Bank of Maharashtra
(One Family… One Bank… Mahabank)

Expression of Interest (EOI) for Information Security Audit of Various IT Services and branches

EOI REFERENCE # <092020>

बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
ONE FAMILY ONE BANK

Central Office, 'LOKMANGAL'
1501, Shivaji Nagar, Pune – 411 005

Cost of EOI: Rs.17,700/-

Invitation for EOI offers:

Bank of Maharashtra invites Expression of Interest (EOI) responses (Technical responses) to appoint a service provider to conduct Information Security Audit of various IT services and branches. Bank of Maharashtra is inviting technical proposals from the capable firms for conducting work as per the scope of work mentioned in this Expression of Interest (EOI) document

The purpose of this Expression of Interest ("EOI") is solely to enable Bank of Maharashtra ("Bank") in defining the requirements for Appointment of service provider to conduct Information Security Audit of various IT services and branches and empanelment of eligible bidders for the period of contract.

No contractual obligation on behalf of Bank of Maharashtra whatsoever shall arise from the EOI process unless and until a formal contract is signed and executed by duly authorized officers of Bank of Maharashtra and the bidder.

The Bank may modify any / all of the terms of this EOI and shall be entitled to invite RFP from eligible EOI Respondents. This EOI will provide the detailed scope of work.

A complete EOI document may be obtained from
Bank of Maharashtra
CISO Cell, IRM Dept, Head Office, Lokmangal, 1501, Shivajinagar,
Pune – 411 005 or can be downloaded from the site bankofmaharashtra.in

EOI Response Submission:

EOI Reference number	**092020**
Price of EOI copy	**Rs.17,700/- (Including GST)**
Date of commencement of issue of EOI document	16/09//2020
Last Date of sale of EOI document	14/10/2020 14:00 Hours
Queries to be mailed by	30/09/2020
Pre Bid Meeting	05/10/2020 11:00 Hours
Last Date and Time for receipt of EOI offers	14/10/2020 14:00 Hours
Time & Date of opening of technical bids	14/10/2020 15:00 Hours
Address of Communication	Bank of Maharashtra CISO Cell, IRM Dept, Head Office, Lokmangal, 1501, Shivajinagar, Pune – 411 005
Contact Telephone Numbers	020-25614351
E-mail Id	tanvi.kochhar@mahabank.co.in, akshay.mahajan@mahabank.co.in, ciso@mahabank.co.in
Website	www.bankofmaharashtra.in
Last Date of submission of EOI response	14/10/2020 14:00 Hours
Address for submitting Response	Bank of Maharashtra CISO Cell, IRM Dept, Head Office, Lokmangal, 1501, Shivajinagar, Pune – 411 005
Address of Communication	As above
Contact Telephone Numbers	020-25614351

Applicants have to purchase EOI document to participate in pre-bid meeting. Procurements for MSMEs will be as per the policy guidelines issued by Ministry of Micro, Small and Medium Enterprises (MSME), GOI from time to time.

Please note that the prospective bidder needs to purchase the EoI document from the Bank will commence an online pre bid meeting on 05/10/2020 at 11:00 Hours.. In case the prospective Service Provider downloads the document from website of the Bank, the cost of EOI document should be paid along with the Bid response. However, **in order to participate in the pre-bid meeting, the EOI document must be purchased by the prospective bidder.**

Procurements for MSMEs will be as per the policy guidelines issued by Ministry of Micro, Small and Medium Enterprises (MSME), GOI from time to time. MSMEs registered under the SPRS (Single Point Registration Scheme) of NSIC and complying with all the guidelines thereunder as well as those issued by GOI from time to time shall be eligible. MSMEs meeting all the eligibility criteria laid down in this shall be eligible to bid for this RFP. Exemptions regarding Tender document fees and EMD shall be available to the eligible MSMEs. Applicable guidelines for PPP-MII Public Procurement (Preference to Make in India), Order 2017 shall be applicable to eligible bidders.

Applicants can deposit Tender Fees/ EOI Fees/ amount in following account through NEFT/RTGS.

Following details is under:

Name: Bank of Maharshtra - IT Payment
A/C : 60058099506
IFSC : MAHB0001150
Branch : Pune Main

Technical Specifications, Terms and Conditions and various formats and pro forma for submitting the tender offer are described in the tender document.

Deputy General Manager
CISO & IRM

1. Introduction:

Bank of Maharashtra is a leading Public Sector Bank serving the nation for over 83 years. It has a three tier organizational set up consisting of Branches, zonal Offices and Head Office, The Head Office of the Bank is at 1501, Shivajinagar, Pune – 411005. The Bank has 1800+ fully computerized branches spread across the country. In the state of Maharashtra itself it has more than 1100+ branches, the largest network of branches by any Public Sector Bank in the state. The Bank has set up specialized branch offices to cater to the needs of SMEs, Corporate, agriculturists and importers & exporters.

The bank has fine-tuned its services to cater to the needs of various sections of society and incorporated the latest technology in banking offering a variety of services. The products and services offered by the Bank include demand deposits, time deposits, working capital finance, term lending, trade finance, retail loans, government business, Bancassurance business, mutual funds and other services like demat, lockers and merchant banking etc.

In order to enhance the security of critical infrastructure of the Bank and to manage Cyber security risks, the Bank wishes to conduct Information Security Audit of various IT services functional within the Bank. Bank intends to issue this bid document to the bidders to participate in the competitive bidding for setting up a strong audit framework with monitoring capabilities.

This EOI has been prepared solely for the purpose of enabling Bank of Maharashtra ('Bank') to select a Service Provider (SP) for conducting the work as per the scope of work provided in this document.

The EOI document is not recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the bank and any successful bidder as identified by the bank, after completion of the selection process as detailed in this document.

