

Central Bank of India



Tender Document

Tender Reference Number:

CO:DIT:PUR:2018-19:257

Request for Proposal

For

Empanelment of vendors for various information /cyber security related services.

Cost of the Tender Document: Rs. 5000/- (Rs. Five thousand Only)

TABLE OF CONTENTS

Section I: Requirement Description	7
1. Introduction:	7
2. RFP Objective:	7
Section II: Eligibility Criteria	8
Section III: Technical Requirement	10
1. Scope of Work (SoW):	10
Section IV: Bid Guidelines	37
1. Bid Price.....	37
2. Bid Security	37
3. Technical Bid	38
4. Offer Validity Period	39
5. Bidding Document:	39
6. Erasures or Alterations	39
7. Right to Alter Quantities / Repeat orders.....	39
8. Bidder Queries	40
9. Amendment of bidding documents:	41
10. Terms of execution of work:	41
11. Overview of Evaluation Process (Two Part Offer):	41
12. No Commitment to Accept Lowest or Any Tender	41
13. Late Bids	41
14. Evaluation Criterion:.....	42
15. Awarding of Assignment	45
16. Order Cancellation:	45
17. Liquidated Damages:	46
18. Inspections & Tests:.....	46
19. Media & Documentation:	47
20. Supplier's Obligations:	47
21. Delays in the Suppliers Performance:	47
25. Confidentiality	49
Section V: Terms and Conditions.....	51
1. Terms of execution of work.....	51
2. Indemnity	51
3. Publicity	53
4. Patents Rights:	53
5. Force Majeure:	53
6. Limitation of Liability	54
7. Compliance with Laws	54
8. Corrupt and Fraudulent practice.....	55
9. Information ownership	56
10. Arbitration.....	56
11. Assignment& Subcontract:	57
12. RFP Ownership:.....	60
13. Proposal Ownership:	60

14. Tender / RFP Cancellation:	60
15. Other Terms and Conditions:	60
16. Language and Currency of BIDs:	61
17. Penalty	61
Section VI: Annexure	62
Annexure-A: Acceptance of terms and conditions	62
Annexure – B (Technical Proposal)	63
Annexure-C: Eligibility criteria	64
Annexure C1- Statement of Bidder (For last 3 years from 01.04.2015)	67
Annexure C2 - Specific Work Experience of Vendor during past three years in BANKS	68
Annexure C3 List of Experienced Staff working in the Company	69
Annexure C4 Priority list of Services and Assignments by the ITCSSPs in BFSI Sector	70
Annexure – D (Reference Site Details)	73
Annexure - F Undertaking for providing Performance Bank guarantee	74
Annexure –G (Undertaking)	75
Annexure H: Performance Bank Guarantee	76
Annexure –I Compliance to RFP terms & conditions	78
Annexure – J: Pre Bid Query Format	80
Annexure – K (Know Your Employee)	81
Annexure - L: Format of BANK GUARANTEE FOR EMD	82
Annexure –M: Non-Disclosure Agreement	84
Annexure -- N: Integrity Pact	88

Bid Details: Central Bank of India invites sealed tender offers (technical offer and commercial offer) from reputed Companies / firms / Service Providers who have proven experience in the field of work/consultancy related to Information Security, Information Technology (IT) / Information System (IS) Audit, Cyber Security and related work and fulfil the eligibility criteria as given in this document

The copy of tender document may be obtained from Dept. of IT, 1st Floor, Plot No. 26, Sector – 11, CBD Belapur, Navi Mumbai on all working days in person. The details are given below:

Important information regarding Bid submission

Tender Reference No.	CO:DIT:PUR:2018-19:
Price of Tender documents	Rs.5,000/-
Earnest Money Deposit (EMD)	Rs. 3,00,000/-
Date of commencement of sale of RFP documents	11.04.2018
Submission of Queries (if any) by bidders	On or before 21.04.2018
Date , Time & Venue of Pre-bid meeting	23.04.2018 ; 3 pm Central Bank of India, DIT, 1 st floor, Sec.11, Plot No.26, Opp. Belapur Rly. Stn., CBD Belapur, Navi Mumbai 400 614.
Last date and time for receipt Bids	15.05.2018 upto 3 pm
Date and time of opening Technical bid	15.05.2018 ; 3.30 pm
Place of submission of Bids	Central Bank of India, DIT, 1 st floor, Sec.11, Plot No.26, Opp. Belapur Rly. Stn., CBD Belapur, Navi Mumbai 400 614.
Address for communication	Same as above
Place of opening bids	Same as above
Contact numbers	022-67123583/67123669
E-mail address	sminfosec@centralbank.co.in smitpurchase@centralbank.co.in infosec@centralbank.co.in
Web site	www.centralbankofindia.co.in

