Indian Institute of Banking & Finance
(An ISO: 9001-2015 organisation)
(CINU91110MH1928GAP00)
2nd Floor, Tower-I
Commercial-II, Kohinoor City
Kurla-West
Mumbai-400070

REQUEST FOR PROPOSAL FOR CONDUCTING INFORMATION SYSTEM AUDIT OF INSTITUTE'S SYSTEMS

TO BE SUBMITTED ON OR BEFORE
28th September-2020 by 5PM

Addressed to:

Chief Executive Officer
Indian Institute of Banking & Finance
Corporate Office
2nd Floor, Tower-I, Commercial-II
Kohinoor City
Kurla-West
Mumbai-400070

Forwarded to:

The soft copies of technical and commercial proposals should be forwarded to Dr. Sudhir M Galande, Dy.CEO to the e-mail id: sudhirmg@iibf.org.in with due password protection.

Note:
(IIBF reserves the right to cancel this request for RFP and / or invite afresh one with or without amendments to this RFP, without any liability or any obligation for such RFP and without assigning any reason. Information provided at this stage is indicative and IIBF reserves the right to amend / add further details in the RFP document.)

1. ABOUT IIBF:

Established in 1928 as a Company, Indian Institute of Banking & Finance (IIBF), formerly known as The Indian Institute of Bankers (IIB), is a professional body of banks, financial institutions and their employees in India with a mission to develop professionally qualified and competent bankers and finance professionals primarily through a process of education, training, examination, consultancy/counselling and continuing professional development programs. During its 92 years of service, IIBF has emerged as a premier institute in banking and finance education for those employed as well as seeking employment in the sector. Since inception, the Institute has awarded several banking and finance qualifications, viz., JAIIB, CAIIB, Diplomas and Certificates in specialized areas and helped in sustaining their professionalism in banking and finance through continuing professional development programs.

IIBF is a 'Distance Learning' Institute. The candidates who appear for examinations, get adequate educational/knowledge inputs through various educational services offered by the Institute. The pedagogy of Distance Learning offered by the Institute is given below:-

I. Publishing specific courseware for each paper/examination;

II. Tutorials from accredited institutions;

III. Contact classes;

IV. Video lectures;

V. Virtual classes

VI. E-learning through portal;

VII. Campus training for selected courses, etc.

As a professional body, IIBF ensures that its members are enriched by latest developments and updated knowledge of the profession they practice. Towards this end, the Institute offers a daily e-news letter called "Fin @ Quest", a monthly bulletin – "IIBF-Vision", a quarterly journal – "Bank Quest". It also sponsor research on banking & finance and publishes the research reports. The Institute offers Management Development courses in collaboration with leading Management Institutions, besides organizing Seminars, Workshops, Conferences, Lectures, and short duration programs, etc., as part of Continuing Professional Development(CPD).

The Institute's Governing Council consists of eminent personalities from the banking and finance sector, academicians and professionals.

IIBF is an ISO 9001-20015 certified organization with its Corporate Office in Mumbai and three Professional Development Centres in Delhi, Chennai, and Kolkata.

2. Major Activities of the Institute:

2.1 **Membership:** IIBF currently has 8,87,380 individual members. There are 764 Institutional members (Banks and Financial Institutions).

2.2 **Courses Offered:** The Institute currently offers the following courses:

Flagship Courses:

- **JAIIB**
- **CAIIB**
- **Diploma in Banking and Finance**

Diploma Courses:

- Diploma in Treasury, Investment and Risk Management, Diploma in Banking Technology, Diploma in International Banking and Finance, Advanced Wealth Management Course etc.

Certificate Courses:

- Certificate course in Anti- Money Laundering and Know Your Customer, Trade Finance, Information System Banker, Credit Card for bankers, IT Security, Cyber Crimes & Fraud Management, FEMA, Rural Banking etc.

Blended Courses:

- Blended course in Credit Management, Treasury, Compliance, HRM etc. (For details visit- www.iibf.org.in)

All these examinations are backed by specially developed courseware. The Institute has published these courseware and they are available with the publishers' viz. M/s Macmillan India Ltd. M/s Taxman Publications Pvt. Ltd and also with leading book shops.