2. Background:

2.1 Overview:

The IT infrastructure of the bank of Maharashtra is ISO27001:2013 certified. The Bank also has Cyber Security Operations Centre (CSOC) in place. It has also taken various security measures such as DLP Solution, Patch management Solution, NAC etc.

The scope of work includes regular Information Security audits for various IT services of Bank. It also includes audit of critical infrastructure of the Bank. In order to setup a robust audit management framework with monitoring capabilities, entire audit activities should be automated using audit management software application. The requirements of this software application are provided later in this section.

The audit management software system shall streamline gathering responses, compiling audit reports, and tracking audit observations to closure, The Audit software shall include planning and scheduling tools that are integrated with risk based assessments to help focus on the high-priority areas.

The audit management software shall also include built-in analytics that allow the Bank to trend and filter the data to help identify general issues. The audit software shall include an

industry comparison based on consultancy experience and results from similar previous engagements.

Expression of Interest (EOI) are invited online from applicants:

a) Who meet the eligibility criteria as set out in Annexure – A
b) Who have solution strictly in line with the technical parameters.
c) Agreeing to abide by the terms and conditions contained in this Request for EoI document.

2.2 Purpose

Bank of Maharashtra is requesting submission of interest for empanelment of Information Security Service Providers (ISSPs). The eventual engagement from this process will be at Bank of Maharashtra. The empanelment will be made for next Three years subject the satisfactory performance. The purpose of this EOI is to seek abilities of the interested company's proposal for empanelment of Information Security Service Providers (ISSPs).

3. Eligibility Criteria:

The entities empanelled with CERT-In, desirous of empanelment for providing Information Security Services for bank are invited to submit their EOI. The criteria and the process of evaluation of the subsequent RFP and subsequent selection of the successful bidder(s) will be entirely at Bank's discretion. This EOI seeks interest only from the entities empanelled with CERT-In to provide Information Security Audit Services with adhering to Bank's requirement(s).

This EOI is not an offer by Bank of Maharashtra, but an invitation to receive responses from the ISSPs. No contractual obligation whatsoever shall arise from this EOI.

Interested applicants who fulfil the eligibility criteria as per Annexure-'A'are requested to submit information as set out in Annexure-'A' of this document.

4. Scope of Work:

The applicant should describe how their solution/capabilities will fulfil the requirements as desired in Appendix-I of this document. The applicants should furnish information on the lines of Annexure-B in their EOI response.

5. Process before submission of EOIs:

i. **Raising of queries/clarifications on Request for EOI document: The applicants requiring any clarification on this document should submit their written queries on as given in invitation section for EOI to: tanvi.kochhar@mahabank.co.in, akshay.mahajan@mahabank.co.in, ciso@mahabank.co.in (Landline No. 020-25614351)**

ii. **Modification in Request for EOI document:** At any time prior to the deadline for submission of EOIs, BOM may at its sole discretion, modify any part or parts of this document. Such change(s), if any, may be in the form of an addendum/corrigendum and will be uploaded in Bank's website -https://www.bankofmaharashtra.in. All such change(s) will automatically become part of this Request for EOI and will be binding on all applicants. Interested applicants are advised to regularly refer the Bank's Corporate Websites (URLs referred above).

iii. **Extension of date of submission of EOIs:** Request for extension of date for submission of EOIs will not be entertained. However, the Bank at its sole discretion may extend the deadline in order to allow prospective applicants a reasonable time to take the amendment/changes, if any, into account.

6. Format and Signing of EOI:

The applicant should prepare EOI strictly as desired in this Request for EOI document.

a. EOI should be typed and submitted on A4 size paper, spirally and securely bound and with all pages therein in serial order. All details should be covered as requested.
b. All pages of the EOI should be signed by only the authorized person(s) of the company/firm. Any interlineations erases or overwriting shall be valid only if the person(s) signing the EOI authenticates them. The EOI should bear the rubber stamp of the applicant on each page except for the un-amendable printed literature.
c. Contact detail of the authorized signatory and an authorized contact person on behalf of the applicant is to be provided as under:

Particulars	Authorized signatory for signing the EOI	Authorized contact person.
Name		
Designation		
Email id		
Landline		
Mobile No.		
Fax No.		
Address		

The applicants should demonstrate in EOIs that they meet all parameters given in **Annexure-'A'** of Request for EOI.

7. Empanelment Process and The Model of Engagement:

The EOI will be examined by the Bank and the empanelment process will done through RFP process. The option of closed / open floating of RFP is at the discretion of the Bank. The successful bidder(s) through RFP process shall be required to enter into a contract/SLA with the Bank.

The empanelment is for Three years from date of signing of SLA with the Bank. The services of Vendors empaneled will be engaged as and when requirements arises as per following models.

7.1 Price model: For an assignment / project / task (Viz., Comprehensive Security Review of Applications / Preparation of policy document / Forensic Audit etc.) Bank will call for RFP from the empaneled ISSPs based on its suitability providing the complete scope of work. The vendors have to quote the prices considering the efforts involved. The lowest quoted vendor will be awarded the assignment.

7.2 Man-days Hire model: For given N man-days / man-months, resource cost will be arrived based on the discovered prices through a RFP, say the cost is Y. Vendors will be asked to quote the discount percentage on Y in sealed cover. Whoever offers maximum discount on Y will be awarded the contact.

7.3 Nomination model: For special projects or on emergency basis Bank may assign the project on nomination basis on negotiation basis.

8. Last Date for submission of EOI:

The last date for submission of EOI is 07th Oct 2020. In case the designated day happens to be a holiday; the next working day will be deemed as the last date for submission of EOI.