It is essential that all clarifications / queries / suggestions be submitted to Central Bank of India at the above address at least two working days before the date of the Pre-bid meeting. Vendors, who furnish the Tender Fees of RFP Document before pre-bid meeting, will be eligible to participate in the pre-bid meeting.

Fees for RFP document Rs. 5000/- to be paid in the form of Demand Draft issued by a Scheduled Commercial Bank in favour of “Central Bank of India” payable at Mumbai and the DD should be submitted prior to the pre bid meeting.

If any vendor chooses not to attend the pre-bid meeting, their queries if any may not be entertained by the Bank. However, they will be allowed to participate in the RFP process and the said fee for RFP

document can be submitted along with the “Technical Offer” on or before the prescribed last date of submission of the tender offers.

Earnest Money Deposit of Rs.3,00,000/- (Rs.Three lakhs only) must accompany all tender offers (as specified in this tender document). EMD should be submitted along with the “Technical Offer”.

Tender offers (Technical) will be opened, in the presence of the tenderer’s representatives who choose to attend the opening of tender. No separate communication will be sent in this regard.

Jacob Ninan
Dy. General Manager - CISO

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Central Bank of India (hereinafter referred to as Bank), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

Section I: Requirement Description

1. Introduction:

Central Bank of India herein after referred to as the “Bank”, established in 1911, was nationalized in the year 1969 and today is a leading public sector bank listed in BSE/NSE.

The organizational structure of the Bank consists of four tiers viz., Central Office (CO), Zonal Offices (ZO) and Branches. CO, consisting of various functional departments deals with mainly policy formulation, setting of targets and monitoring of performance. The Bank has set up 13 Zonal Offices to exercise immediate supervision and control over the 59 Regional Offices, which in turn supervise the branches under their jurisdiction. The Bank has a network of 4700 plus branches, spread across the length and breadth of the country with presence in all the States and Union Territories. The Bank has also established its Wide Area Network at 4500 plus locations all over India covering administrative and branch offices and is planning to enlarge it during the current year.

The Bank also has specialized branches catering to the specific needs of Retail customers, Industrial Units, Corporate Clients, Forex Dealers, Exporters and Importers, Small Scale Industries and Agricultural Sector. The Bank has sponsorship in 3 Regional Rural Banks (RRB). Bank has implemented Core Banking Solution in all 4720 branches.

2. RFP Objective:

The Bank invites Request for Proposal [RFP] from reputed Companies / firms / Service Providers who have proven experience in the field of work/consultancy related to Information Security, Information Technology (IT) / Information System (IS) Audit, Cyber Security and related work and fulfil the eligibility criteria as given in this document. The Bidder should provide various consultancy, services and activities related to Information Technology and Cyber Security Services for the Bank.

Bank intends to have an Empanelment of Information Technology / Cyber Security Service Providers (ITCSSPs) for IT and Cyber security and IS Audit related work, approximately for a period of two years at Bank’s discretion. This would be subject to annual review. Bank reserves the right to de-empanel any empanelled ITCSSPs. Empanelment does not confer any rights on the vendors to necessarily receive assignments/jobs. This allocation of assignments/jobs will be at the sole discretion of the Bank.

Bank intends to empanel 10 bidders in premium service providers / consultants category under this RFP.

In case the empanelled ITCSSPs do not respond to the quotation / inquiry by Bank on three occasions or do not perform / execute the assignment during the validity of the empanelment, they may be delisted from the Panel by the Bank. The decision of the Bank will be final and binding on the Empanelled ITCSSPs.

The purpose of the Bank behind this RFP is to seek a detailed technical and commercial proposal for empanelment of Information Security Service Providers & Consultant (ITCSSPs).

Section II: Eligibility Criteria

Only those Vendors who fulfil the following criteria are eligible to respond to the RFP. Offers received from the vendors who do not fulfil any of the following eligibility criteria are liable to be rejected.