2.3 **Web Portal:** The web portal disseminates information with regard to Institute's profile, it's products & services. It also facilitates in online registrations of examinations, membership, training and other activities by receiving the fees online. The portal also offers educational support towards various courses(examinations) through e-learning and video lectures. These support services are rendered by respective service providers.

3. Introduction of the Assignment (Broad Requirements):

The Indian Institute of Banking & Finance (IIBF) desires to select an IS Auditor/audit firm who could take up the job of auditing the information systems of the Institute. The auditor/auditing firm has to create an audit plan, execute the audit, identify the gaps and submit a comprehensive audit report so that the Institute could bridge the gaps presented in the audit.

In this connection, the Institute wishes to invite bids through this RFP (Request for Proposals) from reputed and experienced IS Auditors/audit firms to provide audit services to the Institute.

4. Availability of RFP Document:

The detailed RFP Document covering eligibility requirements, technical specifications, terms & conditions, statement of work, and service agreement could be downloaded from IIBF's website i.e**. http://www.iibf.org.in/tender**

5. Compliance to Terms and Conditions:

The prospective bidders are requested to submit the bids strictly in accordance with the terms and conditions and specifications contained in the RFP document including amendments, if any, issued by IIBF prior to submission of RFP. The formats prescribed in the RFP documents should be scrupulously followed by the bidders. Bids that do not adhere to the terms and conditions are liable for rejection.

6. Brief Objective, Audit Approaches, Audit methodology, qualifications of auditors

6.1 **Objectives of Audit:**

The objectives of the audit are as under:

- Safeguarding of Information System Assets/Resources
- Maintenance of Data Integrity, Reliability and Confidentiality
- Maintenance System Effectiveness.
- Assurance of System Efficiency.

6.2.Audit Approaches:

The following IS audit approached be adopted while auditing the systems.

- Auditing around the computer
- Auditing through the computer
- Auditing with the computer

The IS audit checklists should be prepared based on globally accepted standards.

The risk findings from the audit must be classified as Low, Medium, High, Very High and Extremely high in each specific audit areas.

6.3 Audit Methodology:

The IS audit shall be carried out by manual procedures, computer assisted procedures fully automated procedures, depending on the chosen audit approach.

6.4. Qualification of Auditors:

The audit should be carried out by CERT-In empanelled audit firms/auditors having Qualifications such as **CISA/ DISA /CISSP /CISM / GIAC(SANS)** with minimum 5 years

7.Broad Scope of the Work:

The scope of IS Audit should encompass the physical and logical audit of IT assets/sources. Following is the broad scope of the work.

(A) Physical Security Audit: The audit should cover the physical access mechanisms of the systems, servers, software and other tools.

(B) Logical Security Audit:

I. Hardware Audit:

The audit should cover all the hardware items of the Institute including, (a)PCs, (b)Servers (c)Printers (d)Scanners and (e)all peripherals.

II .Software Audit:

1.Application Systems developed by the Institute

- o Candidate Life Cycle Management System
- o Training Module
- o Leave Management Module
- o Claim Request Module
- o Complaint Management System
- o Bank Reconciliation Module
- o Question Bank Module
- o Audit of the VPN/VDI (being used for work from home)

2.Packaged software used by the Institute:

(a) MS-Office,
(b) E-Mail Tools
(c/)Browsers
(d) All utility Software
(e)Freeware and Sharewares used by IIBF

3.All Server Software: Windows OS/Linux/Unix, IIS, Application Servers etc.,

4.Database systems : Audit Should cover all the database systems

III. Network Audit:

The audit should cover all the network equipment including (i)Routers (ii)Switches (iii)Firewalls (iv)LAN/WAN (v)Internet gateways (vi)I/O outlets, jack-panels, patch panels etc.,

IV. Security Audit:

i The audit should cover the security tools such as anti-virus tools, password policies, IT Policy, Firewall policies, and directory services and other access policies

ii ***The security audit of conduct of computer based online examinations through service providers***

V. Compliance Audit:

After completion of initial audit the bidders are requested to carry out the compliance audit for the vulnerabilities pointed out in the audit to complete the audit process

The following points must be taken care while carrying out IS audit.