9. Process after submission of EOIs:

i. All EOIs received by the designated date and time will be examined by the Bank to determine if they meet criteria/terms and conditions mentioned in this document including its subsequent amendment(s), if any and whether EOIs are complete in all respects.

ii. On scrutiny, the EOIs found NOT in desired format/illegible/incomplete/not containing clear information, in view of BoM, to permit thorough analysis or failing to fulfill the relevant requirement will be rejected for further evaluation process.

iii. Bank reserves the right, at any time, to waive any of the requirements of this Request for EOI document if it is deemed in the interest of Bank.

iv. If deemed necessary, the Bank may seek clarifications on any aspect of EOI response from the applicant. If a written response is requested, its reply must be provided within 3 (three) days by the applicant.

v. Bank may shortlist the applicants who fulfill the eligibility criteria, have solution as per the requirement of the Bank and are agreeing to abide by the terms and conditions of the Bank. Bank's judgment in this regard will be final.

vi. Bank may issue a Request for Proposal (RFP) to shortlisted applicants for inviting technical and indicative commercial bids for next process of procurement. However, please note that short listing of applicants should not be treated as a contract for the proposed work.

vii. Applicants will be advised about shortlisting of their EOIs or otherwise. However, applicants will not be provided with information about comparative position of their EOIs with that of others.

viii. Nothing contained in this EOI shall impair the Bank's Right to issue 'Open Tender' on the proposed solution.

10. Terms & Conditions:

i. Last Date of Submission of EOI: The EOI should be submitted on date mentioned in invitation section of this EoI document, at :
The Deputy General Manager & CISO,
Integrated Risk Management Dept., Pune

ii. **Disclaimer:** Subject to any law to the contrary, and to the maximum extent permitted by law, BOM 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 including forecasts, statements, estimates, or projections contained in this EOI 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 BOM or any of its officers, employees, contractors, agents or advisors.

iii. **Cost of EOI submission:** The ISSP shall bear all costs associated with the preparation and submission of its EOI/bids including cost of presentation(s), if any etc. Bank will not be responsible or liable for these costs.

iv. **Governing language:** The EOI and all correspondence/ communications and other documents pertaining to the EOI, shall be written in English.

v. **Governing Law:** The contract shall be interpreted in accordance with the laws of the Government of India.

Annexure A – Technical Details-Ability of the ISSP

The Audit firms intending to submit offer for such empanelment shall fulfill the following eligibility conditions and shall submit the documentary evidence for the same:

S. No.	Eligibility Criteria	Documents required	Complied Y/N
A. General Criteria			
1	*The vendor must be a firm/ company / organization registered under Companies Act/Partnership Act/LLP Act etc.*	Partnership Firm-Certified copy of Partnership Deed. Limited Company-Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. Reference of Act/Notification For other eligible entities-Applicable documents	
2	Shall have been in existence for five years as on 30-09-2020.	Partnership Firm-Certified copy of Partnership Deed. Limited Company-Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. For other eligible entities-Applicable documents	
3	The firm shall not be blacklisted / barred by Government of India or any regulatory body in India.	Self-Declaration	
4	The firm should have a pool of at least 20 professionals with international accreditation like CISA (Certified Information Systems Auditor), CISSP (Certified Information Security Professional), CEH (Certified Ethical Hacker) and BS7799/ISO27001 trained lead auditors etc. employed with them	List of existing (on role of the firm) professionals with their qualifications and certifications is required.	
B. Financial Criteria			
5	Shall have a minimum average annual income of Rs.50.00 crores (Rupees Fifty Crores) during last three financial years viz. 2017-18, 2018-19 & 2019-20	Copy of audited Balance Sheet and P&L statement for the financial years. 2017-18, 2018-19 & 2019-20	

S. No.	Eligibility Criteria	Documents required	Complied Y/N
6	The firm should be profit making for last 3 financial years viz. 2017-18, 2018-19 & 2019-20	Copy of audited Balance Sheet and P&L statement for the financial years 2017-18, 2018-19 & 2019-20	
C. Technical Criteria			
7	Bidder should be CERT-IN empaneled as on the date of submission of bid	Copy of certificate	
8	Must not be application implementer/Solution providers/ IS Auditor in last 3 years in Bank of Maharashtra	Self-undertaking	
9	The bidder should have conducted at least three Information Security audits of data centers and other IT Infrastructure of PSU banks in India in the past five years including a) Vulnerability assessment of servers/ security equipment/ network equipment; & b) External attack and penetration test of equipment exposed to outside world through internet	Reference Letter from Customer/ Document Proof	

List of resources with technical qualifications

Sl. No.	No. of Resources available with the Company	Category of the resource	Academic Qualifications	Professional Qualifications	No. of years of IS experience	Experience in Domain s

Annexure A1 – Experience/Expertise of the bidder (For Last 3 Years) (Scheduled Commercial Bank clients should appear at top, followed by BFSI (non-banking), Govt. Depts, etc)

S.No	Name, Address & Contact details of clients	Particulars of the order	Month & year of order	Description of services (relevant to Scope of Work in this RFP, give reference number only)	Value of order	Period of engagement	Date of completion (as per contract)	Date of completion (actual)	Remarks for extended completion, if any
1									
2									

Annexure A2 – Specific Work Experience of Vendor in Bank (Please write 'Yes' or 'No' in the box + Bank Name (Blank means 'No')

Activities	Core Banking	ATM	Internet Banking	Mobile Banking	Treasury Operations
VA					
PT					
Application Security					
Secure Network Architecture					
Process Review					
BCP/DR Review					
Fraud Investigation					
Cyber Forensics					
Other Activities (Pl Specify)					

Annexure - A3 – Specialized/emerging threat handling capacity of ISSP

List of activities (like Cyber Forensics/Fraud investigations etc.) carried out by the bidders across the industries

