, security equipment etc., so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed by the Bank.
- The reports should be substantiated with the help of snap shots/evidences /documents etc. from where the observations were made.
- For continuous audit, the observations are to be submitted on a monthly basis and exceptions, if any, are to be reported immediately. This reporting shall not be taken into account while arriving at the completion of Phase I.

2.7.2.iii) In Depth Analysis of findings /Corrective measures & suggestions

- Findings of the entire IS Audit process should be critically analyzed and controls should be suggested as corrective /preventive measures for strengthening / safeguarding the IT assets of the Bank against existing and future threats in the short /long term.
- Report should contain suggestions/recommendations for improvement in the systems wherever required.
- If recommendations for risk mitigation /removal could not be implemented as suggested, alternate solutions to be provided.
- Also, if the formal procedures are not in place for any activity, the process and associated risks may be evaluated and recommendations be given for improvement as per the best practices.

2.7.3. Documentation Format

- All documents shall be handed over in **three copies**, signed, legible, neatly and robustly bound on A-4 size good-quality paper.
- All documents shall be in plain English.
- Soft copies of all the documents properly encrypted in MS Word / PDF format and audit observations in MS Excel format shall also to be submitted along with the hard copies.

3. INSTRUCTIONS TO THE BIDDERS

3.1 GENERAL INSTRUCTIONS :

The bidder is expected to read the instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.

The bidder, 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 recipient or to any of their authorized officer(s), including those which are provided by the Bank on its web-site.

The bidder has to submit the Commercial Bid for any one or all the verticals – I (ICT audit), II (VAPT) and III (concurrent audit). A bidder can bid for all the three verticals or any one or two verticals. Non-participation in all the three bids will not be a cause for disqualification of a bidder but participation in any one of the vertical is compulsory.

3.2 TWO STAGE BIDDING PROCESS :

The response to the present tender will be submitted in two parts:

- Part A containing the General Terms and Conditions including Compliance to Scope of Work for each of the verticals and
- Part B containing the Commercial Bid for each of the verticals.

The bidder will have to submit Part A and Part B portion of the Bids separately in sealed envelopes, duly super-scribing

- **"Information Systems Audit – Bids – Part A Technical Bid"** and
- **"Information Systems Audit – Bids – Part B Commercial Bid – Vertical No-..."**

respectively.

No column shall be left blank or altered. Part-B should be duly filled in, signed and kept in a separate sealed envelope. In case the bidder quotes for multiple verticals, separate Part-B to be filled for EACH OF THE VERTICAL and should be kept in separate envelopes duly specifying the VERTICAL NUMBER and NAME on the cover of the envelope.

All the sealed covers should be put in a sealed outer cover envelope and outer cover should bear the title **"Information Systems Audit-BID-Due for submission on or before 09.04.2020 at 3.00 pm".** All the pages of both Part-A and Part-B of the bid should be signed by Authorised Signatory of the Bidding firm.

PART A of the Bid shall NOT contain any pricing or commercial information at all. In the first stage, only Part A of the bids will be opened and evaluated. Those bidders satisfying the requirements as determined by the Bank and accepting the terms and conditions of this document shall be short-listed.

Under the second stage, the Commercial Proposals (Part B) of only those bidders, who have been short listed as above, will be opened in the presence of their authorized representatives. The bidder should arrange for a presentation on IS Audit Methodology and approaches to be adopted and the capabilities of the firm to the accomplishment of the tasks assigned before opening of the bid.

3.2. a. PART A- TECHNICAL BID

Part A of the Bid shall contain the Bidders information as per the "List of the Documents to be submitted by the Bidders" under Para 6.

3.2. b. PART B COMMERCIAL BID

Part B of the Bid shall contain Commercial offer **for each of the vertical** (as per the prescribed format) in separate sealed cover.

It is mandatory to provide the functional & technical details in the exact format as given in the RFP. The offer may not be evaluated by Bank in case of non-adherence to the format or partial submission of technical details.

If required by the Bank, the bidder shall arrange for a presentation on IS Audit Methodology and approaches to be adopted and the capabilities of the firm to the accomplishment of the tasks assigned before opening of the bid.

3.3 – SUBMISSION OF COMMERCIAL BID (CB):

The Commercial Offer should be submitted on an all-inclusive cost basis and Bank will not pay/reimburse any other charges including travelling expenses / visit charges / hotel stay for any travelling/ training undertaken by the Bidder's staff / personnel throughout the period of contract.

3.4 – BID PROCESS TIME FRAME :

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion should the need arise. Changes to the timeframe will be relayed to the affected Respondents during the process.

Description	Norms
Cost of RFP Document	Rs.5,000/-
EMD (Earnest Money Deposit)	Rs.200,000/-
Date of issue of Tender Notification	13.03.2020
Last date and time of receiving pre-bid queries in writing / thru email to isaudit@indianbank.co.in	20.03.2020
Date of Pre-Bid meeting	Will be intimated in the Bank's website
Last date of Bid Submission	09.04.2020
Commercial Bid Opening date	Will be intimated in the Bank's website

* All dates mentioned above are tentative dates and the bidder acknowledges that it cannot hold the Bank responsible for breach of any of the dates.

3.5. PRE-BID MEETING:

A pre-bid meeting will be conducted and date and venue for the same will be ported in the Bank's website. The purpose of the pre-bid meeting will be to clarify the doubts of the bidders, if any.

In case the probable bidder wants to participate in the Pre-bid Meeting to be held on the date specified by the Bank, they should register themselves with the Bank one day in advance. Only those Bidders or their Representatives (Maximum 2 persons) who have registered with the Bank will be allowed to participate in the pre-bid meeting.

The text of the questions raised (without identifying the source of enquiry) and the responses given, together with amendment(s) to the bid document, if any, will be mailed to all the bidders.

3.6. AMENDMENT OF BIDDING DOCUMENTS

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 requested by a prospective bidder(s), may modify the bidding document by amendment(s).

All prospective bidders will be communicated of the details of amendments and clarifications, allowing atleast 3 days' time prior to the last date for receipt of bids. Such amendments/clarifications shall be binding on all the bidders and signed copy of the amended document should form part of the Technical Bid.

Bank reserves the right to rescind / cancel the tender process at any time, or reissue this tender at its discretion by notifying in Bank's website, without thereby incurring any liabilities to the affected Audit Organization(s). Reasons for cancellation / reissue, as determined by the Bank in its sole discretion include but are not limited to, the following:

- Services Contemplated are no longer required or not required immediately
- Scope of work was not adequately or clearly defined due to unforeseen circumstances and/or factors and/or new developments
- The assignment is not in the best interest of the Bank
- Any other reason

3.7. COST OF RFP DOCUMENT

Applicants wanting to participate in the tender process should apply within the specified date/time along with a Demand Draft (DD) for Rs. 5,000/- (Rupees Five Thousand Only - non-refundable) in favour of Indian Bank payable at Chennai.

RFP response submitted without the Demand Draft shall not be considered except in the following cases:

- In line with extant Government guidelines, Micro and Small Enterprises are exempted from payment of cost of RFP document subject to submission of documentary proof for having registered with any of bodies specified by Ministry of Micro, Small and Medium Enterprises.
- Applicants who have already participated in the EOI process of the Bank, floated for empanelment of IS Auditors in Aug/Dec 2019 and paid the tender fee of Rs 5,000/- are exempted from payment of tender fee for this RFP process.
- Such Applicants who have submitted DD for attending pre bid meeting need not submit the DD for tender fee again, along with RFP Document.

3.8. BID SECURITY (EARNEST MONEY DEPOSIT)

The bidder shall furnish, as part of their bid, a bid security in the form of a bank guarantee issued by a scheduled commercial bank, in the form provided in the bidding documents for a sum of Rs. 2,00,000/- (Rupees Two Lakhs only) and valid for One Hundred and Twenty days (i.e. Bid validity 90 days + 30 days = 120 days) from the last date for submission of bid. Bank may seek extension of Bank Guarantee, if required.

Unsuccessful bidders' bid security will be discharged or returned after the expiration of the period of bid validity prescribed by the bank or after issuing purchase order to the successful L1 bidder.

The successful bidder's bid security will be discharged upon the bidders signing the contract and furnishing the performance security.

The bidder will forfeit the bid security,

a. If a bidder withdraws its bid during the period of bid validity specified by the bidder on the bid form.

Or

b. in the case of a successful bidder, if the bidder fails to sign the contract or to furnish the performance security.

3.9. AUTHORIZATION TO BID

Responses submitted by a Bidder to this RFP (including response to functional and technical requirements) represent a firm offer to contract on the terms and conditions described in the Tender document. The proposal shall be made in the legal name of the Bidder and shall 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.

3.10. LANGUAGE OF BIDS

All bids and supporting documentation shall be submitted in English.

3.11. BID CURRENCY

All costs and charges related to the bid shall be expressed in Indian Rupees.

3.12. PERIOD OF BID VALIDITY

The Bids shall remain valid for a period of 90 days from the closing date for submission of the bid. A bid valid for a shorter period shall be rejected by the bank as non-responsive. Bids must clearly state the validity of the bid and its explicit expiration date. Bank may seek the extension of bid validity, if required.

3.13. BIDDING

The cost of bidding and submission of tender documents is entirely the responsibility of bidders, regardless of the conduct or outcome of the tendering process.

3.14. BID SUBMISSION

Bids duly sealed should be delivered **before 15.00 hours on or before 09/04/2020.** Bids may be sent by registered post or hand delivered so as to be received at the following address:

The Assistant General Manager,
Indian Bank Corporate Office
Expenditure Department
254-260 Avvai Shanmugam Salai
Royapettah, Chennai 600 014
Website: www.indianbank.in
Phone: 2813 4536, 2813 4468
E-mail: isaudit@indianbank.co.in

Bank is not responsible for non-receipt of bids within the specified date and time due to any reason including postal delays or holidays.

In the event of the specified date for the submission of bids, being declared a holiday for the bank, the bids will be received up to the appointed time on the next working day.

The bank may, at its discretion, extend this deadline for the submission of bids by amending the bid documents, in which case all rights and obligations of the bank and bidders previously subject to the deadline mentioned above will thereafter be subject to the deadline as extended.

3.15. ACCEPTANCE OF BIDS

Last date for submission of bids is 15:00 hours on 09/04/2020. Bids received after 15.00 Hrs on will not be accepted under any circumstances.

The envelope containing Part A portion of the bids will be opened immediately thereafter at 15:30 hours on 09/04/2020 in the presence of bidders. All bidders are requested to be present.

The bidders' names, bid modifications or withdrawals and the presence or absence of the requisite bid security and such other details as the bank, at its discretion, may consider appropriate, will be announced at the bid opening. No bid shall be rejected at bid opening, except late bids, which shall be returned unopened to the bidder.

Selected bidders will be communicated of the date of opening of the commercial offer to enable them to send their representative in whose presence the bid will be opened.

3.16. EVALUATION AND COMPARISON OF BIDS

General Evaluation

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.
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 annual IS audit/VAPT of Indian Bank and/or Allahabad Bank will not be considered for Vertical I and II in line with RBI guidelines on rotation of auditors.

Technical Evaluation

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. 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).

Commercial Evaluation

a) Bank will open Part II (Commercial) of the quote after evaluation of Part I after giving due notice to the technically qualified bidders.

b) The comparison of prices among the bidders shall be based on the total price quoted covering the entire scope of work for EACH OF THE VERTICAL as per the Tender documents, inclusive of all cost/charges and exclusive of all applicable taxes.

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

d) Bidder whose quote is the least for each of the vertical, shall be treated as the successful bidder for the respective VERTICAL and shall be issued Work Order to the address provided by the audit organization at the time of quotation.

Bank reserves the right to

- 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.
- 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.

- accept or reject any or all bids without assigning any reason thereof and 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.
- 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.
- alter the requirements, in part or whole, during the RFP process, and without re-issuing the RFP.
- 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.

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

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).

The calling for quote does not confer any right on the bidder for being awarded any work order.