The bidder shall submit the proofs of minimum eligibility criteria as given below-

1. The bidder should be a registered company /partnership firm / LLP(Limited Liability Partnership Act 2008) in India and should be in existence for minimum of Five years as on the date of RFP and currently empanelled by CERT-In.
2. The bidder should have minimum annual turnover of Rs. 50 crores during the last three financial years (i.e. 2014-2015, 2015-16 & 2016-17). (Document required in support - Audited Balance Sheet, Profit & Loss accounts for the same).
3. The bidder should have net profit during the last three financial years (i.e. 2014-2015, 2015-16 & 2016-17). (Document required in support - Audited Balance Sheet, Profit & Loss accounts for the same).
4. The Bidder should have experience & expertise in handling Assignments / Services related to comprehensive security review of Data Centre/Enterprise Network, Active Directory, Application Security, Security review/ IS or IS-IT Audit (including Vulnerability Assessment and Penetration Testing (VAPT)), Forensic Audit, Technical investigation related to frauds etc. in India for BFSI Sectors during last three Financial years (i.e. 2014-2015, 2015-16 & 2016-17).
5. Bidder must have carried out Minimum Two Information Security and/or IS Audit related Assignments in BFSI during the last Financial year i.e. on or after 01.04.2017.
6. The Bidder should have experience in & expertise in handling Assignments / Services related to providing guidance in implementation of ISO 27001:2013 and/or ISO 22301:2012 in India in Minimum two BFSI during last three financial years (i.e. 2014-2015, 2015-16 & 2016-17).
7. The Bidder should have a minimum three each of CISA, CISSP, ISO 27001:2013 LA/LI, CEH certification holder as permanent employees in their organization. In addition to this, Bidder should also have minimum ten staff with any of the following qualifications / Certifications.
 - i. Certified PCI DSS professional
 - ii. CISM
 - iii. COBIT Certificate Holder
 - iv. CCNA / CCNP
 - v. CHFI

- vi. GIAC
- vii. CRISC
- viii. SSCP
- ix. ECSCA
- x. Offensive Security Certified Professional
- xi. ECIH
- xii. ISO 22301:2012 LA/LI

Please note that person holding multiple certificates shall be counted once only. Minimum certified manpower strength should be of 10.

8. The companies or firms, bidding for tender, should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs). The bidder shall give an undertaking (on their letter head) that they have not been black listed by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was black listed by any of the Govt. Authority or PSUs, the name of the company or organization must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered. Please refer Annexure-G.
9. The bidder should not be declared as NPA by any of the Banks in India. The bidder shall give an undertaking to this effect (on their letter head).
10. The bidder shall not assign or sub-contract the assignment or any part thereof to any other person/firm without the consent of the Bank. Even if bank has consented for sub-contracting, the bidder will be primarily responsible for all the activities done by the sub-contractor, under the scope.
11. Vendor should not be a consultant / System Integrator at present in Central Bank of India and/or RRBs sponsored by Central Bank of India for its core project (CBS) to avoid any conflict of interest.

Note: The Bidder must comply with all the above mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily. The requirements mentioned above are mandatory.

Bidder should fulfil all the eligibility criteria. Only those who fulfil all the eligibility criteria will qualify for further evaluation.

- Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made. The Bank reserves the right to verify / evaluate the claims made by the Bidder independently.
- Reference Site, Customer Name and Contact information to be provided to the Bank with whom discussion can be done.

Documents required to be submitted along with those mentioned in eligibility criteria above:

- 1) Audited Balance sheet & Profit and Loss Statement for last three years.

- 2) The list of skilled staff with their qualification and certification. (Copy of the certificates of the staff should be submitted).
- 3) Purchase Order/Reference Letter for the assignments handled in past. Bidder can mask the client details in case the assignment is very confidential and related to any incident or forensic investigation. For any other assignments bidder can mask the details like value of order in case NDA with client. However in all cases bidder has to provide the undertaking that information provided by them are true and if any deviation found on later stage Bank has right to forfeit the Bank guarantee, also may blacklist the bidder to participate in any future RFP/assignments.

Section III: Technical Requirement

1. Scope of Work (SoW):

Types of present and future activities and services required by Bank are covered/defined in this RFP is illustrative and indicative but not exhaustive. The scope may also undergo changes/updates due to implementation of new products, technology, projects, configuration requirements, business needs, legal and regulatory requirements etc. Vendors are expected to update and include additional relevant items in these activities to conform to global best practices and currently available knowledge base.