Note: The bidder must fulfil all the requirements of the project to realise the objectives enumerated in this RFP document or any changes in the scope/terms & conditions that may be decided during the pre-bid meeting.

The detailed scope of IS audit is given in Annexure-I:

8.Bidding Process:

Institute is inviting the technical and commercial bids from experienced and capable bidders for planning, executing and submit an audit report. The evaluation criteria for technical and commercial bids are given in clauses 11.1 and 11.2 respectively. The entire work should be undertaken on a turnkey basis. Further, the bidding process shall involve the following steps:

a) Issue of Tender Notification :This RFP is made available at the Institute's web site www.iibf.org.in/tender.

b) Pre-bid meeting

The pre-bid meeting may be held via zoom meeting tool on the scheduled date as Mentioned in clause 8.All the queries received from the bidders shall be taken up and shall be answered/clarified by the Institute.

The responses to the pre-bid bid queries and/or any further changes in the RFP shall be communicated to the bidders during the meeting and the final outcome shall be uploaded on the website and shall be placed under the URL: www.iibf.org.in/tender. The bidders who submit the pre-bid queries and unable to attend the pre-bid meeting may download the outcome of the pre-bid meeting from the website subsequently.

9.Schedule of activities of Bidding:

The schedule of activities of bidding process is as under:

Sr. No	Description	* Date
1	Date of Releasing the Request for Proposal (RFP)	27th August– 2020
2	Last date of submission of written requests for any Clarifications from prospective bidders. Queries may be sent to the e-mail id: gnrao@iibf.org.in or amodrele@iibf.org.in	8th September - 2020
3	Pre-bid meeting for clarifications on written Queries	18th September – 2020
4	Last date of submission of Proposals by e-mail up to 5PM	28th September – 2020
5	Examining the technical bids by the tender committee	29th September – 2020
6	Technical presentations from the bidders f r o m 1 1 A M o n w a r d s	1stOctober- - 2020
7	Opening of commercial bids in the presence of bidders who qualify in the technical round	7th October-2020

***Tentative dates:**

The above dates are tentative and IIBF reserves the right at its discretion to change the schedule of activities, including the indicated dates.

10.Minimum Eligibility Criteria:

Sr.	Minimum Eligibility Criteria	Supporting Document
a.	The bidder should be a firm / Pvt. Ltd / limited company registered under the Indian Companies Act, 1956.	Registration certificate Firm / Public / Pvt Ltd. / Ltd. Co.
b.	The bidder should have registered a turnover of Rs.25 lakhs or above during each year for the last three completed financial years.	Self certified copies of the audited balance sheet and profit & loss statement for the last 3 completed financial years.
c.	The bidder should be earning a Net Profit or having +ve Net Worth in each of the last three completed financial years.	Self certified copies of the audited balance sheet and profit & loss statement for the last 3 completed financial years.

d.	The bidder should have executed at least three orders of similar nature / value and preferably in multiple locations of Educational Institutes	• PO • Project completion report
e.	The bidder should provide the proof of accreditation to Quality Management Systems like ISO 9001:2008 or 2015/ SEI CMMI Level 5 / Six Sigma practice(Minimum one certificate is preferable)	Copy of the Certificate
f.	The bidder should posses qualified(with **CISA/ DISA /CISSP /CISM / GIAC(SANS)** at least) IS auditors having minimum 5 years of experience to carryout the IS audit seamlessly.	Self certified statement indicating Number of IS Auditors with qualifications and no. of year/s of experience.
g.	The bidder should not have been blacklisted by any department or undertaking of the Government of India and the Government of Maharashtra or other state governments or any public sector banks	A self declaration letter from the company secretary of the organization to be enclosed

Note:

- Necessary supporting documents should be arranged / numbered in the same order as mentioned above.
- Failure to meet any of these criteria will disqualify the bidder and will be eliminated from the further process.
- The Institute reserves the right to verify and/ or to evaluate the claims made under eligibility criteria. The decision of the Institute, in this regard shall be final, conclusive and binding upon the bidder.
- 'Project Completion Report' should include references of customers for whom website development projects of similar complexity / size / cost have been successfully implemented and is/are in operation. Provide the details of hardware, operating systems, application software, size of network, size of database etc., and certificates from the clients regarding the performance of such solutions provided.