3.17. CLARIFICATION OF BIDS

During the scrutiny, evaluation and comparison of the offers, the bank may, at its discretion, seek clarification from some or all the bidders. The request for clarification and the response shall be in writing/email and no change in the substance of the bid shall be sought, offered or permitted.

3.18. LIABILITIES OF BANK

This RFP is not an offer by Bank, but an invitation for bidder responses. 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.

3.19. 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, interalia 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.

3.20. BID PRICING INFORMATION

By submitting a signed bid, the Bidder certifies that "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. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP. No attempt by the Bidder, to induce any other bidder to submit or not to submit a bid for restricting competition, has occurred."

3.21. NEGOTIATION

The Bank reserves the right to further negotiate on the price offered, with the L1 vendor, if the price quoted is found unreasonable or in any exceptional circumstances.

3.22. POST QUALIFICATION

In the absence of pre-qualifications, the Bank will determine to its satisfaction whether the Bidder selected is qualified to perform the contract.
The determination will take into account the Bidder's financial and technical capabilities. It will be based upon an examination of the documentary evidences of the Bidder's qualifications submitted by the Bidder, as well as such other information as the Bank deems necessary and appropriate, including details of experience and records of past performance.

3.23. NOTIFICATION OF AWARD

The acceptance of a tender, subject to contract, will be communicated in writing at the address supplied for the bidder in the tender response. Any change of address of the Bidder, should therefore be promptly notified to Assistant General Manager, Information Systems Audit Cell, Inspection Department, Indian Bank, Corporate Office, 254-260 Avvai Shanmugham Salai, Royapettah, Chennai – 600 014, Tamil Nadu. Contact phone No: 044- 28134536; 28134468 email-id – **isaudit@indianbank.co.in**

3.24. AWARDING OF CONTRACT AND SIGNING OF CONTRACT

After the Evaluation Process as detailed under para 3.16 of the RFP, the successful bidder will be issued Work Order by the Inspection Department of the Bank, separately for each vertical specifying both the Fixed Contract price and Rate Contract price. The Work Order will be initially for a period one year, renewable at the discretion of the Bank for one more year.

Acceptance of Work Order/Rate Contract Order should be submitted within 7 working days of Work Order along-with authorisation letter.
Within fifteen (15) days of Work Order, the successful bidder shall sign the contract and submit Performance Guarantee covering the period of contract, to the Bank.

If for any reason L1 bidder backs out after issuance of work order/rate contract order or at the time of finalization of the contract or gets disqualified on detection of wrong or misleading information in the proposal or the work order issued to the L1 bidder does not get executed in part / full, the bid security of the bidder shall be forfeited and Bank shall invoke the bank guarantee and blacklist the bidder for a period of one year. Further, Bank also reserves the right to select the next ranked bidder in such circumstances.

3.25. OTHER TERMS AND CONDITIONS

i. Bank reserves the right to

- amend / alter/ modify any/ some/ all of the requirements, as it may deem necessary either at its own initiative or in response to clarification sought by interested Applicants and notify the same on its website before the last date for submission of response under this RFP. All such amendments shall be binding on the Applicants.
- modify or relax the eligibility criteria at any time, without assigning any reason, whatsoever.
- change the dates mentioned in this RFP document, which will be notified on the Bank's website.
- seek more information in due course, if considered necessary.
- waive any minor informality, non-conformity, or irregularity in a bid which does not constitute a material deviation.

ii. The Audit organizations, 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 recipient or to any of their authorized officer(s), including those which are provided by the Bank on its web-site.

iii. Any additional or different terms and conditions proposed by the bidder would be rejected unless expressly assented to in writing by the bank.

iv. The information provided by the Audit organizations in response to this RFP document will become the property of the Bank and will not be returned.

v. Bank will not be liable for any costs incurred by the applicant in the preparation of the response to this RFP.

vi. Bank reserves the absolute right to reject the bid if it is not in accordance with its requirements and no further correspondence, whatsoever, will be entertained by the Bank in the matter.

vii. The bidder shall indemnify Bank against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the goods, software(s), hardware(s) or any part thereof in India and abroad.

viii. 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 services 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.

ix. The bidder shall submit a non-disclosure agreement on behalf of the bidder and in the individual capacity of all the persons involved.

x. Subject to any law to the contrary and to the maximum extent permitted by law, Bank and its Directors, Officers, Employees, Contractors, Agents, and Advisors disclaim all liability from any loss or damage suffered by any person acting or refraining from acting because of any information contained in this tender document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, default, lack of care or misrepresentation on the part of Bank or any of its Directors, Officers, Employees, Contractors, Agents or Advisors.

xi. The selected IS Auditor shall have to complete the assigned jobs within the time limits agreed upon with the Bank at the time assigning the job.

xii. The invitation for RFP and/or allocation of assignments/jobs will be at the sole discretion of the Bank. It is also to be understood and agreed by the Audit Organization(s) that decision of the Bank regarding selection of the Audit Organization(s) for sending invitation for RFP and allocation of assignments during contract period shall be final and binding on all concerned. No communication in this regard, verbal or written, will be entertained.

xiii. Bank reserves the right to limit the number of audits that can be concurrently executed by the IS Auditor for the Bank. The decision of the Bank will be final and binding on the selected audit organizations.

4. CONDITIONS OF CONTRACT

1 ACCEPTANCE OF WORK ORDER

1.1 The successful bidder shall sign; affix official stamp and date on the duplicate copy of the Work Order and return it to the bank as a token of having accepted the terms and conditions of the purchase order. This bid together with notification of award from the Bank will constitute a binding contract.

1.2 Power of Attorney authorizing the representative to sign the documents to be produced as required.

2 SIGNING OF CONTRACT

2.1 The successful bidder(s) shall be required to enter into a contract with Indian Bank, within 15 days of the award of the tender or within such extended period as may be specified by **Deputy General Manager, Information Systems Audit Cell, Indian Bank, Corporate Office, Inspection Department, 254-260 Avvai Shanmugham Salai, Royapettah, Chennai – 600014, Tamil Nadu,** on the basis of the Tender Document, the Tender/bid and the letter of acceptance submitted by the successful bidder, and such other terms and conditions, as may be determined by the Bank to be necessary for the due performance of the work.

3 SUBJECT OF THE CONTRACT

3.1 The IS Auditor shall provide IS Audit services to the Bank's requirement as set out in the request for Proposal issued by the Bank and Commercial Proposal issued by the IS Auditor and other services as per the terms and conditions of Agreement entered with the Bank. Wherever there is a conflict between the documents mentioned herein, the following order of precedence shall apply as appearing herein below,

i. Agreements including all its Schedules entered with the Bank.

ii. Work Order issued by the Bank in favor of the IS Auditor

iii. Request for Proposal from the Bank.

iv. Any subsequent amendment/clarification from the Bank in respect of RFP.

4 CHANGE ORDERS

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

a) the place of audit

b) the Services/deliverables to be provided by the IS Auditor; and / or

c) the substitution of new Services from the IS Auditor. When such substitution is requested by the Bank, the IS Auditor shall notify the Bank in writing within 15 days of its decision to accept or reject the proposed Change Order; and / or

4.2 If any such change causes an increase or decrease in the cost of, or the time required for, the IS Auditor's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule or both in consultation with the IS Auditor and the Contract shall accordingly be amended. Any claims by the IS Auditor for adjustment under this clause must be asserted within fifteen (15) days from the date of the IS Auditor's receipt of the Bank's change order. If the parties cannot agree on an equitable adjustment, the Change Order will not be implemented.

4.3 For any fresh requirement not envisaged in the Offer document, change orders will be issued and payment will be made on mutually agreed terms.

5 CONTRACT PERIOD

5.1 The award of the I S audit assignment will initially be for a period of one year and on satisfactory performance and on completion of the compliance audit for the first year, audit assignment may be extended for another one year at the sole discretion of the Bank.

5.2 The audit assignment is further extendable / renewable at the sole option of the Bank on mutually agreed terms.

5.3 Bank reserves the right to call for additional information from the I S auditor at the time of annual review.

5.4 The entire process of audit shall be completed within the respective calendar quarter/half year/year, as per the timeline stipulated by the Bank, having regard to the Regulatory and other requirements of the Bank.

6 PERFORMANCE SECURITY

6.1 Within 15 days of issue of Work Order, the Auditor shall furnish a Performance Security equivalent to 10% of the Contract Amount or Rupees Two lakhs (Rs.2,00,000 only), whichever is higher in the form of a Performance Bank Guarantee issued by a Scheduled Commercial Bank located in India, valid for the period of contract (with further one month of claim period), in the format prescribed.

6.2 The proceeds of the Performance Security shall be payable to the Bank as compensation for any loss resulting from the Auditor's failure to complete its obligations under the Contract.

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

7 PAYMENT TERMS

7.1 Payments for the job of Information System Auditor for Vertical I and II will be milestone payments after completion of each assignment.

10%	Of the IS Audit Service Provider's fees after two weeks of commencement of the audit work and on submission of audit plan/procedures and methodology covering all the points as per Scope of Work for IS Audit
25%	of the IS Audit Service Provider's fees on submission of Interim report
25%	of the IS Audit Service Provider's fees on submission of final report
25%	On submission of final review Audit (compliance audit) report covering all the points as per the Scope of Work.
15%	On final Sign-off

7.2 Payments for the job of Information System Auditor for Vertical III will be milestone payments based on billing after the completion of assignment for each quarter.

All payments will be made in arrears on submission of invoice, as per the above mentioned payment schedule.

8 IS AUDITOR'S OFFER

8.1 The IS Auditor's bid submitted in response to this RFP and subsequent Offers submitted in response to any queries by the Bank shall form part of the Contract.

9 IS AUDITOR'S OBLIGATIONS

9.1 The IS Auditor is responsible for, and obligated to conduct all contracted activities with due care and diligence, in accordance with the Contract, and using state-of-the-art methods and economic principles, and exercising all reasonable means to achieve the performance specified in the Contract.

9.2 The IS Auditor is obliged to work closely with the Bank's Co-ordinator(s) and staff and act within the scope of audit. The IS Auditor is responsible for managing the activities of its personnel, and will hold itself responsible for any misdemeanours.

9.3 The IS Auditor shall appoint an experienced Representative to manage its performance of the Contract within 30 days from the date of signing of the contract. The Representative shall be authorised to accept orders and notices on behalf of the IS Auditor, and to generate notices and commit the IS Auditor to specific courses of action within the scope of the Contract. The Representative may be replaced only with the prior written consent of the Bank.

9.4 The IS Auditor shall develop the final Project Plan based on Contract requirements, to be submitted to the Bank for review and approval within 15 days from the date of the Contract, with all reasonable and necessary input from the Bank. The Project Plan shall include the following: Definition of project implementation tasks, Acceptance and Service deliverables and milestones;

9.5 The IS Auditor shall complete the IS Audit and deliver the relevant reports in accordance with Contract requirements (as may be further elaborated in the Project Plan), or such schedule and specification changes as the IS Auditor may be entitled to.

9.6 The IS Auditors shall undertake to comply with all the prevailing laws and regulations in India while undertaking the assignment for the Bank.

9.7 Compliance to regulations of reserve bank of India/other regulatory agencies – The Auditors will also undertake to comply with all the requirements of the guidelines of Reserve Bank of India or other appropriate agencies as regards Information Systems Security Standards issued from time to time.

9.8 Performance of the Contract can be treated as complete only after the Bank has received successfully all of the Deliverables and Services as per the terms of the Contract.

9.9 The IS Auditors shall undertake to intimate the Bank immediately about any change/development in their organization, during the period of contract, relating to the requirements of this tender, including but not limited to change in constitution, professional certifications and availability of professional resources.

9.10 The IS Auditors shall undertake to inform Inspection Department of the Bank, before undertaking any other assignment /service to the Bank (other than those covered in this tender) during the validity of the contract.

9.11 The IS Auditors shall undertake to submit their annual audited balance sheet to the Bank during the validity of the contract.

9.12 Bank reserves the right to inform IBA/GOI/RBI in case any major vulnerability is noticed after Security Audit within 6 months from the date of security audit.