Common Deliverables

- Clarifications
- Discussions
- References / Rationale for recommendations

Reports would be in

- Soft copies with screen shots
- Hard copies – Two nos.
- Tool generated Outputs
- Audit evidence
- Soft outputs which are importable into a database, spreadsheet, or GRC platform e.g. XML files, CSV files etc.
- Tracking sheet
- Metrics and Dashboards
- Power point presentation
- Vulnerabilities identified
- Exploit Reports and supporting Evidences
- Vulnerability ratings
- Threat Profile
- Test Plan
- Compliance profile covering compliance with Banks policies, legal and regulatory requirements (inclusive of RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds etc.)
- Short Videos and Presentations for awareness sessions

- Information/Cyber Security Awareness Quiz questions
- Compliance requirements wherever applicable
- Screenshots and code listing or line numbers wherever feasible in code reviews
- Solutions with details and additional resources.

The scope of work includes following but is not limited to:

- A. Bidders are required to indicate the service priority list, based on their skills, competencies, experience, ability and willingness to offer specific services in order of priority.
- B. Bank will have one group of empanelled ITCSSPs, based on the marks obtained in evaluation of Technical Bids.

1.1. Service Type

The detailed scope, work description and deliverables of required services are given in as below:

- 1.1.1 Vulnerability Assessment
- 1.1.2 Penetration testing
- 1.1.3 Technical standard creation & Creation of Standard Operating Procedures (SOPs)
- 1.1.4 General Process Audit
- 1.1.5 IT General Controls Audit
- 1.1.6 ISO 27001 Consulting
- 1.1.7 Vendor Risk Assessment
- 1.1.8 Cyber law Consultancy
- 1.1.9 Red Team Exercises
- 1.1.10 IS / Cyber Security Program Management
- 1.1.11 Log Monitoring
- 1.1.12 Information Security Awareness
- 1.1.13 Web and Application Security
- 1.1.14 Code Review
- 1.1.15 Domain/Channel Process Audit
- 1.1.16 BCP / DRP (ISO 22301) consulting
- 1.1.17 Security solution consulting
- 1.1.18 Product evaluation
- 1.1.19 Data Governance
- 1.1.20 Mobile Application/s Protection
- 1.1.21 Forensic Analysis/Investigations
- 1.1.22 PCI-DSS Consulting/Services
- 1.1.23 Documentation – Policy, Processes, Procedure Creation/Review/ Modification etc.

- 1.1.24 Threat Modelling for various Software/App Development
- 1.1.25 Security and Network Architecture Review
- 1.1.26 Assess, Develop and Review Information Security Performance Dashboards focused on various measures such as effectiveness, ROI to convey value of investment on IS infrastructure across the Bank
- 1.1.27 Assess, Develop and Review Information Security Controls, Standards, Metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.
- 1.1.28 Investigations of cyber frauds reported by the bank/customers to find out the root cause and suggest remedial measures

In addition to these above mentioned services, Bank may also avail services for any other related activity as decided by the Bank during the empanelment period, which should be completed in timely manner as required/stipulated by the Bank

Detailed Scope of work is as under

1.1.1. Vulnerability Assessment

Bank 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 systems (Windows, Linux, AIX, Solaris etc.), Databases (MS SQL Server, MySQL, Oracle, DB2, PostgreSQL etc.), Web servers (WAS, Apache, Tomcat, IIS, OHS etc.), Application servers, Network devices (Cisco, Juniper etc.), Security devices (Cisco, Checkpoint, Juniper, Fortinet, PaloAlto, Sonicwall 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.

The purpose of the vulnerability assessment is to discover all systems on perimeter network or internet facing and to assess these systems for securities vulnerabilities. Vulnerability assessment shall attempt to determine vulnerabilities that may enable unauthorized logical access to protected system via the external network interfaces by a “naive” intruder who has limited and/ or no previous knowledge of the Bank’s network. The vendor will conduct vulnerability assessment against network and security infrastructure components to identify services in use and potential vulnerabilities present.