11.Conflict of Interest:

Any bidder who is in a similar business as that of IIBF in the areas of education, training and certification, will not be considered and no correspondence or queries shall be entertained from such bidder. Institute's decision in this regard shall be final and binding on the bidder.

12.Evaluation of Bids:

The bidders should note that the Technical Proposals shall be evaluated first, for technical suitability. The commercial Proposals of bidders who get qualified in the Technical round shall be opened subsequently. The commercial proposals of bidders who could not qualify in technical round shall be returned back without opening.

The technical proposals will be evaluated as per the clause 11.1 given in this RFP.

12.1.Technical Evaluation:

The total points to be awarded in the technical round will be as under:

Sr.No	Description	Points Earmarked
1	Capability of the Agency and Number of auditors Qualified with **CISA/ DISA /CISSP /CISM / GIAC(SANS)**	40
2	Proposed Audit approach to be adopted	20
3	Projects Handled	20
4	Past Experience	10
5	Support/References	10

Mechanism of awarding Technical Scores to bids:

The bidder/s who score/s highest points will be awarded with full Technical weightage of 70 marks, and accordingly the second highest; third highest scores will be calculated in proportion to the highest points obtained by a bidder in the technical round.

For example:

Suppose in response to the RFP, 3 bids are received from Bidder A, Bidder B & Bidder C then their scores will be calculated as under:

Assume, the bidders obtain the points as given below, based on the techno functional features:

Bidder A gets - 65 points,

Bidder B gets - 70 points

and Bidder C gets – 90 points

As technical points are given 70% of weightage, the technical scores of each bidder are calculated as under: (arriving points proportionately with the highest points

divided by points obtained by a bidder and multiplied by the technical weightage ie. 70)

The technical score of Bidder C will be = points awarded to C' (90)

---------- x 70 =70

Points awarded to C' (90)

$$\text{The technical score of bidder A will be} = \frac{\text{Bidder A's score (65)}}{\text{Bidder C's score (90)}} \times 70 = 51$$

$$\text{The technical score of bidder B will be} = \frac{\text{Bidder B's score (70)}}{\text{Bidder C's score (90)}} \times 70 = 54$$

Note:

- **Bidders who score 70% or above points/marks (will be rounded to nearest integer) in technical round will only <u>be considered as qualified in the round</u>**
- **Bidders who obtain less than 70% points/marks in the technical round shall not be considered for the next process of bidding**
- **No further discussions/interactions will be entertained with a bidder/s who could not qualify in the technical round**
- **The bidder/s who could not qualify in the technical round shall be intimated accordingly. Their EMD and commercial bids(unopened) will be returned to them.**

12.2.Commercial Evaluation:

The commercial bids will be opened in the presence of qualified bidders as per the schedule date given in clause No. 8 of this RFP.

A commercial bid which carries the lowest cost will be given the full weightage of 30 points and other bids are rated in inversely proportional to their prices.

As commercial bids are given 30% of weightage, the commercial score of each bidder is calculated as under:(arriving points in inversely proportional with the lowest price divided by the price offered by a bidder and multiplied by the commercial weightage ie., 30).