10 TECHNICAL COMPETENCE

10.1 The bidder shall provide the names of the persons likely to be involved in the audit along with their technical qualifications acquired to prove that the firm possesses the required technical expertise to conduct the audit. The successful bidder after intimation from the Bank regarding having been selected shall provide as proof Xerox copies/soft copies of the personnel involved in the audit for possessing the valid technical qualification.

10.2 Only persons having CISA/CISM/CISSP/GIAC(SANS)/CEH/OSCP/BS7799/ISO 27001 qualifications and with adequate experience will be utilized by the IS Audit firm for audit. Franchise of I S Auditors will not be permitted under any circumstances.

10.3 Only licensed versions of tools to be used for Vulnerability Assessment/Penetration Testing and the auditors to confirm that there would not be any business disruption due to application of such tools. The details of the tools being used should be submitted to the Bank for prior approval.

10.4 The successful bidder shall ensure adherence to applicable codes of conduct and auditing standards with due professional care.

11 CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

11.1 As the successful bidder(s) will have access to the data/information of the bank while auditing the security, bank will require the bidder(s) and their representatives to sign a confidentiality/non-disclosure agreement undertaking not to disclose or part with any information relating to the bank and its data to any person or persons, as may come into possession of the bidder(s) during course of the I S Audit. The bidder shall also give a declaration stating that he does not have any vested interest in applying for this audit. They are also prohibited from transmitting any information through personal email IDs and cloud storage. The successful bidder should ensure removal of any data/ information of the bank after the completion of the audit period, shall give a commitment to the effect, prior to the commencement of the audit and a confirmation immediately after removal of the same.

11.2 The Non Disclosure Agreement (NDA) has to be executed by the firm as well as individually by the auditors performing the Audit in the format as required by the Bank, on Non-judicial stamp paper of appropriate value.

12 DELAYS IN THE IS AUDITOR'S PERFORMANCE

12.1 The Information System Auditor must strictly adhere to the audit schedule, as specified in the Contract, executed between the bank and the Information System

Auditor, pursuant hereto, for performance of the obligations arising out of the contract and any delay will enable the Bank to resort to any or all of the following:

(a) Claiming Liquidated Damages
(b) Termination of the agreement fully or partly

12.2 If at any time during performance of the Contract, the IS Auditor should encounter conditions impeding timely delivery of the Systems and/or performance of Services, the IS Auditor shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). After receipt of the IS Auditor's notice, the Bank shall evaluate the situation and may at its discretion extend the IS Auditor's time for performance in which case the extension shall be ratified by the parties by amendment of the Contract.

12.3 A delay by the IS Auditor in the performance of its delivery obligations due to reasons solely and directly attributable to the IS Auditor alone and that was in no way contributed to by any act or omission of the Bank or any event of force majeure shall render the IS Auditor liable to the imposition of liquidated damages, unless an extension of time is agreed upon without the application of liquidated damages.

13 ASSIGNMENT AND SUB CONTRACTING

13.1 The IS Auditor shall not assign, in whole or in part, its obligations to perform or right to receive payments under any Contract entered with the Bank.

13.2 The IS Auditor shall not franchise or subcontract or delegate or permit anyone other than their personnel to perform any of the work, service or other performance required under the contract without the prior written consent of the Bank.

13.3 All members of the proposed audit team should be employees on IS Auditor's pay rolls. No part of the engagement shall be outsourced by the IS Auditor to third party.

14 EMPLOYEES

14.1 During the contract period and for a period of three years thereafter, both the Bank and the IS Auditor shall refrain from canvassing each other's employees engaged in the performance of the Contract with a view to offering employment.

14.2 Subject to provisions contained in Clause 13 herein, the IS Auditor has to submit attendance, salary, appointment letters, compliance of all statutory requirements, etc. of all the employees working on Bank's premises as Onsite Resource.

14.3 The IS Auditor shall be required to submit satisfactory documentary evidence for carrying out a background check on the personnel being engaged in audit assignment for the Bank and the personnel should submit Non-Disclosure Agreements prior to their deployment.

14.4 Further, IS Auditor has to undertake not to deploy any professional, who was in the services of the Bank in the last 36 months prior to the date of accepting any audit assignment from the Bank.

14.5 The relationship between the Bank and the IS Auditor is on principal-to-principal basis. Nothing contained herein shall be deemed to create any association, partnership, joint venture or relationship of principal and agent or master and servant or employer and employee between the parties themselves and its employees 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.

15 TAXES AND DUTIES

15.1 The price charged by the Information System Auditor for the services performed shall not vary from the contracted schedule of fees. Taxes as applicable will be deducted from the fees, as per prevailing rules on the date of payments.

15.2 The IS Auditor is responsible for all taxes levied in connection with performances of Services.

16 USE OF CONTRACT DOCUMENTS AND INFORMATION

16.1 The Information System Auditors shall not, without the Bank's prior written consent, make use of any document or information except for purposes of performing the Contract.

16.2 The Information System Auditor shall not, without the Bank's written consent, disclose the Contract or any provision thereof, or any specification or information furnished by or on behalf of the Bank in connection therewith, to any person(s) other than a person(s) employed by the Information Security Audit or in the performance of the Contract. Disclosure to any such employed person(s) shall be made in confidence against Non-disclosure agreements completed prior to disclosure and disclosure shall extend only so far, as may be necessary for purpose of such performance.

16.3 Any document, other than the Contract itself, shall remain the property of the Bank and all copies thereof shall be returned to the Bank on termination of the Contract.

16.4 Any publicity given pursuant to permission given by the Bank shall be subject to the confidentiality requirements as well as within the express authority granted under such permission in writing.

16.5 These provisions shall be applicable for a period of one year after termination of the Contract.

17 INDEMNIFICATION

17.1 The Information System Auditor shall, at their own expense, defend and indemnify the Bank against all actions, proceedings, claims, suits, damages and any other expenses due to loss of data/damage to data arising as a consequence of any negligence during Information System Audit and/or for any other causes attributable to the Information System Auditor. The Information System Auditor shall also indemnify the Bank against all third-party claims of infringement of patent, trademark

or industrial design rights arising from use of the services or any part thereof without any limitation.

18 TERMINATION FOR DEFAULT BY THE BANK

18.1 The Bank, without prejudice to any other remedy for breach of contract, by thirty (30) days advance written notice of default sent to the IS Auditor, may terminate the Contract in whole or in part (if the said default is not cured within the said period of thirty days):

a. if the IS Auditor fails to deliver any or all of the services as stipulated in the contract within the period(s) specified in the Contract, or within any extension thereof granted by the Bank; or

b. if the IS Auditor fails to perform the obligation(s) under the Contract as per the required standards

c. If the IS Auditor, in the judgement of the Bank has engaged in corrupt or fraudulent practices

d. any system(s)/applications(s)/infrastructure that was subjected to VA/PT by the Auditor, ceteris paribus, is found to have been compromised (including instances of near-miss) at a later date, apparently due to vulnerabilities that were not observed/highlighted on timely basis in the audit report.

The above list is not exhaustive and will include any other reasons which may be viewed as detrimental to the interest of the Bank, at the sole discretion of the Bank.

18.2 The IS Auditor shall be entitled to be paid the Contract Price attributable to the portion of the Services executed as at the date of termination.

'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 selection 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.

19 TERMINATION FOR DEFAULT BY THE IS AUDITOR

19.1 The IS Auditor, without prejudice to any other rights or remedies it may possess, may terminate the Contract forthwith in the following circumstance by giving a 30 days notice of termination and its reasons therefor to the Bank.

- if the Bank commits any breach of the terms of the Contract and the said breach has not been cured even after 30 days of the IS Auditor sending a notice to the Bank requesting it to cure the said breach.

19.2 If the contract is terminated by the IS Auditor in terms of this Clause, the IS Auditor shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination and the payment that would become due on completion of the stage encompassing the termination.

19.3 In the event of IS Auditor terminating the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, the Services similar to those undelivered, and the IS Auditor shall be liable to the Bank for any excess costs for such similar services. However, the IS Auditor shall continue performance of the Contract to the extent not terminated and the Bank will pay for the services availed.

20 TERMINATION FOR INSOLVENCY

20.1 if the IS Auditor becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the IS Auditor 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 any part of its undertaking or assets, or if the IS Auditor takes or suffers any other analogous action in consequence of debt; then the Bank may at any time terminate the contract by giving written notice to the IS Auditor. If the contract is terminated by the Bank in terms of this Clause, termination will be without compensation to the IS Auditor, 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.

20.2 if the Bank becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, 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 any part of its undertaking or assets, or if the Bank takes or suffers any other analogous action in consequence of debt; then the IS Auditor may at any time terminate the contract by giving written notice to the Bank. If the contract is terminated by the IS Auditor in terms of this Clause, the IS Auditor shall be entitled to be paid the Contract Price attributable to the portion of the work executed as at the date of termination and the payment that would become due on completion of the stage encompassing the termination and the costs, if any.

21 TERMINATION FOR CONVENIENCE

21.1 The Bank, by 30 days advance written notice sent to the IS Auditor, 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 performance of the IS Auditor under the Contract is terminated, and the date upon which such termination becomes effective.

21.2 The Services that are complete on the date of IS Auditor'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 under mutually agreed terms and prices; and / or

b) to cancel the remainder and pay to the IS Auditor an agreed amount for Services partially completed or already procured.

21.3 The Bank shall not unreasonably terminate the Contract in part if such termination would result in the IS Auditor being unable to complete the remaining contractual obligations. The Bank shall also not terminate the Contract in part if the non-performance is due to the inability of the Bank to fulfil its contractual obligations

22 EXIT REQUIREMENTS

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

23 LIQUIDATED DAMAGES

23.1 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 Information System Auditor under the terms and conditions of the contract and its amendments and the Information Security 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.

23.2 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 Information System Auditor either as per the Contract, executed between the Bank and the Information System Auditor pursuant hereto or under any other Agreement/Contract, the Bank may have executed/shall be executing with the information System Auditors.

24 FORCE MAJEURE

24.1 The IS Auditor shall not be liable for 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.

24.2 For purposes of this clause, "Force Majeure" means an event beyond the control of the IS Auditor and not involving the IS Auditor'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.

24.3 If a Force Majeure situation arises, the IS Auditor shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the

Bank in writing, the IS Auditor 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.

24.4 If an event of Force Majeure continues for a period of one hundred and eighty (180) days or more, the parties may, by mutual agreement, terminate the Contract without either party incurring any further liabilities towards the other with respect to the Contract, other than to effect payment for Products already delivered or Services already performed.

24.5 Notwithstanding the above, the decision of the Bank shall be final and binding on the IS Auditor.

25 NOTICES

25.1 Any notice given by one party to the other pursuant to Contract shall be sent to the other party in writing to the other party's address.

25.2 A notice shall be effective when delivered or on the notice's effective date, whichever is later.

26 RESOLUTION OF DISPUTES

26.1 The Bank and the IS Auditor shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the Contract.

26.2 If, after thirty (30) days from the commencement of such informal negotiations, the Bank and the IS Auditor have been unable to resolve amicably a Contract dispute, either party may require, by giving notice, that the dispute be referred for resolution to the formal mechanisms. These mechanisms may include, but are not restricted to, conciliation mediated by a mutually agreed third party, adjudication in an agreed national forum.

26.3 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 services under the contract.

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

(a) In the event of any controversy or dispute or difference arising between the Bank and IS Auditor regarding the interpretation of any part of the agreement or any matter connected with, arising out of, or incidental to the arrangement incorporated in 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 IS Auditor; 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 Arbitrator appointed subsequently, the Presiding Arbitrator shall be appointed by the Chairman, Indian Banks' Association(IBA), India which appointment shall be final and binding on the parties.

(b) If one of the parties fails to appoint its arbitrator in pursuance of sub-clause (a) above, within 30 days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Chairman, Indian Banks' Association (IBA), India shall appoint the Arbitrator. A certified copy of the order of the Chairman, Indian Banks' Association (IBA) making such an appointment will be furnished to each of the parties.

(c) 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.

(d) 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.

(e) The decision of the majority of arbitrators shall be final and binding upon both the 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.