The assessment should check for various categories of threats including:

- I. Unauthorized access into the network and extent of such access possible
- II. Unauthorized modifications to the network and traffic flowing over network
- III. Extent of information disclosure from the network
- IV. Spoofing of identity over the network
- V. Possibility of denial of services
- VI. Possible threats from malicious codes (viruses and worms etc.)
- VII. Possibility of traffic route poisoning

1.1.1.1. Scope of work for Vulnerability Assessment

- A. General aspects for all systems
 - Access control and authentication
 - Network settings
 - General system configuration
 - Logging and auditing
 - Password and account policies
 - Patches and updates
- B. Specific requirements for Server/OS Configuration Audit
 - File system security
 - Account Policies
 - Access Control
 - Network Settings / Network Port / Network Access Details
 - System Authentication
 - Logging And Auditing
 - Patches And Updates
 - Unnecessary services
 - Remote login settings
- C. 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
- D. 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
- E. Security configuration of desktops, laptops, tablet phones and mobile devices that are used by the business users can be performed on sampling basis as per Bank's requirements.

1.1.1.2. Deliverables

Individual report should be provided for each of servers, network devices, and other audited units with detailed remediation steps. Executive summary with summarized scope, critical findings, and the positive security aspects identified in a manner suitable for the management.

1.1.2. Penetration testing

The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and how this information can be used to further leverage attacks. 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.

Consultant shall perform application security testing, to identify security vulnerabilities in the Bank's applications that may be exploited by a user to obtain unauthorized access. This will also include identification of any configuration issues that may not have been possible to identify during traditional vulnerability assessment.

Consultant shall use automated and manual testing techniques to exploit the weaknesses identified in the application logic, in areas like authentication, authorization, information leakage, field variable control, session timeout & logout, cache control, server side logic, client side logic, error handling, application administration and encryption.

The Scope for penetration testing should include but not limited to list of internet facing websites/ applications in System Detail section.

It is explicit that penetration tester should conduct vulnerabilities assessment consulting with concerned personnel and proper permission of the Bank. Finally remediation and recommendations must be provided along with all findings. The following areas are to be considered for penetration testing:

A. Network Security --

- a. Password Security Testing
- b. Router Security Assessment
- c. Anti-Virus System Security Assessment and Management Strategy
- d. Internet User Security

B. Host Security

- a. Unix/Linux/AIX System Security Assessment
- b. Windows System Security Assessment
- c. Web Server Security Assessment
- d. Other relevant/mapped application Security Assessment

C. Database Security Assessment

- a. All database instances from different OEMs

1.1.2.1. Scope of work for Penetration Testing

- A. Tests for default passwords
- B. Tests for DoS (Denial of Service) vulnerabilities
- C. Test for directory Traversal
- D. Test for insecure services such as SNMP
- E. Check for vulnerabilities based on version of device/server
- F. Test for SQL, XSS and other web application related vulnerabilities
- G. Check for weak encryption
- H. Check for SMTP related vulnerabilities such as open mail relay
- I. Check for strong authentication scheme
- J. Test for sample and default applications/pages
- K. Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
- L. Test for information disclosure such as internal IP disclosure
- M. Look for potential backdoors
- N. Check for older vulnerable version
- O. Remote code execution
- P. Weak SSL Certificate and Ciphers
- Q. Missing patches and versions
- R. This is a minimum indicative list, vendors are encouraged to check for more settings in line with best practices including PCI, OSSTM etc

1.1.2.2. Deliverables

Detailed technical Penetration Test report should be provided which should contain:

- Executive Summary – Summarize the scope, critical findings, and the positive security aspects identified in a manner suitable for the management.
- Categorization of vulnerabilities based on risk level – The report should classify the vulnerabilities as High/Medium/Low based on the Impact and Ease of Exploitation.
- Details of the security vulnerabilities discovered during the review – The detailed findings should be brought out in the report which will cover the details in all aspects.
- Solutions for the discovered vulnerabilities – The report should contain emergency quick fix solutions and long term solutions based on industry standards.

1.1.3. Technical standard creation & Creation of Standard Operating Procedures (SOPs)

The vendor is expected to create a base document with parameters, values etc. and descriptions of risks and hardening & patching/configuration details so as to mitigate the risk associated with OS, system, platform, application, database etc. to be securely configured for use in the Bank. 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. This should include:

- Develop minimum baseline security standard (MBSS) for various systems implemented at the bank.
- Review implementation of the MBSSs for servers OS, Web application, Database, Security Devices, Network Devices, Desktops, etc

1.1.3.1. Deliverables

A document with all the navigation to settings, commands, requirements and recommendations

1.1.4. 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.