For example: Suppose the price quoted by the qualified bidders are as under:

Price quoted by bidder 'A'is = Rs.120/Price quoted by bidder 'B'is = Rs.100/-

Price quoted by bidder 'C'is = Rs.110/-

In this case, bidder 'B' will get full'30' points as it is lowest among others.

$$\text{The commercial score of bidder 'A' will be} = \frac{\text{Bidder B's price(100)}}{\text{Bidder 'A' price (120)}} \times 30 = 25$$

$$\text{The commercial score of bidder 'C' will be} = \frac{\text{Bidder B's price (100)}}{\text{Bidder C's price (110)}} \times 30 = 27$$

The weightages of technical and commercials will be added together to arrive at the Total weightage out of hundred marks for each bidder. The bidder who secures the highest combined weightage will be ranked as H1, second highest as H2 and third highest as H3.

The "H1" bidder shall be awarded the contract after due negotiation of price or otherwise.

Example:

From the above examples, the combined Technical and Financial scores of the bidders would be ranked as under:

Bidder A = 51 + 25 = 76 = H3

Bidder B = 54 + 30 = 84 = H2

Bidder C = 70 + 27 = 97 = H1

The proposal from bidder C of Rs.110.00 will be considered as most responsive bid and it may be called for further price negotiations, if needed.

IIBF reserves the right to negotiate with the vendor who obtains 'H1' score before awarding the contract.

IIBF's decision in respect of evaluation methodology and short-listing the bidders shall be final and no claims whatsoever in this matter will be entertained.

12.3. Proposal Format:

- The technical proposals should be submitted in a soft copy with a password protection. and be marked as "**Proposal for conducting IS Audit of the Institute"-** '**Technical- Information only'.**
- The proposals should be forwarded to Dr.Sudhir M Galande Dy.CEO to the e-mail id: sudhirmg@iibf.org.in along with the passwords.
- A bidder should submit the proposals with clarity & proper pagination so that the papers are not lost
- The proposals, that are not sealed or responses to RFP sent by e-mails will be summarily rejected
- The proposals that are not submitted in the prescribed format or incomplete in details are liable for rejection.
- The proposals containing unauthenticated erasing or alterations will not be considered.

12.4. Contents of the Technical Proposal:

- A company shall submit a letter through its duly authorized official bearing his/her name and designation. The letter shall include, a statement of proprietary information, if any.
- Table of Contents (List of documents enclosed)
- Detailed technical specifications/brochures of the solutions proposed.
- Detailed architecture of the proposed solution with all the features/functions of the systems. This should also include details of the hardware system that will be used to host the web site and contents even though it is a hosted model.
- Proof of implementation of similar project.
- Resume of the proposed Project Management team with Name, Designation, qualification & experience details.

- Specify the Hardware, Operating System, Software licenses, bandwidth required for successful implementation.

- Technical proposal should **not** indicate any cost aspect directly or indirectly.

12.5. Inputs of commercials:

- The bidders should submit commercial bids in a separate soft copy protected with a password. . and be marked as "**Proposal for conducting IS Audit of the Institute"** '**Commercial - Information only'.**

- The commercial proposals should be forwarded to Dr.Sudhir M Galande to the e-mail id: sudhirmg@iibf.org.in along with the passwords.

The bidders must provide all the relevant information of price and not contradict the technical proposal in any manner. **All prices must be quoted in Indian Rupees only**.

The prices offered shall hold good for a period of six months from the date of receipt of the proposals. These prices shall not change till the end of audit period after acceptance of the order letter by the bidder.

13. Acceptance of Audit Report/s:

At the end of the successful completion of the audit and submission of audit report, the Institute shall provide a sign- off towards completion of the audit.

14. Terms and Conditions:

- The bidders must sign / initial on all the pages of the RFP and give an undertaking that they have understood all the terms and conditions as specified in the RFP and shall abide them. This has to be done while submitting the bid/s.

- In case if any bidder seeks to clarify any terms of RFP or have doubts, such clarifications should be raised at the time of pre-bid meeting only. After pre-bid meeting, no deviation from the RFP terms shall be entertained and if any bidder is found to have deviated from the RFP terms, their bids will be rejected and they will be disqualified from the RFP process.