S.No.	Name of the customer/firms	Type of activity	Period

Annexure – A4 Certifications/Accreditations/Awards:

List of Certifications/Accreditations/Awards

S.No.	Name of Certification / Accreditation/Award	Awarded by	Date of issue

Annexure A5 – Mandatory Services Capability List for eligibility

	Standardized Services	Have capability (Y/N)	If Yes in prev col. Indicate priority of interest levels in offering this service to Bank (1 is Top Priority)	Remarks
1.	Vulnerability Assessment			
2.	Penetration testing			
3.	Technical standard creation			
4.	General Process Audit			
5.	IT General Controls Audit			
6.	ISO 27001 Consulting			
7.	Vendor Risk Assessment			
8.	Specialized Services			
9.	IS Program Management			
10.	Log Monitoring			
11.	Information Security Awareness			
12.	Application Security audit			
13.	Code Review			
14.	Red teaming exercises			
15.	Domain/Channel Process Audit			
16.	BCP / DRP audit			
17.	Security solution consulting			
18.	Product evaluation			
19.	Data Governance			
20.	Mobile Application Protection			
21.	Forensic Analysis			
22.	PCI-DSS Services			
23.	ISO 20000			
24.	Forensic Audit			

additional services capability available can be mentioned by the applicant.

Annexure B - Details of the bidder

1. Name
2. Date of Incorporation and / or commencement of business
3. Certificate of incorporation, Company website URL
4. Brief description of the bidder with main line of business
5. Particulars of the Authorized Signatory of the Bidder
    a. Name, Designation
    b. Address
    c. Phone Number (Landline), Mobile Number
    d. Fax Number, Email Address
6. For the last 3 years information as per table below:

Sl.no	Item	2019-20	2018-19	2017-18
1	Annual turnover			
2	Profit			
3	No. of employees in IT Audit function			
4	Total no. of employees in the Company			

Signature and Seal of Company

Appendix - I

Scope of Work:

I. The scope defined below is illustrative but not exhaustive. Deliverables include but not limited to the following;

- Security Review of Bank's IT Infrastructures
- References / Rationale for recommendations

Bank is proposing to procure 'CSR Life cycle management Solution' for end to processing of Security Review of IT infrastructure and MIS purpose. The selected bidders would be required to furnish the reports as per this solution.

Reports would be in

- soft copies, hard copies, copies of screen shots, outputs,
- audit evidence
- soft outputs which are importable into a database, spreadsheet, or GRC platform e.g. XML files, CSV files etc.
- Tracking sheet
- PowerPoint presentation for Top management
- Vulnerabilities identified, Vulnerability ratings
- Threat Profile, Test Plan
- Compliance profile covering compliance with Banks policies, legal and regulatory requirements and industry best practices, whichever are the best
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible in code reviews

II. Service Types:

Services are categorized into two areas viz.

a) Standardized and

b) Specialized.

<u>Standard Services</u>

a) Vulnerability Assessment

BOM expects an authenticated type but non-destructive vulnerability assessment to be carried out. Vendor should be able to cover a broad range of systems like Operating system (Windows, Linux, AIX, HP UX etc), Databases (MSSQL, Oracle, Sybase, DB2, IBM cloudant etc), Web servers (Apache, Tomcat, IIS, Oracle weblogic, etc), Network devices (Cisco, Juniper etc), Security devices (Cisco, Checkpoint, Juniper, Sonicwall etc), Virtualization, Cloud environment etc. Vendors are expected to conduct the audit against the standard configuration document that bank has created, as also the latest global standards and industry best practices. In case, any new asset is identified during project execution, vendor is expected to develop the checklist and conduct the assessment.

Scope of work for Vulnerability Assessment

General aspects for all systems

- Access control and authentication; Network settings

- General system configuration; Logging and auditing
- Password and account policies; Patches and updates

Specific requirements for Server/OS Configuration Audit

- File system security; Account Policies; Access Control
- Network Settings; System Authentication
- Logging And Auditing; Patches And Updates
- Unnecessary services; Remote login settings

Configuration Audit of Networking & Security Devices

- Access Control ; System Authentication
- Auditing And Logging; Insecure Dynamic Routing Configuration
- Insecure Service Configuration; Insecure Tcp/Ip Parameters
- System Insecurities; Unnecessary services
- Remote login settings; Latest software version and patches

Database Configuration Audit

- Database Account Authentication; Password Policy
- Database Account Privileges; Database Auditing
- Database Logging And Tracing; Database Network Access Mechanism; Database Patching
- Database Files And Directories Permission
- Access control and authentication
- Unnecessary services; Remote login settings; Patches and updates

Security configuration of desktops and laptops that are used by the business users can be performed on sampling basis as per Bank's requirements.

b) Penetration testing

The security assessment should use the industry standard penetration test methodologies (like OSSTM) and scanning techniques, and will focus on applications. The application tests should cover but not limited to OWASP Top 10 attacks.

Scope of work for Penetration Testing

1. Tests for default passwords, Tests for DoS, DDoS vulnerabilities
2. Test for directory Traversal
3. Test for insecure services such as SNMP
4. Check for vulnerabilities based on version of device/server
5. Test for SQL, XSS and other web application related vulnerabilities
6. Check for weak encryption, Check for weak hashing
7. Check for SMTP related vulnerabilities such as open mail relay
8. Check for strong authentication scheme
9. Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
10. Test for information disclosure such as internal IP disclosure
11. Look for potential backdoors, Check for older vulnerable version
12. Remote code execution, Weak SSL Certificate and Ciphers
13. Missing patches and versions
14. This is a minimum indicative list, vendors are encouraged to check for more settings in line with best practices including PCI, OSSTM etc

c) Technical standard creation

Creating –

The ISSP is expected to create a base document with parameters, values etc. and descriptions of risks to enable an OS, system, platform, application, database etc. to be securely configured for use in the Bank.