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

26.5 Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligation under the contract unless they otherwise agree.

27 JURISDICTION

27.1 Any dispute arising out of this order/contract will be under the jurisdiction of Courts of Law in Chennai.

28 GOVERNING LAW

28.1 The Contract shall be subject to and construed and interpreted in accordance with the laws of India.

29 GOVERNING LANGUAGE

29.1 All correspondence and other documents pertaining to the contract shall be written in English only.

5. Eligibility Criteria

ELIGIBILITY CRITERIA: Only Companies/LLPs/Firms with CERT-In Certification are required to apply. On expiry of the validity during the contract period, the renewal certificate (or any other documentary evidence to prove the extension of validity of the certificate) should be submitted within 1 month from the date of expiry to ensure continuation of the empanelment. In other words, at any point of time during the period of empanelment, the audit organisation should have valid Cert-In certificate or confirmation of extension.

Applicants who are not empanelled with CERT-In or have been blacklisted / barred / disqualified by any regulator / statutory body or the Applicant is otherwise involved in any such incident with any concern whatsoever, where the job undertaken / performed and conduct has been questioned by any authority, which may lead to legal action, are barred from being considered for selection, hence they need not apply and no further correspondence shall be made with them. If such incident comes to light post selection, the contract with the audit organization shall be treated as cancelled at no cost to the Bank.

SN	Eligibility Criteria	Proof to be enclosed
1.	The Applicant should be a Company registered under Companies Act, 1956/2013 or LLP registered under Limited Liability Partnership Act, 2008 or Partnership Firm registered under Indian Partnership Act, 1932 and should have been operating for at least five years in India as on 31.12.2019.	Copy of Certificate of Incorporation, Memorandum and Articles of Association and / or Copy of Registered Partnership Deed
2.	The applicant should have been included in the latest panel of Information Systems Auditors maintained by Computer Emergency & Response Team, India [CERT-IN] as on date.	Copy of certificate
3.	The applicant should have positive net worth in each of the last three financial years of the applicant.	Certificate from the Chartered Accountant

<table>
<tr><td>4.</td><td>The applicant should have minimum annual turnover of Rs. 1 crore from Information Security audit activities in each of the last three financial years</td><td>Certificate from the Chartered Accountant with break-up of earnings from IS audit</td></tr>
<tr><td>5.</td><td>The applicant should have resources possessing sufficient domain and technical knowledge in respect of development, security and audit of banking applications including Mobile Banking applications. The audit organisation should have minimum one qualified professional holding valid certification in CISA / CISM / CISSP / ISO 27001 (LA/LI) as partners/directors.

In addition to this, audit organization should also have minimum fifteen staff with one or more of the following qualifications / Certifications.
<table>
<tr><td>I.</td><td>CISA</td><td>X.</td><td>SSCP</td></tr>
<tr><td>II.</td><td>CISM</td><td>XI.</td><td>Comp TIA</td></tr>
<tr><td>III.</td><td>CISSP</td><td>XII.</td><td>GIAC</td></tr>
<tr><td>IV.</td><td>ISO 27001 (LA/LI)</td><td>XIII.</td><td>CRISC</td></tr>
<tr><td>V.</td><td>C E H</td><td>XIV.</td><td>ECSA</td></tr>
<tr><td>VI.</td><td>COBIT Certificate Holder</td><td>XV.</td><td>OSCP</td></tr>
<tr><td>VII.</td><td>Certified PCI DSS professional</td><td>XVI.</td><td>ECIH</td></tr>
<tr><td>VIII.</td><td>CCNA / CCNP</td><td>XVII.</td><td>CPTE</td></tr>
<tr><td>IX.</td><td>CHFI</td><td></td><td></td></tr>
</table></td><td>Declaration should be submitted in the prescribed format and curriculum vitae of the professionals to be attached.</td></tr>
<tr><td>6.</td><td>In the last three years as on 31.12.2019, the Applicant must have carried out minimum three audit assignments covering the scope of work of the respective VERTICAL for which the bid is submitted, of which atleast two assignments pertain to Scheduled Commercial Banks having minimum of 200 branches each.</td><td>Copy of Work Order specifying the nature and scope of audit.

In case the Work Order contains inadequate information, any other documentary evidence containing the required details, shall be furnished additionally.</td></tr>
<tr><td>7.</td><td>The applicant should have the capability and willingness to deploy competent resources to carry out assignments, entrusted by the bank at Chennai, Mumbai, Kolkata or any other location as specified by the Bank, at short notice.</td><td>Declaration to be submitted in the prescribed format</td></tr>
</table>

8.	The applicants or their promoters 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. 1. The applicant should also not be involved in any litigation / arbitration proceeding. 2. The applicant should not have been blacklisted nor have been technically disqualified on the grounds of non-performance of contract, by any Government Department / Statutory Body / Public Sector Undertaking / Public Sector Bank in India. 3. The name of the applicant or its promoter/partner etc. 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. 4. The applicant or its sister concern should not have been involved in any unlawful activity as per the laws of the land.	Self-Declaration / Certificate of Fair Practices Code in the prescribed format
9.	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 presently or in the last one year as on 31.03.2019. shall not be eligible to participate in the RFP	Self-Declaration in the prescribed format

Bank reserves the right to seek more information in due course, if considered necessary.

6. DOCUMENTS TO BE SUBMITTED AS PART OF BID

Documents	Details	Whether enclosed (Y/N)
Doc-A	Bid Response Format in printed form - Covering Letter in Letterhead signed by Authorized Signatory in the prescribed format	
Doc-B	Letter of Authority / Power of Attorney for participation in the bid on behalf of the applicant in the prescribed format	
Doc-C	Details of SPOC of the Audit Organization and Core Audit Team in the prescribed format	
Doc-D	(i) Demand Draft for Rs. 5000/- favoring Indian Bank and payable at Chennai OR Declaration for MSME registration OR Declaration of earlier payment details. (ii) Bank Guarantee, towards EMD, in the prescribed format issued by a scheduled commercial bank for a sum of Rs. 2,00,000/- (Rupees Two Lakhs only) and valid for 120 days from the last date for submission of bid	
Doc-E	Documentary proof of existence / Copy of Certificate of Incorporation / Memorandum and Articles of Association in case of company and Registered Partnership Deed in case of LLP/firm	
Doc-F	Documentary proof of Empanelment with CERT-In	
Doc-G	Certificate from Chartered Accountant regarding the Organization's net worth in the last three financial years of the applicant.	
Doc-H	Certificate from Chartered Accountant in respect of the annual turnover in the last three financial years of the applicant with break-up of earnings through IS Audit	
Doc-I	Audited Financial Statements for the last three financial years of the organization with Audit Report	

Doc-J	Declaration / Undertaking / Confirmation in respect of Professional Qualifications as detailed under "Eligibility Criteria" point 6 in the prescribed format	
Doc-K	Curriculum Vitae of the partner/director/ employee with their qualifications / valid certifications in the prescribed format	
Doc-L	Declaration / Confirmation / Details in respect of work experience as detailed under "Eligibility Criteria" points 7, 8 and 9 in the prescribed format	
DOC-M	Documentary evidences such as copies of work orders and/or a letter of satisfactory completion specifying the nature and scope of audit to be attached.	
DOC-N	Self Declaration / Fair Practices Code Undertaking in the prescribed format	
DOC-O	Copy of Bank's Request for Proposal along with amendments / clarifications, if any, duly signed by the authorized signatory of the applicant in acknowledgement of the terms and conditions	
DOC-P	Commercial Bid in the prescribed format	

ANNEXURE I

Detailed Scope of Audit for all locations/audits, to the extent applicable to respective Verticals :

IS Audit will cover entire gamut of computerized functioning including e Delivery Channels & functional areas with specific reference to the following:

1. Policy, Procedures, Standard Practices & other regulatory requirements:

1.1 IT Governance and alignment of Bank's IT strategy with Business goals, Information Security Governance, effectiveness of implementation of Bank's IT Security Policy & Procedures.

1.2 Compliance to National Critical Information Infrastructure Protection Centre guidelines (NCIIPC), guidelines/instructions from RBI/IDRBT, Gopalakrishna Committee recommendations on Information Security, Internet Banking & other delivery channels.

1.3 E-Commerce based on UNCITRAL; VISA, Ru-PAY, Master Card, and other regulatory guidelines; ISO 8583 standards for communication

1.4 CERT-In, PCI-DSS, NPCI and DSCI Guidelines.

1.5 IT Act 2000, IT Act 2008 (amendment) act.

1.6 Best practices of the industry including ISACA's Guidelines / COBIT / ISO standards.

2. Physical and Environmental Security:

2.1 Access control systems including access provided to vendors, Surveillance systems of Data Centre/ DR Site and Near-DR, Premises management

2.2 Assessment of risks and vulnerabilities due to natural calamities; Air-conditioning, humidity control systems, etc. of DC/ DR Site/ NDR etc.

2.3 Fire protection systems, their adequacy and state of readiness.

2.4 Electrical supply, Redundancy of power level, Generator, UPS capacity

2.5 Assets safeguarding, handling of movement of Man /Material/ Media/ Backup / Software/ Hardware / Information.

2.6 Premises Management, Pest prevention / rodent prevention systems, Water leakage detection systems.

2.7 Vendor Audit Reports - For existing vendors -Regular Review and For new/proposed vendors - Vendor Evaluation Reports

3. IT Architecture - Audit of procedures, security

a. Operating Systems Audit of Servers, Systems and Networking Equipment:

3.a.1 Setup & maintenance of Operating System Parameters; OS Change Management Procedures- Version maintenance, hot-fixes &Service packs

3.a.2 Vulnerability assessment & hardening of Operating Systems

3.a.3 User account management including maintenance of sensitive User accounts - Use of root and other sensitive passwords;

3.a.4 File systems security of the OS; Review of Access rights and privileges, role based access control

3.a.5 Use of administrative shares, default login /passwords, remote access / Net meeting or any other such tool

3.a.6 Use of sensitive system software utilities

3.a.7 Remote access polices including Remote Desktop Management.

3.a.8 Users and Groups created, including all type of users' management ensuring password complexity, periodic changes etc.

3.a.9 Profiles and log-in scripts

3.a.10 Services and ports accessibility; validate the process for creating, deploying, managing and making changes to virtual machines and VSAN

3.a.11 Review of Log Monitoring, its' sufficiency, security, preservation and backup; Registry settings, including registry security permissions

3.a.12 Implementation of ADS (Active Directory Services) or Group Policy

3.a.13 Antivirus update and effectiveness of Big-Fix in patch updation

3.a.14 SAN Security ie., data encryption and integrity; SAN Management including performance optimization, scalability, migration

3.a.15 Review of the Logs of Backend Database changes

3.a.16 Review of Adherence to licensing requirements.

3.a.17 Review of Unauthorized off port services running

3. b. Application level Security Audit:

3.b.1 Logical Access Controls- To review all types of Application Level Access Controls including proper controls for access logs and audit trails to ensure the Sufficiency & Security of Creation, Maintenance, monitoring and Backup of the same

3.b.2 Input controls, Processing controls, and Output controls for all critical Bank's systems

3.b.3 Interface controls - Interfacing of software with ATM switch, EDI, Tele banking server, Web Server and Other interfaces at Network level, Application level and security in their data communication

3.b.4 Authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition

3.b.5 Audit trail / Audit log generation, storage, retrieval and management

3.b.6 Data integrity & File Continuity Controls

3.b.7 User ID / Password Management; Hard coded user-ids and password, Segregation of duties, access control over development, test and production regions

3.b.8 Review of Parameter maintenance process and controls implemented therein

3.b.9 Change management / Patch management procedures including change request, unit/integration testing, impact analysis documentation, adequacy of user acceptance tests, roll-back procedure and version control. Availability of documentation pertaining to change requests with all changes traceable.

3.b.10 Exceptional procedures and approval mechanism for emergency changes viz. Backend Updations in the Bank's systems including CBS, Exim Bills, etc., Parameter Relaxations, Single Sided transactions, etc.

