

 <p>बैंक ऑफ महाराष्ट्र Bank of Maharashtra भारत सरकार का उद्यम एक परिवार एक बैंक</p>	<p>निरीक्षण व लेखा परीक्षा विभाग Inspection & Audit Department प्रधान कार्यालय: लोकमंगल, 1501, शिवाजीनगर, पुणे-5 Head Office: LOKMANGAL, 1501, SHIVAJINAGAR, PUNE-5 टेलीफोन/TELE :020-25614383, 25614343 ई-मेल/e-mail : agminsp@mahabank.co.in</p>	 <p>स्वच्छ भारत एक कदम स्वच्छता की ओर 'स्वच्छता अभियान' की सफलता हेतु हम प्रतिबद्ध हैं</p>
--	--	---

**EXPRESSION OF INTEREST (EOI) FOR
EMPANELMENT OF INFORMATION
SYSTEMS (IS) AUDITORS
[EOI Ref #BOM/IAD/ISA/03/2019]**

Bank of Maharashtra Head Office, Pune invites applications in the prescribed format from the Firms / Companies / Organizations who are conducting Information Systems Audit and willing to have their Firm / Company / Organization empaneled for carrying out Information System Audit of IT systems / applications used by the Bank.

The format for application along with the details regarding eligibility criteria, other terms & conditions and scope of work can be obtained from the Bank's website <https://www.bankofmaharashtra.in> under "Tenders".

The duly filled in application form (along with required authenticated proofs) in sealed cover superscribed as 'Application for Empanelment of Information Systems Auditor – EOI Ref #BOM/IAD/ISA/03/2019' should reach this office **on or before 18-04-2019 by 2:00 p.m.** at the above address.

The sealed EOI responses received will be opened in the presence of bidder representatives who choose to attend the opening of EOI responses **on 18/04/2019 at 16:00 Hrs.**

**Deputy General Manager
Inspection & Audit Dept**

**CRITERIA AND TERMS & CONDITIONS FOR EMPANELMENT OF
INFORMATION SYSTEMS (IS) AUDITOR**

ELIGIBILITY CRITERIA:

Audit Firms / Companies / Organizations fulfilling the following criteria are only eligible to respond to this EOI document. **The Audit Firms / Companies / Organizations are required to submit authenticated proof in support of each of the item listed in the eligibility criteria.**

1. Should have at least one qualified CISA (Certified Information Systems Auditor from ISACA), as Member.
2. Should have proven track record of conducting a number of Information Systems Audits (including VA & PT) during the last 3 years. The Audit Firms / Companies / Organizations that have conducted Information Systems Audit of Systems such as Core Banking Solution (eg. Bancs24), EFT Switch, Internet Banking, Mobile Banking, DR Site including VA & PT Testing etc in at least one Commercial Bank / Public Sector Organization / Statutory Body during the last 3 years shall be preferred.
3. CERT-in empanelment is mandatory.
4. Having unblemished track record and should not have been blacklisted by any Financial Institution / other organizations / any government department. Further, the name of the Audit Firm / Company / Organization or its promoter/ partner etc. should not be in the defaulters / barred / caution list published / displayed at websites of public bodies such as by RBI / IBA / ECGC / SEBI / CICs etc. **The Audit firm / company / organization should furnish self-attested affidavit on stamp paper in this regard.**
5. Should have office at a major centre of the country, preferably Pune / Mumbai.

OTHER TERMS & CONDITIONS:

- i) The Empanelment of IS Auditor will be purely the prerogative of the Bank. Such empanelment will be for a maximum period of 2 years from the date of empanelment.
- ii) Application on the Letter Head of the Audit Firm/Company/Organization in the format placed below (along with required authenticated proofs) should be submitted to Deputy General Manager, Inspection & Audit Dept., Bank of Maharashtra, Head Office, Lokmangal, Shivajinagar, Pune - 411005, Maharashtra, as per the 'Tenders' Link on the Bank's website <https://www.bankofmaharashtra.in>
- iii) Usual KYC norms like Identity and address proof of Firm/Company/Organization are mandatory.
- iv) PAN Number and GST Registration Number are mandatory for applicant.
- v) The Audit Firms / Companies / Organizations should have taken up the Information Systems Audit assignments on their own without subcontracting the assignment.
- vi) Wherever any of the Proprietor / Partner / Director of the Audit Firm / Company / Organization is related to any of the employees / Directors of the Bank, the relationship with such employees / Directors should be specifically mentioned in the application form.
- vii) The Application Form should be in printed format duly authenticated by the Authorized Signatory (viz. Bidder or any person duly authorized to bind the bidder to the contract). The Authorized Signatory should give a declaration and through authenticated documentary evidence establish that the person is empowered to sign the Application Form & related EOI documents and bind the bidder. All pages of the Application Form & related EOI documents except brochures if any are to be signed by the authorized signatory.
- viii) The Application Form & related EOI documents should contain no interlineations,

erasures or over-writings except as necessary to correct errors made by the Bidder. In such cases, the person/s signing the EOI response document should initial such corrections.