Scope of work

This document will need to be based on the global standards, documentation available, OEM/Vendor advisories and documents and incidents / vulnerabilities related information available in the public domain / vendor's own knowledge base and experience. This will also be required to be updated annually and more frequently in case of need /discovery of new vulnerabilities etc.

d) General Process Audit

Assess whether the data processing that takes place in systems and IT occurs in a controlled environment, supporting data integrity and security.

Scope of work for general process audit

The activity includes detailed assessment of the following:

- Assess the controls implemented in the system for :Input, Processing, Output, Functionality
- Logical Access Controls - Review all types of 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. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per their role and/or functional requirements
- Assess sufficiency & accuracy of event logging, adequacy of Audit trails, SQL command prompt usage, database level logging etc.
- Assess interface controls - Application interfaces with other applications and security in their data communication.
- Assess authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition.
- Assess Data integrity & File Continuity Controls
- Assess controls for user maintenance, password policies are being followed are as per bank's Information Security policy with special attention to the use of hardcoded User Id & Password
- Assess controls for segregation of duties and accesses of production staff and development staff with access control over development, test and production regions.
- Review of all types of Parameter maintenance and controls implemented.
- Assess controls for change management procedures including testing & documentation of change.
- Identify gaps in the application security parameter setup in line with the bank's security policies and leading best practices
- Audit of management controls including systems configuration/ parameterization & systems development.
- 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.
- Review of customizations done to the Software & the SDLC Policy followed for such customization.
- Verify adherence to Legal & Statutory Requirements
- Provide suggestions for segregations of Roles/Responsibilities with respect to Application software to improve internal controls
- 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.

- Check the sufficiency and coverage of UAT test cases, review of defects & tracking mechanism deployed by vendor & resolution including re-testing & acceptance.
- Backup/Fallback/Restoration /Recovery & Restart procedures

The above should be done in consonance with standards like ISO 27001, Bank's Information Security Policy and Standards, legal & regulatory requirements & global best practices.

IT General Controls Audit

Assess whether the data processing that takes place in systems and IT occurs in a controlled environment, supporting data integrity and security.

Scope of work for IT General Controls Review

1. Change Management- To provide reasonable assurance that only appropriately authorized, tested, and approved changes are made to in-scope systems. The following attributes needs to be tested with appropriate evidences:
    a. All changes are authorized, tested, approved and monitored
    b. Responsibilities are appropriately segregated
    c. Procedures for Emergency changes
2. Logical Access- To determine that only authorized persons have access to data and applications (including programs, tables, and related resources) and that they can perform only specifically authorized functions. The following attributes needs to be tested with appropriate evidences:
    a. General Security settings with respect to Application, Operating System and Database
    b. Privilege User Management
    c. Procedures for New User setup, Terminated Users, Transfers
    d. User Access Reviews
    e. Segregation of Duties
3. Backup Management- To determine that the data supporting business information is properly backed-up so that it can be accurately and completely recovered if there is a system outage or data integrity issue. The following attributes needs to be tested with appropriate evidences:
    a. Backup and Recovery
    b. Job Scheduling
4. Entity Level Controls: To determine the adequacy of internal controls that help ensure that management directives pertaining to the entire entity are carried out. The following attributes needs to be tested with appropriate evidences:
    a. Quality Assurance Management process review
    b. Management review and governance over systems performance
    c. Presence of adequate policy and procedures documents and its adherence
    d. Review of previous audit/test reports and the actions taken on the recommendations
5. Others: Review the following:-
    a. Audit logging and review mechanism
    b. Patch Management procedures
    c. Antivirus management

ISO 27001 Consulting

BOM wants to develop detailed Information Security Management System which is focused on the on-going management of information security requirements. The intent of the ISMS in BOM is to define the processes requirement to ensure that risks are identified, apprised to management and addressed in an effective manner.

The key components that needs to be put in place as that part of ISMS includes

- Risk identification and mitigation planning
- Allocation of responsibility for mitigation
- Status tracking of mitigation
- Management reporting

- Security maturity evaluation over a period of time

Scope of Work for ISMS

1 Define ISMS Structure and roles and responsibilities.
2 Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.
3 Discuss with the stakeholders and develop criteria for accepting risks and identify the acceptable levels of risk.
4 Interact with key stakeholders and identify all information assets like software assets, databases, records, physical assets, process and service assets, people assets and so on
5 Evaluate the value of the assets based on business impact after detailed discussions with the stakeholders.
6 Perform Risk Assessment by categorizing the assets by profiling threats, assessing vulnerabilities, analysing impact, and ranking/ prioritizing risks based on the level of threat, level of vulnerability and asset value.
7 Analyse and evaluate the risks based on its business impacts, realistic likelihood of security failures, level of risk and the risk acceptance criteria.
8 Identify and evaluate options for the treatment of risks
9 Select control objectives and controls for the treatment of risks
10 Present proposed residual risks to management and obtain their buy-in for implementing and operating ISMS
11 Prepare a Statement of Applicability document
12 Assist in implementing security controls (network architecture, access control systems, and secure configuration guidelines etc.).
13 Assist in defining roles and responsibilities of the enforcer, enabler, and auditor; and establish a total compliance program
14 Conduct internal audits with a trained team; drawing up performance metrics; conducting awareness programs among end users; defining processes, roles and responsibilities; ensuring that the Management reviews and works on the Action Plan to close non conformities (NCs).
15 Develop a framework for periodic risk assessment and mitigation; continual user and IT administrator awareness sessions;
16 Develop a framework for security effectiveness measurement and maintenance of dashboards.