3.b.11 Review adequacy and completeness of controls; Identification of gaps in application security parameters

3.b.12 Audit of management controls including system configuration/ parameterization

3.b.13 Audit of controls over operations including communication network, data preparation and entry, production, documentation and program library, Help Desk and technical support, capacity planning and performance, availability of user & operation manuals

3.b.14 Monitoring of outsourced operations, Adequacy of Vendor support and whether in line with Service Level Agreements

3.b.15 Manageability with respect to ease of configuration, transaction roll backs, time taken for end of day, day begin operations and recovery procedures

3.b.16 Review of Software customization and adherence to SDLC Policy for such customization

3.b.17 Adherence to Legal & Statutory Requirements

3.b.18 Application level Recovery & Restart procedures; Backup/Fallback/Restoration procedures and contingency planning

3.b.19 If outsourced, escrow arrangement with application owner

3.b.20 Auditing, both at client side and server side, including sufficiency and accuracy of event logging, SQL prompt command usage, Database level logging etc

3.b.21 Adequacy of hardening of all Servers and review of application of latest patches supplied by various vendors for known vulnerabilities as published by CERT, SANS etc

3.b.22 Bank's IT Department will take necessary action to protect information contained on a server / storage device that is no longer in use e.g. erase and reformat disks. The Auditors shall examine instances of any lapses on this score.

3.b.23 Application-level risks at system and data-level including system integrity risks, system-security risks, data risks and system maintainability risks

3.b.24 Review of Software benchmark results and load and stress testing of IT infrastructure performed by the Vendors

3.b.25 Special remarks may also be made on following items- Hard coded user-id and Password, system mail retrieval and storage

3.b.26 Review of Sufficiency and coverage of UAT test cases, UAT defects and tracking, resolution including re-testing and acceptance.

3.b.27 Review of Change management procedure during conversion, migration of data, version control etc

3. c. Audit of DBMS and Data Security:

3.c.1 Logical access controls which ensure access to data is restricted to authorized users; authorization, authentication and security are in place; Segregation of duties

3.c.2 Audit of data integrity controls including master table updates; integrity is ensured to avoid concurrency problem

3.c.3 Confidentiality requirements are met; Physical access and protection

3.c.4 Use of Data Repository Systems, Data Definition Language, Data Manipulation Language (DML) and Data Control Language, Audit of log of changes to Data Definitions

3.c.5 Protection of Sensitive Information during transmission between applications/databases

3.c.6 Availability of Catalog Server, Synchronization of control file and catalog server

3.c.7 Database Backup Management, storage, retrieval, restoration procedures from older version to newer versions

3.c.8 Purging -Policy, procedures and process of purge of data

3.c.9 Security of oracle systems files viz. control files, redo log files, archive log files, initialization file, configuration file, Table space security, utilization, modifications, etc

3.c.10 Password check-up of Systems and Sys Users

3.c.11 Checking of database privileges assigned to DBAs and Users (privilege like ALTER SESSION, ALTER SYSTEM and BECOME USER etc.

3.c.12 To examine and review different types of Logs generated from users/ background/ memory process etc. and to examine the controls ensuring sufficiency & security of creation, maintenance and backup of the same

3.c.13 Procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner and necessary safeguards for its confidentiality, integrity, availability and authenticity are taken as per IT Security Policy

3.c.14 Patches and new versions are updated as and when released by vendor/ Research and Development team

3. d. Product Audit / Functionality Audit:

3.d.1 Input Controls
3.d.2 Processing Controls
3.d.3 Output Controls
3.d.4 Review of product specific functionality& features
3.d.5 Logical Access Controls - To review Application Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same.
3.d.6 Auditability both at Client & Server side including sufficiency & accuracy of event logging, adequacy of Audit trails, SQL command prompt usage, database level logging etc.
3.d.7 Interface controls - Application interfaces with other applications and security in their data communication.
3.d.8 Authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition.
3.d.9 Data integrity & File Continuity Controls
3.d.10 User maintenance, password policies as per bank"s IT security policy with special reference to use of hardcoded User Id & Password
3.d.11 Segregation of duties and accesses of production staff and development staff with access control over development, test and production regions.
3.d.12 Review of all types of Parameter maintenance and controls implemented.
3.d.13 Change management procedures including testing & documentation of change.
3.d.14 Identify gaps in the application security parameter setup in line with the bank's security policies.
3.d.15 Audit of management controls including systems configuration/ parameterization & systems development.
3.d.16 Audit of controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and technical support, capacity planning and performance, Monitoring of outsourced operations.
3.d.17 Review of customizations done to the Software & the SDLC Policy followed for such customization.
3.d.18 Adherence to applicable Legal & Statutory Requirements
3.d.19 Suggestions for segregations of Roles/Responsibilities with respect to Application software to improve internal controls
3.d.20 Review of documentation for formal naming standards, design process of job roles, activity, groups, profiles, assignment, approval & periodic review of user profiles, assignment & use of Super user access.
3.d.21 Sufficiency and coverage of UAT test cases, review of defects & tracking mechanism deployed by vendor & resolution including re-testing & acceptance.
3.d.22 Backup/ Fallback/ Restoration/ Recovery & Restart procedures

3.d.23 Security in SDLC processes, security of application, security testing processes, in-built security with the application development and maintenance procedures, license management, escrow agreements.

4. Network – Audit of Network Security architecture, Management, network devices, traffic and Performance analysis, review of NW monitoring software

4.1 Network Security architecture of the entire network including understanding traffic flow in the network at LAN & WAN level

4.2 Review of appropriate segregation of network into various trusted zones. Analysis of Network Security controls including logical locations of Security components like firewall, IDS/IPS, proxy server, antivirus server, email Systems, VSAT IDUs etc. in various zones

4.3 The Auditors shall review to ensure that access to Bank's Corporate e-mail facility is granted to authorized users

4.4 Review of redundancy for Links and Devices in CBS Setup both at central level and branch level

4.5 Review of security measures at the entry and exit points of the network

4.6 Checking Inter-VLAN Routing and Optimization, Study of incoming and outgoing traffic flow among web servers, application servers, database servers, DNS servers and Active Directory

4.7 Audit of VLAN segregation, access to servers, encryption mechanisms for connectivity and access, remote access provisioning etc

4.8 Review of Routing policy, Route path and table audit; Review of placement of security devices and DMZ's; Routing protocols and security controls therein

4.9 Audit of network architecture from disaster recovery point of view

4.10 Access control for DMZ, WAN, and for specific applications of the respective zones

4.11 Firewall policy, configurations, deployment and effectiveness

4.12 Review of all types of network level access controls & logs, for ensuring sufficiency & security of creation, maintenance and backup of the same, delegation of rights to users in accordance with job functions.

4.13 Secure Network Connections for CBS, ATM and Internet Banking including Client / browser based security

4.14 Review of Methodology adopted in maintenance of Network devices, their performance, replacement at all locations, DC/DR/NDR/ Branches/ offices.

4.15 Evaluation of centralized controls over Routers installed in Branches, DC/DR/NDR & their Password storage and Management

4.16 Audit of VSAT & Wireless connectivity infrastructure

4.17 Internet access management including cyber-roam - creation, maintenance, authentication procedures, access rights, deletion etc as per Bank's security policy

4.18 Active directory management – creation, maintenance, allocation of access rights and user groups, restrictions etc

4.19 Incident management: Audit of Incident Management and handling processes, roles and responsibilities, alerting and incident response procedures, verification of incident reports and effectiveness measurement, awareness of security incidents and events, Adherence to SLA

4.20 Privileges available to outsourced vendors

4.21 Review of

- Network documentation policy
- Network topology diagram
- nomenclature of server names, labelling, roles and allocation of IP Addresses
- Creation of change log for each server
- Documentation of software versions and proof of licence
- Documentation of hardware /firmware components, mode of connectivity of device, configuration, back up for configuration, password management for each device
- Documentation of backup procedure
- Violation logging management
- Risk Acceptance (Deviation).
- Password management.
- Authentication.
- Network Information security administration.
- Cryptography.
- Policies and rule sets including ACLs (Access Control Lists).
- Violation logging management.
- Information storage & retrieval.
- Audit trails.
- PKI management.
- PIN management.
- Review access control documentation and configuration.

4.22 Session Management

4.23 Configuration Audit of Network Devices

- Routing protocol analysis.
- Checking of HSRP configurations, if any, and its working.
- Review of network devices roles and configuration through configuration audit.
- Service proxies, circuit-level gateways and packet filters.
- VPN configuration and encryption.
- Updated version of OS / patches.
- Auditing, logging, monitoring and alerting mechanism
- Session management.
- Domain name services.
- Separate Configuration audit of Firewall rules and its review
- Validation of following services for security, effectiveness and efficiency on all Network devices:

  i. IP directed broadcasts

  ii. Incoming packets at the router sourced with invalid addresses

  iii. TCP small services.

  iv. UDP small services.

  v. All source routing.

  vi. All web services running on router.

  vii. Logging & Auditing.

  viii. Banner checking.
- Configuration to defy security attacks like IP spoofing, ICMP redirects, banner grabbing using Telnet/FTP/HTTP etc, IP directed broadcasts

4.24 Verification of network devices for security threats including but not limited to DoS, DDoS, Spoofing, DNS poisoning, SYN flood etc

4.25 Checking for all known Viruses, Trojans, Root kits, Worms

4.26 Open TCP/UDP ports

4.27 Review of traffic & performance through

- LAN/WAN link utilisation/quality analysis/bandwidth availability/usage etc
- Capacity planning analysis including scalability
- Congestion area at various topology layer and traffic pattern analysis
- Analysis of latency/response time in traffic across various links
- Analysis of load balancing mechanism

4.28 Security audit of Wireless networking infrastructure deployed by the Bank including but not limited to Encryption technique, Authentication mechanism

etc. of endpoints using technology like WLL, VSAT, RF, CDMA etc. for connectivity

4.29 Access control audit for all Networking Devices viz. Routers, Switches, IDS/ IPS, VSAT Infrastructure Firewalls etc.

- Routers/ switches/ Firewalls/ IDS/ IPS are using AAA (Authentication, Authorization and Accounting) model for all user authentications.
- Password enabled on the routers/switches in encrypted form and comply with minimum characters in length
- Privileges available to Systems Integrator and outsourced vendors.
- Review of access lists for different network segments (to different outside Networks).
- Delegation of privileged use in accordance with job function.
- Local and remote access to the Networking devices is limited & restricted.
- Cyber incident observed during contract period and availability of RCA (Root Cause Analysis) and/ or Forensic analysis.

4.30 Network Traffic & Performance Analysis:

- Packet flow performance.
- Base line Configurations

4.31 Network Monitoring Software Review

- Review of functional capabilities and effectiveness of NMS software.
- Review of availability of tools to generate ad-hoc reports from system logs

5. Backup, Storage Media Management, Handling and Recovery Testing:

5.1 Audit of

- Backup & recovery/restoration testing procedures
- Library structures and register maintenance
- media maintenance procedures, definition of standards for external identification of magnetic media
- access controls, movement and storage of backup media to support accountability
- Consistency in handling and storing of information and its labelling in accordance to its classification
- Sufficiency checks of backup process to ensure data integrity/restorability from earlier versions, readability / validity of the data to the present environment, periodicity of backup storage and retrieval, compatibility of the data retrieval and destruction of data and media etc.
- Controls for Prevention of Data Leakage through removable media or other means
- Synchronization between DC/NDR & DR Site databases

5.2 Adherence to Policies for media handling, disposal and transit

5.3 Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement

5.4 Review of Retention periods and storage terms, as per regulatory requirements for documents, data, programs, reports, messages (incoming & Outgoing), keys/certificates used for encryption and authentication, log files for various activities

5.5 Responsibilities for media library management and housekeeping procedures are assigned to specific members of the IT function to protect media library contents

5.6 Standards are defined for the external identification of magnetic media and control of their physical movement and storage to support accountability.