- The bidder must provide a Project Manager who shall act as a single point of contact for all activities regarding this project. The Project Manager(PM) should make on-site decisions regarding scope of the work and any other changes required therein. The bidder should not

change the project manager during the currency of the project as far as possible. In case if it is imminent to change the Project Manager the out going PM should properly handhold the project to the incoming PM.

- The bidder shall provide all reference manuals, booklets, e-books and other materials required to maintain the systems effectively in soft copy.

- The technical proposal will be evaluated based on the technical inputs as well as compliance of terms and conditions mentioned in the RFP.

- Functional & technical information of the solution being offered must be provided in the exact format as given in RFP.

- The bidder shall bear all costs associated with preparation and submission of the proposal, attending pre-bid meeting or arranging product walk through and technical presentations etc.

- The Institute may call for any clarification from all or any of the bidders in connection with their offers.

- The bidder shall be responsible to provide complete documentation of the audit (soft copy) which should cover the following:

    - Audit plan
    - Approach of Audit, Tools used for Audit
    - Audit Reports

- Bidder shall submit progress report of the project as per clause No.17 (Project Schedule) of this RFP. Bidder will be responsible to implement appropriate project control measures and report the same to Institute in timely manner.

- Any effort by a bidder to influence IIBF on any matter relating to the proposal, its
  evaluation, comparison, selection may result in rejection of the bidder's proposal.

15.Earnest Money Deposit (EMD):

- A bidder who is interested to respond to the RFP, should deposit an earnest money of Rs.35,000/- (Rupees thirty five thousand only) in the form of a Bank Guarantee from any commercial bank, which is valid for six months favouring to IIBF and payable at Mumbai. The bidder may use any format of bank guarantee from any commercial bank.

- The Bank Guarantee(BG) may be submitted in a soft copy with digital signature if possible or the bidder may submit the scanned copy of bank guarantee and the original may be submitted at the time of picking up the order. The soft copy of BG should be accompanied by the technical bid. The EMD will not carry any interest.

15. 1.Refund of EMD:

- EMD is refundable to unsuccessful bidders after completion of RFP process i.e. after declaration of successful bidder of the RFP process.
- The bank guarantee towards EMD of the successful bidder shall be refunded after execution and submission of audit report.

15.2. Forfeiture of EMD:

The EMD (earnest money) submitted by the bidder towards RFP will be forfeited if the bidder-

- Withdraws the bid after acceptance of the bid by IIBF; or
- Withdraws the bid before the expiry of the valid period of the RFP; or
- Violates any of the provisions of the terms and condition of the RFP
- Or in case the successful bidder picks up the order and does not proceed with the project. This period will be decided by the Institute.

16.Rejection of Bids:

The bids are liable to be rejected if:-

1) Received after the expiry of the due date and time.
2) Not received with password protection.
3) It is a conditional bid.
4) Not in conformity with the terms and conditions mentioned in the RFP.
5) It is incomplete including non-furnishing of the requisite documents.

IIBF reserves the right to reject the bid/s without assigning any reasons. The decision of IIBF will be final, and no communication whatsoever will be entertained in this regard.

17.Project Schedule:

The successful bidder should conduct the IS Audit and complete the same within 3 calendar months from the date of issue of work order, as time is the essence of the contract.

18.Penalty for delay of Assignment:

The Institute shall impose a penalty of Rs.5000/- per week delay attributable to bidder towards the final delivery of audit findings and reports beyond the project schedule given in clause 17 of the RFP. The contract may be terminated if the total penalty crosses more than 10% of the project cost. There shall be no penalty if the delay is attributable to the Institute. However, the bidder should reasonably prove that such delays are attributable to the Institute.

19.Deliverables: Audit Findings and Reports:

The bidders must submit the Risk analysis report along with Risk Matrix with scoring model as part of the IS audit findings.

The following reports should be delivered for each area of auditing-

1) IS Audit (Technical & Process) Report of all the areas covering the objectives, efficiency and effectiveness
2) Presentation to the Top Management of the findings of the Reports
3) Risk Analysis Report
4) Recommendations for Risk Mitigation
5) Gap analysis and recommendation for mitigation
6) The check list with guidelines for the subsequent audit (hard & soft copies)

The report findings should cover all the areas mentioned in broad and details the scope of the work given under clause 7 and Annexure-II of the RFP.