1.1.4.1. 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, and 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 being followed are as per bank's IT& IS 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/ ISO 22301, Bank's IT & IS Security policies, legal & regulatory requirements & global best practices.

1.1.4.2. Deliverables

Detailed findings and recommendation report with solution

1.1.5. 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 and the need of complying with local laws and their requirements relating to information security.

1.1.5.1. Scope of work for IT General Controls Review

- A. Change Management Review (Monthly/Quarterly/Half-yearly) - To provide reasonable assurance that only appropriately authorized tested, and approved changes are made to in-scope systems. The following attributes need to be tested with appropriate evidences:
 - All changes are authorized, tested, approved and monitored

- Responsibilities are appropriately segregated
 - Procedures for Emergency changes
- B. 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:
- General Security settings with respect to Application, Operating System and Database
 - Privilege User Management
 - Procedures for New User setup, Terminated Users, Transfers
 - User Access Reviews
 - Segregation of Duties
 - Password Management
- C. 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:
- Backup and Recovery
 - Job Scheduling
- D. 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:
- Quality Assurance Management process review
 - Management review and governance over systems performance
 - Presence of adequate policy and procedures documents and its adherence
 - Review of previous audit/test reports and the actions taken on the recommendations
- E. Incident Response Management
- Review of Incident Management Plan
 - SLA Monitoring
 - Review the Cyber Crisis Management Plan
 - Review the effectiveness of Escalation Matrix and incident resolution time including RTO and RPO
- F. Others: Review the following:-
- Audit logging and review mechanism
 - Patch Management procedures
 - Antivirus management

1.1.5.2. Deliverables

Provide report of findings and recommendations with solutions. The report should be prepared keeping the following points in view:-

- Identification of gaps/deviancies/deficiencies/vulnerabilities/risks and detailed observations and its potential impact on the business

- Industry best practices
- Specific recommendations for improvement
- Adequate verifiable audit evidences
- Test cases for all application/databases/OS

1.1.6. ISO 27001 Consulting

Bank currently having its Data Center, Disaster Recovery Center and Near site locations certified with ISO 27001:2013 standard. To advance maturity levels further, Bank is in process of implementing various new IT security tools and wants to develop detailed Information Security Management System (ISMS) which is focussed on the on-going management of information security requirements. The intent of the ISMS in Bank is to define the processes requirement to ensure that risks are identified, appraised 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

1.1.6.1. Scope of Work for ISMS

- Define ISMS Structure and roles and responsibilities.
- Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.
- Discuss with the stakeholders and develop criteria for accepting risks and identify the acceptable levels of risk.
- 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.
- Evaluate the value of the assets based on business impact after detailed discussions with the stakeholders.
- Perform Risk Assessment information systemwise 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.
- Analyse and evaluate the risks based on its business impacts, realistic likelihood of security failures, level of risk and the risk acceptance criteria.
- Identify and evaluate options for the treatment of risks 9 Select control objectives and controls for the treatment of risks
- Present proposed residual risks to management and obtain their buy-in for implementing and operating ISMS
- Prepare a Statement of Applicability document
- Create, update and review the ISMS policy, procedure documents as per standard and tools, technologies & practices followed in consultation with concern stakeholder.

- L. Assist in implementing security controls (network architecture, access control systems, and secure configuration guidelines etc.).
- M. Assist in defining roles and responsibilities of the enforcer, enabler, and auditor; and establish a total compliance program
- N. 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).
- O. Develop a framework for periodic risk assessment and mitigation; continual user and IT administrator awareness sessions;
- P. Develop a framework for security effectiveness measurement and maintenance of dashboards.