e) Vendor Risk Assessment

Scope of Work

IT and operational controls

Outsourcing of critical functions related to IT and Business should be assessed on periodic basis and should include

- To assess Information Security Risk in Outsourced Vendor Operations
- To conduct risk assessment of all outsourced vendors carrying out key operational processes for Bank vis-à-vis ISO 27001:2013 standard
- To assess whether outsourced vendors meet/incorporate adequate level of security controls commensurate with the business information they receive/ store/process from or on behalf of Bank
- To assess whether the outsourced vendors comply with the IS Policy of the organization wherever applicable
- To assess adequacy of privacy and data protection controls at vendor premises

Specialized Services

a) IS Program Management

Scope of Work

- Supporting monitoring of all information security related activities
- Maintaining overall data

- Providing snapshots, dashboards, tracking
- Continuously scanning external environment

Deliverables include but not limited to the following;

- Dashboards, Portal, MIS, Tracking
- Presentations, Advisories

b) Log Monitoring

Scope of Work

- Monitoring logs , Providing alerts, Storage,
- Correlation through SIEM solutions and add-on tools
- Assistance in mitigation, Tracking & Closure of incidents

c) Information Security Awareness

Scope of Work

- General Information Security Awareness
- Specialised Information Security Training to different groups like branch users, users at administrative offices, Senior Management, Top Management, Board of Directors, Bank's business partners and customers of all categories

d) Application Security

Technical Assessment

1 The assessment should cover both business logic and technical risks

2 The assessment report should contain a detailed threat list of the application. The threat list should contain the possible risks to the application both from a business and technical aspect

3 The tester should attempt to identify and exploit vulnerabilities that include the OWASP Top 10, including (not limited to top 10 only. The tester may be required to identify other OWASP vulnerabilities also).

Process Assessment

1 Authorization and Segregation of Duties Controls

- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of user application entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).
- Perform sample testing of user application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment).
- Populate issue and findings log with the gaps / deviations / issues noted (if any)

2 Assessment of Role based Security for Applications under scope

- Review of user creation/modification/deletion/maintenance procedures for the in-scope applications
- Review of privileged access rights granted to application, system administrators, service providers and vendors
- Assess the process for review of user logs for administrator and system users
- Review ongoing monitoring of effectiveness of implemented procedures and controls
- Perform sample testing of application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel.
- Review of account and password policy including controls such as
- Users are assigned unique accounts
- Adequate passwords are maintained e.g. alphanumeric, minimum number of characters. etc.
- Periodic password changes and preventing repeated use of passwords and

- Review of implementation of password policy at system and application levels
- Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts
- Segregation of duties controls /maker-checker controls through appropriate design and implementation of user roles / profiles.
- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of application's entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).
- Understand how unsuccessful access attempts to applications in scope are logged and monitored
- Review the implementation and effectiveness of user access management in applications in the event of leaves.
- Review the segregation of development, production and test environments of applications
- Understand the manpower deployment for application maintenance
- Based on the control design weaknesses identified above, identify the areas for conducting forensic study.

e) Code Review

The code review activity should help the bank in uncovering any vulnerability that an adversary may potentially exploit

Scope of Work for Code Review

- Conduct in-depth understanding of the application architecture
- Prepare a threat profile listing all threats that are applicable to the in scope application
- Study the code layout in terms of pages, classes, modules, interfaces and custom protocols
- Conduct manual and automated code review (Black Box, Grey Box or White Box, as the case may be) as per criticality of the code using the latest tool(s).
- Use combination of tools like custom scripts, static code analyzers, process, file and registry usage monitors, dis-assemblers, de-compliers etc.
- Verify the findings reported by the tools and prioritize them based on their criticality and impact

f) Domain/Channel Process Audit

Scope of Work for Code Review: Same as given above for Application Security Assessment

g) **Red Teaming exercises.**

1. The bidder shall conduct Red Team Exercise to focus on giving the bank's security teams a practical experience combatting real cyber-attacks to simulate the tools, tactics and procedures (TTPs) of real-world attackers that target our environment, while avoiding business damaging tactics.
2. Red Team is required to identify exploitable security holes across an organization's attack surface using a variety of composite attack vectors. This should include relationships between systems, software, and people.
3. The Red Team Exercise, should involve the full attack lifecycle, from initial reconnaissance to mission completion. The objective is to test and validate the ability to detect malicious activity and evaluate the response to the detected events. The Red Team Exercise should provide an accurate situational awareness of the security posture of a given system/network. Technical specifications for red team assessment is as given in table below.
4. Test the security team's effectiveness in dealing with a cyber-attack
5. Train the security team to better respond to future cyber attacks
6. Determine the level of effort required to compromise the sensitive data or IT infrastructure

7. Identify and mitigate complex security vulnerabilities before an attacker exploits them
8. Receive fact-based risk analysis and recommendations for improvement

h) BCP / DRP

BOM wants to implement a comprehensive continuity management program which will comprise of detailed business impact analysis and development to business and IT strategies. This will be followed by the development and BOM wide response plans.