20.Termination of contract:

Both the parties can terminate the contract by giving three months notice in writing:

i. In the event of bidder choosing to terminate the contract the Institute reserves the right to invoke performance bank guarantee and/or take such other steps as deemed necessary.

ii. IIBF may at its discretion terminate the contract if it is found that the services rendered by the bidder are not satisfactory and may invoke performance guarantee.

21.Payment Schedule:

The entire payment shall be made after completion of IS Audit, submission of audit findings and reports.

22.Non-Disclosure:

The contents of the proposal and all the project outputs should not be disclosed to any party unless Bidder and IIBF mutually agree in writing to the same. Bidder will not use the contents of this proposal to bid for any other contract.

The IPR of the content will vest with IIBF and the bidder agrees to deliver the content to IIBF at the end of the contract period.

23.Reservation of rights of IIBF:

The Institute reserves the right to change / add / modify / relax any / all conditions stipulated or increase / decrease items requested as also to accept / reject any / all offers without assigning any reasons whatsoever.

The Institute also reserves the right to cancel this RFP or go for a fresh one with or without any amendments without any liability or any obligations.

The decision of the Institute in selecting the bidder would be final and conclusive and the Institute will not entertain any correspondence in this regard.

The Institute also reserves the right to:

- Waive or Change any formalities, irregularities, or inconsistencies in proposal format delivery
- To negotiate any aspect of proposal with any bidder and negotiate with more than one bidder at a time
- Extend the time for submission of proposals

24.Adherence to Terms and Conditions:

The bidders who wish to submit responses to this RFP should note that they shall abide by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the bidders, such bids are liable to be disqualified and may not be considered for the selection process.

25.Notification of the Contract:

The Institute shall inform the outcome of the RFP process with the successful bidder in writing. The Institute is not obliged to inform the outcome of the RFP with the unsuccessful bidders or cite any reasons thereof.

26.Last date of Submission of Proposals:

Bidders are requested to offer the best price, and submit the bids abiding all terms and conditions on or before **28th September -2020 by 5.00 pm** in soft copies with password protected . The proposals should be labelled as **'Proposal for conducting IS Audit of the Institute' (Technical-Information only) 'Proposal for conducting IS Audit of the Institute' (Commercial-Information only).**

The technical and commercial proposals should be Addressed to:

Chief Executive Officer
Indian Institute of Banking & Finance Kohinoor City,
Commercial II, Tower I,
Second Floor, Kirol Road, Kurla-West
Mumbai – 400 070.

Note:

The soft copies of technical and commercial proposals should be forwarded to:

Dr. Sudhir M Galande, Dy.CEO to the e-mail id: **sudhirmg@iibf.org.in** with due password protection.

Annexure-I

Detailed Scope of the Work

Given below is the indicative scope of the work and is not restricted to the items mentioned.

I. Information Security Architecture:

- o Information Security Organisation Structure
- o Roles and Responsibilities
- o Application Security Policy
- o Password Security Policy
- o Data Centre Security & Monitoring
- o Virus control Policy
- o Backup Policy
- o Physical security policy
- o Environment security policy
- o Incident Management PolicySecurity of conduct of examinations through service providers
- o Business continuity and Disaster recovery plan

II. Data Centre/Server Room Audit:

- o IS Audit of Data Centre operations Candidate Life Cycle Management System
  - (i)Physical security
  - (ii)Physical access controls;
  - Environment management systems such as electrical supply, UPS, air-conditioning, fire detection and suppression, generator, etc.

- o Operating System (OS)
  a) Set up and maintenance of operating system parameters;
  b) Updating of OS Patches;
  c) OS Change Management Procedures;
  d) Use of root and other sensitive passwords;
  e) Use of sensitive system software utilities;
  f) Interfaces with external applications (such as payment gateways)
  g) Hardening of Operating System.