6. Privacy, Data Protection & Fraud Prevention:

6.1 Policy on implementation and Assurance to the management regarding proper controls and periodic updation of the same to prevent Cyber Frauds / IT Frauds and detection mechanism

6.2 Isolation and confidentiality in maintaining bank's customer information, documents, records by the bank including information available to Call Centre vendors, related sub-systems, Hardware, Software, applications, infrastructure used by the vendors involved in development/testing

6.3 Prevention of unauthorized access of former employees; People on notice period moved to non-sensitive role; Retired/Dismissed staff to be removed from the Active User List on immediate basis; Close supervision of staff in sensitive position

6.4 Review of documents / media retention policy; Media control within the premises

6.5 Procedures to prevent access to sensitive information and software from Computers, disks and other equipment or media when they are disposed of or transferred to another user are defined and implemented

6.6 Such procedures guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party

7. Business Continuity Methodology and Management and effectiveness of DR Drill process

7.1 Review of methodology adopted in identification of critical business process, systems and establish its ownership

7.2 Escalation procedure and policy with reference to efficacy of Emergency Response team/ Recovery team/Salvage Team/Incidence Reporting team

7.3 Review the adequacy of processes for conducting business impact analysis, risk assessment on the basis of Business Impact Analysis (BIA); Review and assess the adequacy of recovery strategies deployed by bank including cryptographic disaster

7.4 Participate in the DR Drill conducted by the bank every half year, once from the DR site and the other from the Data Centre and review DR Drill activity with respect to documented procedures, highlight any deviations from such procedures or improvements, if any, thereupon, including the effectiveness and efficiency of the automated tool for Switch over / Switch back activities

7.5 Adherence to Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO') based on policies/guidelines

7.6 Data Backup – periodic media verification for its readability, offsite storage and movement of backups at the time of DR Drill; restoration of backup at DR Site

7.7 Review of owned and shared resources with supporting function

7.8 Assurance from Service providers for critical operations for having BCP in place with testing performed on periodic basis

7.9 Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Bank and service providers

7.10 Adequate insurance maintained to cover the cost of replacement of IT Resources in event of disaster.

7.11 Time delay in transmission and restoration of daily data at DRS

7.12 Comment on success of Drill exercises

7.13 Review of escalation procedure adopted during disaster in branches, as per RTO & RPO of BCP Policy of the Bank

7.14 Review of events which could restrict successful shifting to DRS in case of any disruptions at main site

8. Addressing of HR issues and training aspect including:

8.1 Providing for the safety and wellbeing of people at branch or location at the time of disaster

8.2 Participation in drills conducted by RBI for Banks using RTGS/ NDS/ CFMS services

8.3 Security awareness training to staff; Communication of individual security Roles & Responsibilities to Employees

8.4 Review of segregation of duties.

8.5 Communication of individual security Roles & Responsibilities to Employees

8.6 Prevention of unauthorized access of former employees

8.7 Close supervision of staff in sensitive position

8.8 People on notice period moved to non-sensitive role

8.9 Retired/Dismissed staff to be removed from the Active User List on immediate basis.

9. Asset Inventory Management:

9.1 Records of assets maintained - Existence of Inventory Database & Controls, which identify and record all IT assets and their physical location, and a regular verification schedule which confirms their existence, review and updating including remarks on under-utilization, if any

9.2 IT assets classification, ownership definition & Labelling of Assets

9.3 List of approved software and its license, Modality for Checking and restriction of usage of unauthorized software, Approved Software storage controls

9.4 Legal and regulatory requirement of Importing or exporting of software

9.5 Proper usage policies for use of critical technologies by Outsourced Vendor/Employee

9.6 Maintenance of Inventory logs for media

9.7 Proper utilization of infrastructure of IT Assets, license and Warranty / AMC details and overloading of resources

10. Outsourcing policy and review of risks –

10.1 Compliance to Outsourcing Policy/IS Security policy

10.2 Review of Coverage of confidentiality clause/Non-disclosure Agreement and clear assignment of liability for loss resulting from information security lapse in the vendor contract

10.3 Service levels are defined and managed; review of financial and operational condition of service provider with emphasis to performance standards, imposing penalties wherever deviations are observed, business continuity preparedness

10.4 Review of monitoring of vendors activities as per SLAs

10.5 Review of physical / logical access provided to third party contractors working onsite

10.6 Service Level Agreements (SLAs); audit of SLA management for all kinds of services like Data Centre, DR site, ATM Switch, Internet Banking, Physical Security, Facility Management, etc.

10.7 Review of formal agreements executed to take care of all the risks associated with outsourcing

10.8 Where any assets, including those belonging to the Bank, are used by any mandated third party for providing services to external customers, whether they be subsidiaries or otherwise, IS Audit shall audit all assets, processes, procedures, connectivity, and any other related areas in as much as they intrude into or access Bank's assets or network or pose a risk to the Bank.

10.9 Review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness

11. IT Operations:

11.1 Business Relationship Management

11.2 Customer Education and awareness for adaptation of security measures; Mechanism for informing for deceptive domains, suspicious emails within the organisation/to customers

11.3 Review of monitoring of domain names to help prevent Entity for registering in deceptively similar names

11.4 Personnel scheduling - Shift hand-over process

11.5 Day begin and Day end process, Audit of SOD / EOD procedures, controls, control of transactions affecting intermittent accounts, control of systems generated transactions, re-posting of night region transactions, Job schedulers and execution/rollback of standing instructions.

11.6 Reviews of console log activity during system shutdown and hardware/ software initialization

11.7 Processes documentation; Operational procedure/documentation for Data Centre/Near-DR/ DR Site

11.8 Review of monitoring of operator log to identify variances between schedules and actual activity

11.9 Duty / Role segregation mechanisms/ procedures

11.10 Application Security covering access control.

11.11 Use of Internet as per the Bank□s Security Policy.

11.12 Issue and maintenance of Digital signatures.

11.13 Review of monitoring of system performance and resource usage to optimize Computer resource utilization.

11.14 Operational procedure for Data Center and DRS

12. Capacity Management:

12.1 Review of monitoring of system performance and resource usage to optimize Computer resource utilization and whether the same is as per Bank's policies

12.2 Service Continuity and availability management ; Avoidance of single point failure through contingency planning

12.3 Implementation version control

12.4 Key parameters of applications in CBS application, Operating System, RDBMS and Admin levels.

13. Project Management:

13.1 Process & Procedure involved in Information System Acquisition, Customization, Maintenance including version control, SW Library, ESCROW arrangement

13.2 Development, modification, maintenance and enhancements to In-house applications including version control, maintenance of SW library

13.3 Changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment

13.4 Scrambling of sensitive data prior to use for testing purpose

13.5 Release Management

13.6 Segregation of development, test and operating environments and review of segregation of duties while granting access in Development, test and live environment

14. Audit of Help Desk activities :

14.1 Review of functioning of centralized help-desk and the policy/procedure adopted

14.2 Review of methodology adopted in incident reporting, handling, resolution, and escalation to prevent recurrence with proper documentation including root cause analysis

14.3 Review of methodology adopted in prioritization/timely resolution of reported problems;

14.4 Audit trails and centralised archival of communication to and from helpdesks

14.5 Trend analysis and reporting

14.6 Development of knowledge base

15. Anti-Virus and Big-Fix, NTP server monitoring and implementation:

15.1 Proactive virus prevention and detection procedures are in place and implemented Virus definitions are updated regularly.

15.2 Review of monitoring of antivirus servers and clients located at branches, Zonal/Corporate Office in various locations for having updated latest versions and definitions.

15.3 Audit of anti-virus protection at servers/clients located at Data Centre/Near DR/DR site, Gateway level AV protection etc

15.4 Review of Implementation of automated security/OS updates in DC/NDR/DR/branches through Big-Fix

15.5 Review of implementation of synchronised time throughout network through NTP servers

16. Audit of Internet Banking & Mobile Banking Infrastructure:

16.1 Review of the process of Net Banking/Mobile Banking application, interface, data & Operational Security with reference to the Policy of the bank and regulatory requirement

16.2 Review of the net-banking/mobile banking architecture, connectivity, monitoring; creation, maintenance and modifications through RM Module at Branch level/Central Level

16.3 Review of controls to mitigate the risks due to Phishing / Vishing etc.

16.4 Systems audit of the Unified payments Interface (UPI) mobile application with PCI-DSS / PA DSS testing / Application Security Testing etc., as per NPCI guidelines. The auditors shall also comment on the deviations, if any, in the processes followed from the process flow submitted to the NPCI. (Auditor shall refer RBI Guidelines, NPCI Circulars, Industry Standards like ISO-27001, PCI-DSS etc. while performing an audit exercise)

16.5 Adequacy, generation & availability of Reports for financial, regulatory, statutory, MIS & statistical purpose covering all Mobile/net banking transactions

16.6 Adherence to Operational/Statutory guidelines issued by RBI, NPCI, PCI-DSS & other Regulatory bodies' with reference to Internet/ Mobile Banking Application

16.7 Audit of various functionalities provided in the application like Fund transfer, Transactions & queries, Cheque Book related, PAN/TAN validation etc.

16.8 Review of risk control measures in net-banking interfacing with CBS, access for NEFT/RTGS/ SFMS servers for LCs, payment of taxes, access to external sites like IRCTC, e-commerce transactions through gateway, 3D security management / 2nd factor authentication

16.9 Review of Customer feedback and appropriate resolution and reply communication to customers

16.10 Compliance of License agreement for all software/Hardware/OS

16.11 Adequacy of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Auditability etc. for the Internet/Mobile Application Solution

16.12 Adequacy of PIN/ Password Management Controls (Generation, Re-generation, Authorization, Verifications etc.) of Internet Banking/ Mobile Banking & Key Management features

16.13 Audit of various security features including but not limited to Transaction level security, Platform Security & reliability includes Database, Network & transmission Security, Registration features, Administration Portal features, Call logging, tracking & Dispute Resolution features etc.

16.14 Analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Incident management report etc

16.15 Review to ensure strong access control measures & Confidentiality in the transmission, processing or storing of customer data both by Service Provider and Bank

16.16 Compliance of SLA provisions with the service provider

17. a) ATM Switch & ATM Facility Management (Outsourced)

17.a.1 Compliance of Service Level Agreement (SLA) with the outsourced ATM Switch Vendor & ATM facility management vendor including PIN Management, card Printing and Management, Hot listing of cards, Time Management in delivering ATM Cards/PINS to customers/ Home branch

17.a.2 Adherence to various limits accepted with the Switch Vendor/Managed Services Vendors in the SLAs w.r.t. Uptime/Availability/Penalties etc.

17.a.3 Process Audit of Debit Card Management System (DCMS) including issue, hot-listing, regeneration and printing of PIN

17.a.4 Audit of Fraud Risk Management Tool deployed in the ATM switch for real time monitoring, process of configuration of policies, rules for real-time detection/ prevention of fraud

17.a.5 ATM Process Audit comprising ATM Operational Controls, Consortium issues, Reconciliation, posting, settlement between Master/VISA/RuPAY Cards & Gateway vendors handling e-commerce transactions, dispute Management, Controls against Skimming, etc

17.a.6 Audit of the Reconciliation activities being carried out w.r.t transactions involving various Acquirer, Issuer, Merchant, Interchange, other stakeholders etc. found in the ATM switch files with the transactions found in Host, Interchange & Partner Bank's switch. Also, Chargeback processing including VISA chargeback, NFS Chargeback etc. to be checked for appropriateness

17.a.7 Connectivity to partner networks and two way authentication between Bank's Server & Third Party's Server (in case of STP Transactions like online bills payment etc. for Customers/ Users)

17.a.8 Adequacy of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Auditability etc. at the ATM Switch/ATM Service Centre; Verification of the detailed security procedures & processes of the ATM Switch vendor including security controls for remote login of ATM Switch

17.a.9 Adequacy of Physical/environmental Security Controls at the ATM Switch (DC & DR) Presence of Biometric Authentication devices for Access Control, Fire Detection mechanisms & other Safety standards, Video Surveillance Systems/CCTV etc. to be checked

17.a.10 Analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Incident management report, reconciliation between Bank's GL and Vendor's GL

17.a.11 ATM Cash Management including outsourced Cash Management services; Review of daily operations including cash acceptance through Bunch Note Acceptors (BNA), reconciliation, EOD process through ADMIN menu, relevant Journal reports, dispute management, etc

17.a.12 Adequacy of contingency arrangement (Fallback / fail over procedures, Redundancy & Back-up) in the event of System Breakdown/Failure w.r.t Recovery/Restart facilities, Diagnostics for identification, Protection of Data, Backup facilities

17.a.13 Adequacy of Data/Network Security features with respect to the connectivity between ATM Switch (DC & DR Site), Bank's CBS DC/DRS, ATM Back Office etc Review of adequacy/appropriateness of the security protocol implemented (IPsec, SSH, SSL etc.), Network Security System Hardware/Software deployed (Firewall, IDS, Anti-Virus etc.), Adequacy /Reliability /Redundancy of the Bandwidth provided etc.