Activities under BCM

1. Systems Study
   - Read the existing BCP policy of BOM and review it against leading practices to identify gaps.
   - Benchmark it with the requirements of standards such as BS25999
   - Discuss the recommendations with the BOM and assist in documenting the new policy and associated processes / documents based on the recommendations accepted by BOM
2. Assist in documenting a high level roadmap and timeframe for the BCP engagement
   - Understand the business operations of BOM including the processes, underlying IT infrastructure and locations
   - Identify key activities to be carried out as part of the BCP engagement
   - Mutually decide the deliverables and resource plan of the project and collect relevant documents, information and data
   - Conduct Kick-off workshop with business process owners to provide overview of the project, overview of Business Impact Analysis (BIA), Recovery objectives etc.
3. Business Impact Analysis
   - For the identified locations and business units, conduct detailed discussions with the relevant stakeholders to populate the BIA document. The BIA should necessarily:
     - Identify critical business functions/processes, their resource requirements and interdependencies
     - Estimate the financial and operational impacts of disruptions
     - Determine the recovery time objective (RTO) and recovery point objective (RPO) for mission critical functions
   - The business impacts should be assessed keeping in mind the following:
     - the impact on staff or public wellbeing;
     - the impact of damage to, or loss of, premises, technology or information;
     - the impact of breaches of statutory duties or regulatory requirements;
     - damage to reputation;
     - damage to financial viability;
     - deterioration of product or service quality;
     - Environmental damage.
   - Review the results of business impact assessment, recovery time objectives for operations and recovery point objectives for data and systems, and validate for consistency and incorporation of accepted inputs
   - Estimate the resource requirements for each critical activity after resumption taking the following into account:
     - staff resources, including numbers, skills and knowledge (people);

    - the works site and facilities required (premises);
    - provision of information (whether electronic or paper-based) about previous work or current work-in-progress, all of which is sufficiently up-to-date and accurate to allow the activity to continue effectively at the agreed level (information); and
    - external services and suppliers (supplies).
- Undertake a Risk assessment exercise in consultation with relevant stakeholders:
    - Determine the criteria for risk acceptance.
    - Identify acceptable level of risks
    - Analyse the risks
    - Evaluate threats and vulnerabilities
    - Assess impacts that might result from exploitation of vulnerabilities by threats.
- Identify the most probable threats to the organization and or location within the organization and analyse the related vulnerabilities of the organization to those threats
- Evaluate the existing physical and environmental security and controls and assess their adequacy relative to the potential threats of the organization
- Evaluate the risk mitigation strategies
- Provide a findings / recommendations report to management

4. BCM Strategy
    - Determine and guide BOM in the selection of alternative business recovery operating strategies for recovery of business operations within the recovery time objectives, while maintaining the organization's critical functions.
    - Identify and document recovery strategies for each line of mission critical business functions based on RTO/ RPO after discussion with the stakeholders
    - Deliberate with the management of BOM and assist in determining the relative costs for implementing strategies and provide cost benefit analysis
5. IT Strategy
    - Provide high level strategy guidance for IT systems in order to fulfil the recovery objectives
    - Provide guidance for improving the organization's DR strategy.
6. BCM Planning and plan development
    - Create and document detailed plans including business resumption, site restoration, crisis management, technology recovery and critical staff management, communication plan etc.
    - Document roles and responsibilities of people and teams having authority (both in terms of decision-making and authority to spend) during and following an incident.
    - Define the purpose and scope of each specific plan and present it to top management for review.
    - Conduct meetings and awareness sessions for key stakeholders who will put the plan into effect.

- Establish and document clear guidelines and a set of criteria regarding which individual(s) have the authority to invoke the plan(s) and under what circumstances.

7. Implementation and Training
   - Create the teams and allocate responsibilities in line with BCP
   - Conduct training and awareness sessions for end users
   - Assist BOM in implementing procedural and technical measures as per plan
8. BCM Testing and Maintenance
   - Create overall testing and maintenance plan
   - Identify test participants, test dates and test outcomes
   - Develop process for BCM improvement based on test results
9. Certification Support

i) Security solution consulting

Scope of Work

The Service Provider shall review the requirement for a type of IT security solution. The review shall document the capabilities that would be most appropriate to meet organization needs. The service provider should assemble a list of the type of solutions designed for these needs/or prepare a customised solution requirement. The service provider shall deliver a Solution Requirements Report and Possible Solutions List. For each solution identified as requiring further evaluation, the service provider shall do a POC/comparative evaluation for the solutions either directly or in coordination with the provider of the solution and submit a report with comparison to client giving all solutions. The decision about selection and procurement of the final solution will rest with client. The report shall also address data collection capabilities, utility (e.g., ease of use, error messages, documentation quality), security controls, reporting capabilities, solution support, and compatibility with the organization's other IT security solutions and procedures. The service provider shall prepare and deliver a report documenting advantages and disadvantages of each solution. The service provider shall prepare a recommendations report on whether solution will meet the organization requirement. Recommendations shall be based on cost, response time, ease of use, ease of implementation and operation, customer support, and quality of documentation.

j) Product evaluation

The objective of the activity is to help bank identify and analyse various security products based on requirement and suitability for the bank.

Scope of Work for product evaluation:

The Service Provider shall review the requirement for a type of IT security product. The review shall document the capabilities that would be most appropriate to meet organization needs. The service provider should assemble a list of the type of products designed for these needs. The service provider shall deliver a Product Requirements Report and Possible Products List. For each product identified as requiring further evaluation, the service provider shall do a POC for the products either directly or in coordination with the supplier of the project and submit a report with comparison to client giving of all products. The decision about selection and procurement of the final product will rest with client. The report shall also address data collection capabilities, utility (e.g., ease of use, error messages, documentation quality), security controls, reporting capabilities, product support, and compatibility with the organization's other IT security products and procedures. The service provider shall prepare and deliver a report documenting advantages and disadvantages of each product. The service provider shall prepare a recommendations report on whether product will meet the organization requirement. Recommendations shall be based on cost, response time, ease of use, ease of implementation and operation, customer support, and quality of documentation.

k) Data Governance

- Ensuring formulation of an scalable and robust Data Classification Framework
- Ensuring templates created are reusable and simplistic
- Ensuring identification of structured and unstructured data