III. Application Software Audit:

a) Authorisation Control such as concept of maker checker, exceptions, and error conditions.
b) Authentication mechanism.
c) User Management & Password Management

d) Parameter Maintenance
e) Access rights;
f) Access logs/ Audit Trail generation;
g) Change management procedures including procedures for testing;

IV. Database Audit:

a) Secure use of SQL;
b) Control procedures to safeguard parameter files;
c) Logical access controls;
d) Control procedures to safeguard sensitive database passwords;
e) Control procedures of purging Data Files;
f) Procedures for data backup, restoration, recovery and readability of backup data

V. Website Audit:

- To assess flaws in software used for website hosting including security of web server, application server and design of the applications.
- Audit password-cracking tools that are used to guess them by repeated malicious attempts.
- Search for back-door traps in the software.
- Audit for malicious attempts of Distributed Denial of Services (DDOS) and Denial of Services (DOS) attacks.
- Audit the attempts of penetration through perceivable network equipment/addressing and other vulnerabilities.
- Check Vulnerabilities like IP Spoofing, Buffer Overflows, session hijacks, account spoofing, Frame spoofing, Caching of web pages, cross site scripting, cookies handling, injection flaws

o Check system of penetration testing and its effectiveness
o Sniffing:
  o 128-bit SSL Certificate & PKI verification.
  o Whether solution architecture provides 24 X 7 availability to customer .
  o To check whether date and time stamp are appearing correctly on all reports.
  o To check whether servers are updated with latest security patches. Remote server Management Software used, Web server is up to date, IOS version in Router is vulnerable one.

- Confirm whether the Rule based configuration is done in Firewall properly.
- To ascertain IDS are configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized. Make sure the IP routing is disabled.
- Confirm whether Maker-Checker concept is followed while changing system parameters.
- Check Logical Access Controls Techniques viz. Passwords, Smart Cards or Other Biometric Technologies.
- Make sure Proxy Server is deployed between Internet and proxy systems.

- Find out the vulnerabilities of unnecessary utilities residing on Application server.
- Computer Access, messages are logged and security violations reported and acted upon.
- Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
- Proper infrastructure and schedule for back up is fixed, testing of back-up data done to ensure readability.
- Legal issues : Electronic Record is authenticated by Asymmetric Cryptosystem and hash function.
- Secrecy and confidentiality of Customer preserved.
- If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought.
- Regulatory and Supervisory issues.:
- Any other items relevant in the case of security.
- All the guidelines issued by CERT-IN should be adhered with regard to online services offered by the Institute.

VI. Security Audit of Network Management:

- Network admission control
- Hardening of systems, switches and routers
- Patch update Management
- Port based security controls
- Process control for change management
- security incident and management
- access control for DMZ application
- control filtering for web access and data leakage
- Net scanning-vulnerability assessment
- Network admission control, hardening of system, switches routers, port based security control
- Penetration testing
- Password cracking
- Intrusion detection system testing
- Router testing
- Denial of Services testing
- While doing the penetration test on server in live environment the ISA should ensure optimum performance of the System.
- Audit of Network design from security, integrity and availability point of view.
- Audit of setting of Network equipment from security and functionality point of view
- Evaluation of Firewall policy and its implementation.
- Network performance testing (including suggestions for increasing the performance)
- Review of appropriateness of the network topology

- Review of adequacy or otherwise of the hardware installed.
- Network stress / Load test
- Network Information Security and Administration

VII-Disaster Recovery Site - BCP:

IS Audit of DR Site with respect to

1. Disaster Recovery Plan/Policy of the Institute
2. Log shipping management

Review the Disaster Recovery Plan/Procedures and its implementation by the cloud vendor at the Data Centre and Disaster Recovery Site

Annexure – II

Commercial Template for conducting IS Audit in the Institute

Sr. No	Particulars	Amount in (Rs.)
1	One time charges for conducting IS Audit of the Institute	

Note: The charges should be quoted exclusive of taxes. Taxes shall be paid at actuals as applicable