- ix) The Application Form & related EOI documents submitted to Bank should not bear any corrections, alterations, over writings and additions in hand writing.
- x) Bank will have the right to seek more information in due course, if considered necessary.
- xi) Bank will not entertain applications from firms / companies / organizations or their subsidiaries who have provided relevant consultancy, supplying of the systems, system development, and maintenance and/or integration related to IT or networking services or have rendered such services during the preceding 36 months to the Bank.
- xii) The applications received by the Bank will be screened by a Committee of Executives constituted for this purpose, which will consider empanelment of Audit Firms/Companies/Organizations for Information Systems Audits based on their Information Systems Audit experience, CISA certified staff, number of qualified staff employed, work experience, office location, number of offices etc and any other factor considered necessary by the Committee for which the Decision of the Committee shall be final.
- xiii) Only the Audit Firm / Company / Organization provisionally selected for empanelment will be communicated through email. No individual intimation will be sent to the Audit Firm / Company / Organization whose application is not considered for empanelment. No further correspondence will be entertained in this regard.
- xiv) Bank reserves the right to reject any or all applications for empanelment without assigning any reasons therefor.
- xv) Depending on the requirement of the Bank, the empanelled firm / company / organization will be approached for closed tendering process of various Information System Audits during the period of 2 years from the date of empanelment. The Audit Firm / Company / Organization finally selected (after closed tendering process) will be required to sign & submit Non-Disclosure Agreement to the Bank, before undertaking any assignment.
- xvi) Bank would always have the option to cancel the empanelment of the auditing firm / company / organization without any justification to them.
- xvii) The Information System Auditor will be evaluated on the basis of its performance and usefulness to the Bank during review of empanelment by the Bank at annual interval or as convenient to the bank.
- xviii) In the event of gross negligence / malpractices noticed by the Bank in the Information System Auditor's conduct / scope of work, apart from depaneling the firm / company / organization, the Bank reserves the right to include their names in the cautionary list for circulation to all the Banks through IBA.
- xix) The Bank may maintain a cooling period at its discretion in case of Information Systems Audit of same IT System/Setup of the Bank, by the same Audit Firm / Company / Organization in past 36 months.
- xx) In competing for and if selected, in executing the agreements, the Audit Firm / Company / Organization will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
- xxi) If the empanelled Information System (IS) Auditor(s) not responding to the quotation / inquiry by Bank on three occasions during the validity of the panel, they may be delisted from the panel by the Bank.
- xxii) The empanelled Information System (IS) Auditor(s) shall be required to submit satisfactory documentary evidence for carrying out a background check on the personnel (if required) to be engaged in audit assignment for the Bank before their deployment.
- xxiii) Bank reserves the right to limit the number of IS Audits that can be concurrently executed by a firm for the Bank.
- xxiv) The empanelled Information System (IS) Auditor(s) shall undertake to keep confidential all the information that they have access to during the course of their assignments within the bank.

- xxv) The empanelled Information System (IS) Auditor(s) shall ensure adherence to applicable codes of conduct and auditing standards with due professional care.
- xxvi) The empanelment status of the empanelled Information System (IS) Auditor(s) depends on the quality of service rendered by them and the extent of Bank's satisfaction.
- xxvii) The empanelled Information System (IS) Auditor(s) shall not use Bank of Maharashtra's logo and/or the reference of their association with Bank of Maharashtra in any manner that would bring the Audit Service or Bank of Maharashtra into disrepute.
- xxviii) The Bank reserves the right to make any changes in the terms and conditions, if required.