17.a.14 Adequacy, generation & availability of Reports for accounting, regulatory, statutory, reconciliation, MIS & statistical purpose covering all ATM transactions

17.a.15 Scalability & Interoperability for expanding network in future & sharing arrangements.

17. b) Credit Card and Debit Card Management (Outsourced)

17.b.1 Compliance of Service Level Agreement (SLA) with the outsourced Credit Card /Debit Card Vendor inclusive of charging penalties in case of non-adherence to acceptable level of service

17.b.2 Review of security involved in sharing confidential customer details with the vendor, mutual sharing of reports, payment reconciliation etc

18. Audit of Integrated Treasury & Payment Gateway:

18.1. Verification and evaluation of supervisory functions for Mid Office operations.

18.2. Adherence to FEDAI guidelines in the matter of assignment of roles and responsibilities.

18.3 Adherence to FEDAI guidelines pertaining to segregation of duties.

18.4 Implementation of authorized access mechanism to Dealers room including complete restriction in usage of communication devices inside the Dealing Room.

18.5 Periodic reconciliation of Old entries.

18.6. Maintenance of minimum number of Nostro accounts to avoid idle balance outstanding and charges incurred thereupon.

18.7. System driven automated Rates and Deals on real time basis and adherence to permissible time limit.

18.8. Audit of Swift network connectivity at INTEGRATED TREASURY having interface with CBS.

18.9. Justification of Penalty/ fine paid if, any.

18.10. Documenting of dealer movement and monitoring of dealing hours

Payment Gateway & Other Office

18.11. Audit of External network connectivity at Payment Gateway & other Offices facing the external network.

18.12. Verification of controls for RTGS, NEFT, SFMS, NDS -PDO, GILTS, CBLO etc. at Payment Gateway, as per the regulators policies and Guidelines.

18.13. Review of BCP/DRP for the above setups.

18.14. Compliance of SLA provisions with the concerned vendor

19.Audit of Financial Inclusion (FI) Infrastructure, DP & Online Share Trading:

19.1. Audit of External network connectivity for FI Infrastructure, USB infrastructure, POS infrastructure & Online Share Trading infrastructure with Bank□s CBS network. Review of network architecture security for these setups and adequacy of the security controls.

19.2. Verification of controls as per the Bank's security policies, regulatory policies, PCI-DSS, NPCI & other statutory guidelines.

19.3. Review of BCP/DRP for the above setups.

19.4. Sample configuration checking of POS terminals & USB Laptops for compliance.

19.5. Compliance of SLA provisions with the concerned vendors.

19.6. KBS server implemented by various Technical Service Providers (TSP .

19.7. Financial Inclusion Gateway of M/s FINO.

19.8. Rupay card PIN based transactions using PIN Pad devices.

19.9. Security Audit of transaction using Rupay Card and Aadhar Enabled Payment System.

20. General scope:

20.1. Review of Privileges available to Systems Integrator and Outsourced Vendors.

20.2. Evaluation of role, responsibility and accountability of IT Process owners.

20.3. Audit of DR Site including verification of systems / controls at the DR site, Assessment of environment and procedures at the DR site, Parameter Management, Adequacy of infrastructure, fallback procedures, Assessment of access control, comparisons of DR Site setup with Data Centre with respect to infrastructure (Hardware, Application Software, Systems Software etc.)

20.4. Vulnerability Assessment & IS Audit of Delivery channels, 3rd Party Products and interfaces like Internet Banking, SMS Banking, e-Credit & e-Retail, corporate email systems, Cash Management System, CIBIL, EXIM Bills, OGL, ALM, HRMS, RTGS, NEFT, EMS (Tivoli), AML, CTS, DP Services, CMS Hub, Trade Finance, Government Business, ATM Interface, SAS, Helpdesk module, E-mail System, and any other modules integrated with the Core System, as on the date of the audit.

20.5. Audit of e-mail access and usage, mail size and restrictions, attachment restrictions, AV & Spamming Control agents and archival for mail.

20.6. Software change management– Change and version control management, audit of movement from development to test to production; data access & segregation, access control to source code and libraries, audit of application development and maintenance processes, user access controls to application and database, audit of patch updates and upgrade processes.

20.7. Encryption standards/ message integrity standards, data privacy processes, efficiency of audit trails, audit trail synchronization mechanisms.

20.8. Security in SDLC processes, security of application, security testing processes, in-built security with the application development and maintenance procedures, license management, escrow agreements.

20.9. Audit of issuance & usage of Digital signature as per Bank's established guidelines & procedures.

20.10. Security Management- Patch Management & AV processes, audit of roles and responsibilities.

20.11. The scope of work further includes guiding/helping the Bank staff in putting in place the correct practices and conducting of a compliance audit.

20.12. The scope of work also includes sharing with Bank's IS Audit team all the formats, check lists, scoring sheets, scripts etc. that will be used during the process of IS Audit and explaining to the Bank's IS Audit team, all the processes, procedures involved in arriving at audit findings including interpretation of outputs generated by various audit tools.

20.13. Audit of availability of Bank's documented operating procedures for critical processes like Backup, capacity planning, equipment maintenance, application monitoring, server monitoring, networking monitoring, security monitoring etc.

20.Risk Analysis & Development of Risk Matrix/Profile:

20.1 The scope of work should be based upon Risk Analysis of the Information Systems of the Bank, as per regulatory guidelines and will include following steps:

Step 1: System Characterization

Step 2: Threat Identification

Step 3: Vulnerability Identification

Step 4: Control Analysis

Step 5: Likelihood Determination

Step 6: Impact Analysis

Step 7: Risk Determination

20.2 The Risk Analysis / Risk Matrix will be based on Adequacy of internal controls, business criticality, regulatory requirements, amount or value of transactions processed, customer facing systems, financial loss potential, number of transactions processed, availability requirements, experience of management and staff, turnover, technical competence, degree of delegation, technical and process complexity, stability of application, age of system, training of users, number of interfaces, availability of documentation, extent of dependence on the IT system, confidentiality requirements, major changes carried out, previous audit observations and senior management oversight.

ANNEXURE II

Indicative Count of applications, servers, etc. for the merged entity

SN	Description	Approx. Count
1.	Bank's IT setups	50
2.	Third party service providers	5
3.	Applications	380
4.	IPs/URLs	1600
	Of the above,	
	Critical and external facing / mobile applications and servers	200

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 audit.

ANNEXURE III

DOCUMENT A – RFP Response format and Undertaking

(Letter to the Bank signed by Authorised Signatory on the Applicant's letterhead)

To

Indian Bank,

Information Systems Audit Cell

Corporate Office, Inspection Department

Chennai – 600 014

Dear Sir,

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Audit of Indian Bank's ICT Infrastructure - Response to RFP**

Ref : **RFP No CO:INSP:5 /2019-20 dated 13/03/2020**

With reference to the above RFP, having examined and understood the instructions, terms and conditions, we hereby enclose our offer for conducting IS Audit of the systems, as detailed in your above referred inquiry.

We confirm that the offer is in conformity with the terms and conditions as mentioned in your above referred RFP. We further confirm that the information furnished in the proposal, annexures, formats, etc is correct. Bank may make its own inquiries for verification and we understand that the Bank has the right to disqualify and reject the proposal, if any of the information furnished in the proposal is not correct. We also confirm that we shall abide by the conditions, clauses, terms and conditions mentioned in the RFP document.

We confirm that we are Cert-in empanelled audit organization 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.

We understand that the Bank may debar us from participating in future tenders and report the matter to regulatory authorities in case any of the details furnished are found to be false.

We confirm that the offer shall remain valid for 90 days from the closing date for submission of the bid.

We undertake to intimate the Bank immediately about any change/development in our organization during the period of contract 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 Corporate Office Inspection 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 understand that the Bank is not bound to 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.

We further acknowledge that we cannot hold the Bank responsible for any breach of dates in the course of this RFP process. We also understand that execution of contract for first year does not entail the Auditor renewal for second year as an obligation.

We understand that Bank is not bound to accept any or all responses received with regard to the captioned RFP. We also understand and accept that it does not confer any right with regard to participation in any manner whatsoever and Bank at all times will have absolute right in its decision and is authorised to suspend our candidature without assigning any reason.

We further understand that the finalized prices will be frozen for a period of two years from the date of entrustment of assignment and that the Bank, at its discretion may entrust the assignment again 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 declare that we have disclosed all material information, facts and circumstances to the Bank.

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.

If selected, we understand that it would be on the basis of the Eligibility & Evaluation criteria as specified in the captioned RFP.

We acknowledge and understand that in the event that the Bank discovers anything contrary to our above declarations; it is empowered to forthwith disqualify us from further participation in the process.

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.

Yours faithfully,

Authorized Signatories

(Name, Designation and Seal of the Applicant)

Date:

DOCUMENT – B – LETTER OF AUTHORITY / POWER OF ATTORNEY FOR PARTICIPATION IN THE RFP ON BEHALF OF THE COMPANY / LLP / FIRM

(Letter to the Bank on Applicant's letterhead)

I, _____, the Company Secretary/ authorized person of _____ [Name of Company / LLP / Firm], certify that _____ who signed the bid in response to Bank's RFP is /are authorized to do so and bind the Company/LLP / Firm by authority of its board/governing body.

Date:

Signature

(Organization's Seal) (Name)

Document C - Details of SPOC of the Audit Organization and Core Audit Team

(Letter to the Bank signed by Authorised Signatory on the Applicant's letterhead)

Date:

To,

The Assistant General Manager

Indian Bank, Corporate Office

Inspection Department

IS Audit Cell

Dear Sir / Madam,

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Indian Bank's ICT Infrastructure**

I. Details of the Audit Organisation :

S. No	Details	
1.	Name of the Audit Organization	
2.	Constitution	
3.	Year of Incorporation	
4.	Registered Office / Complete Postal Address	
5.	Telephone, Mobile and Fax Numbers	
6.	Email Address	
7.	Name and address of the directors/ Partners	
8.	Date of original empanelment with CERT-In and and Expiry date of current empanelment.	

II. Single Point of Contact (SPOC) for all Bank related queries and assignments undertaken :

Details	Contact 1	Contact 2
Name of the Contact		
Title / Designation		
Telephone Number		
Fax No		
Mobile Number		
Email address		
Address for communication		

III. Profile of Core audit team to be assigned for the project

SN	Name	Designation	Part time/ Full time	Role in IS Audit (Task/Module)	Professional Qualification	Years of IS Audit experience

Yours faithfully,

Authorized Signatories
(Name, Designation and Seal of the Applicant)

DOC D - FORMAT OF BID SECURITY GUARANTEE

To

Indian Bank

Corporate Office Inspection Dept

Information System Audit Cell

254-260, Avvai Shanmugam Salai

Royapettah, Chennai 600 014

RFP Ref No -

Whereas..... (Hereinafter called "the Bidder") who intends to submit bid dated..... (date of submission of bid) for the supply of ..... (name and/or description of the goods) (Hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that We..... (Name of Bank) of ..... (Name of Country), having our registered office at ..... (address of Bank) (hereinafter called "the Bank"), are bound unto Indian Bank in the sum of _____for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents.

Sealed with the Common Seal of the said Bank this ____ day of _____ 2020 ____.