- Ensuring implementation of a lightweight data labeling product for effectively managing unstructured data
- Ensuring identification of granular rule sets for DLP solution implementation

Scope of work

1. Review of existing Data Asset Classification Policy and Methodology
2. Perform data risk assessment to assess security loopholes from where data can get leaked
3. Develop a robust data governance framework which encapsulates:
   - Data Identification; Data Classification
   - Records Management; Data Security control matrix
   - Secure Data disposal processes
4. Develop Data Classification Guideline and Procedure document (encompassing complete data lifecycle including registration, maintenance, de-classifying and deregistration/ discarding process)
5. Prepare the Data Classification Project Plan clearly identifying the milestones timelines, approach and resources required.
6. Conduct Data Flow Analyses for the business units across the enterprise
7. Identify key documents & data that need to be classified
8. Identify the supporting applications and corresponding databases for classification and DLP protection.
9. Identify the owner, custodian & authorized users (white listed users)
10. Populating data in Data Classification Repository
11. To create a granular matrix that defines DLP authorization for individual user (Employee) and DLP channels (such as USB, email, print etc.)
12. Implement data labeling solution for classifying all unstructured data based on the data classification policy
13. Data Disclosure, sharing, exchange with internal / external stakeholders and government / public agencies / legal requirements.

l) Mobile Application Protection

Identify and verify the mobile application security vulnerabilities against industry global standards such as OWASP, PCI compliance, RBI, MPFI etc.

Scope of Work for Mobile Application Protection

- Perform assessments to identify vulnerabilities that can be exploited using applications on mobile phones for both registered and anonymous users
- Understand the features, functions in the application
- Create a detailed threat profile and a test plan
- Perform automated and manual tests like HTML Source Code Analysis, SQL Injection, Session Hijacking, LDAP Injection, Authentication Bypass etc.
- Assess adequacy ,generation & availability of Reports for accounting, regulatory ,statutory , reconciliation , MIS & statistical purpose covering all Mobile banking transactions
- Check Adherence to Operational/Statutory guidelines issued by RBI & other Regulatory bodies w.r.t Mobile Banking Application
- Perform audit of various functionalities provided in the application like Fund transfer, Transactions & queries, Cheque Book related etc.
- Perform verification of the detailed security procedures & processes of the Mobile Banking Solution provider as a part of the existing operational rules & regulations covering transaction, Data &Operational Security setup & establishing the adequacy of the same w.r.t the current Setup.
- Check adequacy Of Operational Security features through Access Control, User Rights, ,Logging , Data integrity ,Accountability , Auditability etc. for the Mobile Application Solution
- Check adequacy of MPIN Management Controls (Generation, Re-generation, Authorization, Verifications etc.) of Mobile Banking & Key Management features.
- Conduct audit of various security features including but not limited to Handset Security features , Transaction level security features, Platform Security & reliability features

including Database, Network & transmission Security features, Registration features , Administration Portal features, Call logging , tracking & Dispute Resolution features etc.
- Perform analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Incident management report etc.

m) Forensic Analysis

The vendor should be able deploy personnel who can conduct forensic analysis on demand basis and help bank to conduct forensic analysis activities

Scope of Work for Forensic Analysis

The vendor should have skillset to handle the forensic analysis activities across various IT systems, applications and infrastructure systems in the bank.

Vendor should conduct the activity in a structured fashion using global best practices for conducting forensic analysis. Methodologies and tools should be handled by the vendor for handling the forensic analysis

Vendor should have defined process for the management of the evidences that are collected during the forensic analysis.

n) PCI-DSS Services

Scope of Work for PCI DSS

Ensure compliance to the following PCI DSS standard requirements:

- Build and Maintain a Secure Network
  - Setup secure processes for managing security devices including firewalls
  - Implement the process for secure commissioning of servers, network devices, security devices and applications
- Protect Cardholder Data
  - Implement controls to mitigate the risks to card holder data
  - Implement encryption across links including WAN, Internet to protect card holder data
- Maintain a Vulnerability Management Program
  - Setup processes for antivirus management
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Implement controls for authorization and authentication
- Regularly Monitor and Test Networks
  - Implement controls for tracking and monitoring all access to network resources and cardholder data
  - Implement controls to enable periodic testing of IT infrastructure including wireless, applications
- Maintain an Information Security Policy
  - Define policies and procedures that addresses information security for employees and contractors
- Guidance on PCI DSS compliance
  - Provide guidance to implement controls and best practices to achieve compliance.

o) ISO 20000

The primary objective of this activity is to implement and certify IT Services Management (ITSM / SMS) for defined scope of work.

Scope of Work for ISO 20000 certification

1) Develop and Implement IT Services Management (ITSM) and obtain ISO 20000 certification for Bank.
   - Baseline the current Services and the IT infrastructure
   - Assess any existing processes against the defined ISO 20000 processes
   - Compare these to business needs and best practices
   - Define and document the ITSM governance principles and policies

- Design IT Service Management System (ITSM System) by performing the following activities:
    - Define Goals for Service Management & Metrics
    - Identify Services to create IT Service Catalogue
    - Identify Infrastructure
    - Define Roles and Responsibilities
    - Define IT Service Management Processes
    - Identify tools that can aid automation
- Assess the continuity capabilities of IT infrastructure and processes and define approaches to resume critical activities
- Assist the identified coordinators to implement and operationalize ITSM processes through trainings
- Conduct internal audit in line with ITSM implementation requirements
- Support the internal teams with coordination for certification audit

2) The ITSM should be designed in a manner to enable the effective co-existence of any existing standards like ISO9001: Quality Management System (QMS) and ISO27001: Information Security Management System (ISMS)
3) Provide any needed tool/SW to achieve the ISO20000 certification.

End of Document