SCOPE OF WORK

A brief overview of different audit engagements is mentioned below:

Audit Domain	Audit Objective	High-Level Audit Scope
Information Systems Audit	Perform Information Systems Audit based on the requirement of the Bank, in view of but not limited to implementation of new application, change of application, change in Hardware and Network infrastructure, Regulatory / Statutory requirements etc.	Scope of Audit will be communicated based on the requirement of the Bank. It may include Application Functionality and Controls Review/Audit, Functional Vulnerability Assessment / Penetration Testing, Source Code Review, etc.
IT Application Management	Review the application management activity at the Bank to seek assurance that adequate degree of controls are in place for authentication and data processing.	<ul style="list-style-type: none"> • Access Management • Change Management • Incident Management including Service Level Management • Data Processing i.e. Input / Output • Security Assessment of Bank's Internet, Intranet Sites and Mobile Phone Apps • Critical IT Applications • Regulatory and Software License compliance • Vulnerability Assessment / Penetration Testing • Capacity Planning • Review SOPs, AMCs, Service Level Agreements (SLA) for Scope, Validity and Adherence to standards / contracted service levels. • OWASP 10 controls.
Data Center Audit	Review the effectiveness of the process, infrastructure and technology utilised for data center management.	<ul style="list-style-type: none"> • DR Plan Review • Review Data Center Infrastructure • Capacity Planning • Backup and Storage Management • Service Level Agreement Management • Asset Inventory preparation • Configuration management • Change management • Physical and logical security • Access management • Review of various controls in place • Review of Asset Inventory provided by Functional Division • Review SOPs, AMCs, Service Level Agreements (SLA) for Scope, Validity and

		Adherence to standards / contracted service levels.
Independent Assurance of IS Audit Function	<ul style="list-style-type: none"> • Assess efficiency & effectiveness of IS Audit for current and future business goals • Determine value addition from IS Audit to the business units Benchmark, identify and recommend successful practices of Internal Audit. 	<ul style="list-style-type: none"> • Current IS Audit Scope review • IS Audit Approach • Review of IS Audit Reports • IS Audit Policy Review • Skill Enhancement of IS Audit Function for Risk Assessment • Technical Evaluation of available CAAT tools and VA/PT tools • IS Audit Roadmap – 2019-22

In addition to the above, Post Compliance Review/verification cum closure report may also be incorporated in the scope of the Audits.

The above stated activities may primarily be performed at Pune, Mumbai & Hyderabad.

**FORMAT FOR APPLICATION FOR EMPANELMENT AS
INFORMATION SYSTEMS AUDITOR
[EOI Ref #BOM/IAD/ISA/03/2019]**

Sr	Item	Details	Documentary evidence required to be enclosed (Duly Authenticated)
1	Name of the Firm/Company/Organization		Copy of the Certificate of Incorporation along with copy of Latest Audited Balance Sheet.
2	Complete Postal Address		Identity & Address proof.
3	Office Telephone Numbers / Fax		
4	Mobile Numbers		
5	E-mail Address		
6	Constitution		
7	Date of Establishment		
8	PAN of the Firm/Company/Organization (Mandatory)		
9	GST Registration Number (Mandatory)		
10	Location of all offices / branches		List of all branches / offices with contact person, telephone numbers & address.
11	Name and Address of the Partners / Directors (If Partnership Firm / Pvt. Ltd. Co.)		
12	Name, Designation and Contact Details of the person, authorized to deal with the Bank		Letter of Authorization on Letter head of Firm/Company/Organization.
13	Carrying out Information Systems Audits since <year>		
14	Details of Information Systems Audits (including VA & PT) conducted in last 12 months	<Should include Name of Client, Information System/s Audited, List of Locations, Scope of IS Audit, Date of PO, Date of Project Commencement, Date of Successful completion of IS Audit Assignment; Name of person who can be referred to from Client's side with their name, designation, postal	<ul style="list-style-type: none"> - Copies of the Purchase Orders - Experience certificates from the respective Clients.

		address, contact phone, email ID etc.	
15	Details of Technical Manpower deployed for Information System Audits including Name of the Employee, Duration with Organization, Experience in Information Systems Audit & Details of qualifications including CISA.		CISA Certification proof.
16	Must be included in the latest panel of Information Systems Auditors maintained by CERT-in, as on date.		Proof of CERT-In Empanelment.
17	Specify largest Information system audit project handled in terms of scope along with project value.		Copy of this Purchase Order.
18	Whether Outsourcing Information System Audit work to External Information System Auditors / Experts: (Yes / No)		
19	Any other special type of audits conducted, if any		
20	Areas of specialization of the Firm		
21	Any other relevant Details		

I / We confirm that the information furnished above is true and correct and we have not been de-paneled / black listed by any organization in the past and we fulfill all the conditions of eligibility of empanelment with Bank of Maharashtra as Information System Auditors.

The authenticated proofs in support of each of the items listed in the eligibility criteria is also enclosed.

I / We confirm that we accept and will abide by all the terms & conditions contained in the EOI Ref #BOM/IAD/ISA/03/2019. Copy of Pages 2 to 6 of the said EOI, duly stamped & signed by me/us is enclosed.

Place:

Date: <Seal of the Audit Firm/Company/Organization> Authorized Signatory