THE CONDITIONS of this obligation are:

1. If the Bidder

(a) withdraws its Bid during the period of bid validity or

(b) does not accept the correction of errors in accordance with the Instructions to Bidders; or

ii. If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of bid validity:

(a) fails or refuses to execute the Contract Form if required; or

(b) fails or refuses to furnish the performance security, in accordance with the Instruction to Bidders.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This Guarantee will remain in force up to _____ and any demand in respect thereof should reach the Bank not later than _____.

(Signature of the Authorised Official of Bank)

NOTE:

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

DOC - J - FORMAT OF CONFIRMATION OF PROFESSIONAL QUALIFICATIONS

(in respect of eligibility criteria no 6)

(on applicant's letter Head)

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Indian Bank's ICT Infrastructure**

I/We, the undersigned and the Authorised Signatory declare that we are having resources with sufficient domain and technical knowledge in respect of development, security and audit of banking applications including Mobile Banking applications.

I/We confirm that we have the minimum requirement of two Qualified Professionals holding valid certification in CISA/CISM/CISSP/ISO 27001(LA/LI) as Partners / Directors.

The Brief profile of our Partners / Directors is furnished hereunder:

S No	Name	Professional Qualification	valid up to, if applicable	Experience in brief

We confirm that we have _____ number employees in our organization out of which, the brief details of 15 personnel having qualification as called for in the Eligibility Criteria point no "6" is furnished hereunder:

S No	Name	Professional Qualification	Valid upto, if applicable

The Curriculum Vitae of each of our partner/director and employees is enclosed.

We further understand that an employee/director / partner holding multiple certifications shall be construed as only one employee / director / partner.

I/We confirm having personally verified the documentation in respect of the qualification obtained by the personnel and the validity of the professional qualifications, whose Curriculum Vitae has been attached as per the format prescribed in the RFP. We confirm that the details provided are accurate.

I/We also confirm that background verification of the personnel has been conducted prior to their employment with the Audit organisation.

I/We note to provide documentary evidence of the qualifications or professional certifications obtained by the personnel as and when required by the Bank.

I/We note to inform the bank whenever any professional qualification so obtained by the Personnel lapses and note to provide the details of renewed certifications.

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.

I/We undertake not to deploy any professional, who was in the services of the Bank in the last 36 months prior to the date of accepting any audit assignment from the Bank.

I/We confirm that our Audit Organization is having the capability and willingness to deploy competent resources to carry out assignments entrusted by the bank at Chennai, Mumbai, Kolkata or any other location as specified by the Bank, at short notice.

Yours faithfully,

Authorized Signatories
(Name, Designation and Seal of the Applicant)

DOC –K - FORMAT OF CURRICULUM VITAE (CV)

(To be furnished on a separate sheet for each personnel duly signed by Authorised Signatory of the Applicant)

Submitted as part of Document to the Bank for the **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Indian Bank's ICT Infrastructure**

Name of the Person / Designation in the Organization		
Profession		
Date of Birth		
Nationality		
Qualifications (Technical and Academic with year of passing):		
Membership of Professional Societies (please provide validity period wherever applicable)		
Service in this organization from		
Previous employment record	Organization	From to
Details of Key assignments handled in the past three years		
Organization	Month & Year	Details of assignment done

Give an outline of person's experience and training most pertinent to assigned tasks, describing the degree of responsibility held by the person on relevant previous assignments

DOC L - DECLARATION IN RESPECT OF WORK EXPERIENCE

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Bank's ICT Infrastructure**

I/We, the undersigned and the Authorised Signatory declare and confirm that we have sufficient work experience in respect of development, security and audit of banking applications including Mobile Banking applications as per "Eligibility Criteria' of this RFP Document.

The details of the Information Systems Audit undertaken by us during the **last three years** as on 31.12.2019 is furnished hereunder :

SN	Name of the Organization	Nature of Audit assignment	Date of PO	Date of Work completion
In respect of Work experience for **VERTICAL I** of RFP				
1				
2				
3				
In respect of Work experience for **VERTICAL II** of RFP				
1.				
2.				
3.				
In respect of Work experience for **VERTICAL III** of RFP				
1.				
2.				
3.				

Yours faithfully,

Authorized Signatories
(Name, Designation and Seal of the Applicant)

Document – N – Declaration / Fair Practices Code Undertaking

(On Applicant's Letter head)

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Bank's ICT Infrastructure**

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/ Public Sector Organisation/ Statutory Body/ any Government agency /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 last one year as on 31.03.2019.

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 confirm that our Audit Organization is having the capability and willingness to deploy competent resources to carry out assignments entrusted by the bank at Chennai, Mumbai, Kolkata or any other location as specified by the Bank, at short notice.

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 person who is going to conduct the audit is on our rolls and we note to mention the length of his/her service with us.

We undertake not to deploy any professional, who was in the services of the Bank in the last 36 months prior to the date of accepting any audit assignment from the Bank.

In respect of Eligibility Criteria point no 7 of this RFP document, 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 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.

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.

Signature

(Authorized signatory with Applicant's seal)

DOC E - COMMERCIAL BID

General Instructions:

- The Commercial Bid should be submitted in the Audit Organisation's letterhead duly signed and sealed by Authorised Signatory.
- The Commercial Bid should contain the Total project cost, on a fixed cost basis, excluding taxes.
- Bank will not provide any reimbursement for travelling, lodging/boarding, local conveyance or any other related expenses.
- Commercial Bid for **each vertical should include declaration** as indicated in the prescribed format.

The format for the commercial bid for each of the vertical is appended below :

Vertical I - ANNUAL AUDIT

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Bank's ICT Infrastructure – Commercial Bid for Vertical I**

		Amount excluding taxes for one instance (A)	No of instances during the RFP period (B)	Total amount excluding taxes (C)= (A)*(B)
A.1.	Cost of IS Audit for Bank's entire ICT infrastructure as per the scope defined under **Vertical – I** in the RFP, including cost of additional 50 mandays (Inclusive of all fees & expenses)		2 assignments (One per year)	
	Sub-Total for Fixed Contract			
B.1.	Source Code Review of applications with lines of code upto 50,000 on adhoc basis (approx. 25 applications)		25	
B.2.	Source Code Review of applications with lines of code above 50,000 on adhoc basis (approx. 25 applications)		25	
B.3.	IT General security Control audit / Process audit / Application Security audit / Product Functionality Audit / Incident Analysis Review, etc. on adhoc basis (approx 50 mandays)		50	
	Sub-Total for Rate Contract			
Total Cost of Audit for Vertical I				
Total Cost of Audit for Vertical I (Inclusive of all fees & expenses)		(in words)		

a) We hereby understand and declare that the commercial evaluation will be based on Total Cost of audit quoted for Vertical II, while

- Payment for assignment under S.No.A1 will be on **fixed contract price** basis as per the terms of this RFP and
- Payment for other assignments (S.No. B1 to B3) on **rate contract basis** for the actual work done, viz., on the basis of amount quoted per instance under Column A.

b) We understand that the no. of instances indicated in the RFP, **both for Fixed Contract and for Rate Contract**, 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.

Vertical II - VAPT

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Bank's ICT Infrastructure – Commercial Bid for Vertical II**

S No	Particulars	Amount excluding taxes for one instance (A)	No of instances during the RFP period (B)	Total amount excluding taxes (C)= (A)*(B)
A.1.	VAPT of Bank's entire ICT infrastructure, excluding those covered in S.No. 2 below, on half yearly basis as per the scope defined under **Vertical – II** in the RFP (Inclusive of all fees & expenses)		4 (Four Half years)	
A.2.	VAPT of all critical and external facing / Mobile applications and servers of the Bank on quarterly basis as per the scope defined under **Vertical – II** in the RFP (Inclusive of all fees & expenses)		8 (Eight Quarters)	
	Sub-Total for Fixed Contract			
B.1.	Vulnerability Assessment of servers/ Databases/OS/network devices of the Bank on adhoc basis (approx. 30 assignments)		30	
B.2.	Vulnerability Assessment and Penetration Testing of internal and/or external facing applications with upto 20 pages as *per OWASP on adhoc basis*. (approx. 50 assignments)		50	
B.3.	Vulnerability Assessment and Penetration Testing of internal and/or external facing applications with above 20 pages as *per OWASP on adhoc basis*. (approx. 25 assignments)		25	
B.4.	Vulnerability Assessment and Penetration Testing of Mobile applications as *per OWASP on adhoc basis* (approx. 10 assignments)		10	
	Sub-Total for Rate Contract			
Total Cost of Audit for Vertical II				
Total Cost of Audit for Vertical II (Inclusive of all fees & expenses)		(in words)		

a) We hereby understand and declare that the commercial evaluation will be based on Total Cost of audit quoted for Vertical II, while

- Payment for assignments under S.No.A1&A2 will be on **fixed contract price** basis as per the terms of this RFP and
- Payment for other assignments (S.No. B1 to B4) on **rate contract basis** for the actual work done,viz.,on the basis of amount quoted per instance under Column A.

b) We understand that the no. of instances indicated in the RFP, **both for Fixed Contract and for Rate Contract**, 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.

Vertical III - CONCURRENT AUDIT

Sub : **Notice inviting bids from Audit Organizations for conducting Information System Security Audit of Bank's ICT Infrastructure – Commercial Bid for Vertical III**

S No	Particulars	Amount excluding taxes per instance (A)	Number of instances during the RFP period (B)	Total amount excluding taxes (C)= (A) x (B)
A.1.	Continuous and Concurrent IS Audit of CO:ITD, DBD and ISSD, including CDC and NDR		24 (Twenty Four months)	
	Sub-Total for Fixed Contract			
B.1	Process audit / Product Functionality audit / Incident Analysis Review, etc. (approx 50 mandays)		50	
	Sub-Total for Rate Contract			
Total Cost of Audit for Vertical III				
Total Cost of Audit for Vertical III (Inclusive of all fees & expenses)		(in words)		

a) We hereby understand and declare that the commercial evaluation will be based on Total Cost of audit quoted for Vertical III, while
   - Payment for assignment under S.No.A will be on **fixed contract price** basis as per the terms of this RFP and
   - Payment for other assignments (S.No.B) will be on **rate contract basis** for the actual work done, viz., on the basis of amount quoted per instance under Column A.

b) We understand that the no. of instances indicated in the RFP, **both for Fixed Contract and for Rate Contract**, 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.

Yours faithfully,

Authorized Signatories
(Name, Designation and Seal of the Applicant)

DOC F - FORMAT OF PERFORMANCE BANK GUARANTEE

(to be submitted by successful bidder)

To

Indian Bank

Corporate Office Inspection Dept

Information System Audit Cell

254-260, Avvai Shanmugam Salai

Royapettah, Chennai 600 014

RFP Ref No -

Whereas _____ (herein called the "IS Auditor") has submitted its bid dated _____ for providing services of Information Systems Auditor of the Bank's IT infrastructure. which has been accepted by Indian Bank.

Whereas as per the terms, the IS Auditor will have to provide a Performance Security in the form of a Bank Guarantee for Rs. _____ (Rupees _____ only).

KNOW ALL PEOPLE by these presents that WE _____ (Bank name) having our registered office at _____ (Address of the Bank) (hereinafter called "the Bank") is bound unto INDIAN BANK (hereinafter called "the Purchaser") in the sum of Rupees _____ only on behalf of the IS Auditor for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.

Therefore, We hereby affirm that we are Guarantors and responsible to you, on behalf of the IS AUDITOR, upto a total of Rs. _____ (Rupees _____ only) and we undertake to pay you, upon your first written demand declaring the IS AUDITOR to be in default under the contract and without cavil or argument, any sum or sums within the limit of Rs. _____ (Rupees _____ only) as aforesaid, without your needing to prove or to show ground or reasons, for your demand or the sum specified therein.

This guarantee will remain valid for a period upto 13 months from the date of signing of the contract ie., from _____ to _____ and any demand in respect thereof should reach the Bank not later than the above date.

Place : _____

Seal

Signature & Code No

NOTE :

1. Bidders should ensure that seal and code no. of the signatory is put by the bankers, before submission of the bank guarantees.

2. Bank guarantees issued by banks located in India shall be on a Non-Judicial Stamp Paper of requisite value.