1.1.6.2. Deliverables

- Asset register
- Risk Assessment and Treatment Report
- SOA (Statement of Applicability) Document
- Risk Assessment Procedure
- Internal Audit Procedure
- CAPA Procedure
- Effective measurement Metric
- Effective Measurement Procedure
- ISMS Manual
- Document Control Procedure
- Record Control Procedure
- ISMS Scope
- ISMS Policy
- User Awareness Training presentation
- Quiz Questions & Answers
- Internal Audit Report

1.1.7. Vendor Risk Assessment

1.1.7.1. Scope of Work

Outsourcing of critical functions related to IT and Business should be assessed on periodic basis. The review should covers security control areas like HR Security, Physical Security, Email Security, Logical Access control, Business continuity, Change management, Incident management, Media handling, Vendor governance, Network security, Systems security, Legal & compliance and each vendor should be assessed based on applicability of the controls. Assessment checklist should also cover server & desktop assessment on sampling basis, which are used for processing of bank's data. The assessment should also include:

- To access 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

1.1.7.2. Deliverables

Reports on the above areas with recommendations

1.1.8. Cyber law Consultancy

Considering the emerging challenges in Cyber space, Bank aims to avail consultancy on varied subject of Cyber law. Some of the subjects are given below. It is to be noted that the scope given here is illustrative and not exhaustive.

1.1.8.1. Scope of work for cyber law consultancy

- Electronic Banking/ Online Banking/ E-Cash and E-Payments
- Cyber Crime/ Cyber Torts/ Cyber law precaution /cyber rights
- Domain name dispute/ Community standards/ Certification
- Encryption/ Cryptography/ Information Privacy/ Legislation
- Internet, e-mail & cloud policies/ Internet Regulation/ ISP Liability
- Advertisement/ Publicity on internet/ Information Network policy
- Social Media Management
- Content/ Meta tags/ electronic contracts
- Cyber staling/ Cyber Fraud/ Cyber liberties/ Cyber war
- Cyber hate/ Cyber threat/ Cyber laundering/ Cyber Stalking
- Software licensing/ Consumer protection/ Database protection
- Web linking and framing/ internet regulation/ Authentication
- E-learning/ spamming/ Jurisdiction/ search and seizures
- Legal audit of websites
- Internet Policies
- Privacy Privilege & Confidentiality
- Freedom of Expression
- Economic Espionage
- Authentication of Digital Signatures
- ISP Liability
- Computer Network Service

1.1.8.2. Deliverables

- Advisory reports and alerts on the above areas with recommendations and solutions as per practises in the industry

- Advisory report relating to cyber security over cloud, the legal issues relating to the same and the need for complying the local law and their requirement relating with information security.

1.1.9. Red Team Exercises

In order to put Bank's cyber security defence to the test, Bank intends to run a realworld scenario that's designed to measure how well organization's defensive and response capabilities will stand up against social, physical, network and application attacks from a simulated real-life adversary.

1.1.9.1. Scope of Work for Red Team Exercise

- Recognizing security issues within the Bank
- Perform assessment on local/remote networks
- Examining an organization for weaknesses as through the eyes of an industrial spy or a competitor
- Social engineering
- Trusted systems testing
- Password Cracking
- Identification of possible weak points in physical and logical security
- Vulnerability Research and Verification (automated and manual)
- Competitive Intelligence
- Internal application Testing
- Exploit Research
- Security testing of Firewalls, ACL other security devices
- Identification of Rouge Devices
- Cyber war game
- Determining appropriate counter-measures to thwart malicious hacking
- Conduct simulated cyber-attacks on the bank's infrastructure
- Validate protections and monitoring around high-value systems
- Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks

1.1.9.2. Deliverables

- A report presenting results & conclusions of the exercise, covering technical, process and policy issues with a series of industry best-practice recommendations
- Review of results and feedback in a workshop setting, to build awareness and alignment among stakeholders, and a roadmap of measures to improve security & resilience in the future
- Short-term tactical fixes for immediate remediation of any outstanding vulnerabilities within the tested environments
- Vulnerability report with mitigation plan and recommendations
- Long-term strategic initiatives that will proactively thwart any potential repetition of vulnerabilities discovered during the exercise

1.1.10. IS / Cyber Security Program Management

1.1.10.1. Scope of Work

- Supporting monitoring of all information security related activities

- Identification of Information Security Control Objectives
 - Common
 - Management
 - Operational
 - Technical
 - Privacy
- Maintaining overall data
- Providing snapshots, dashboards, tracking
- Continuously scanning external environment
- Cyber Drill
- Cyber Security Operation Centre Review
- Reporting, monitoring, analysis
- Compliance with the Cyber Security Framework as per RBI directives

1.1.10.2. Deliverables

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

1.1.11. Review of Log Monitoring/SOC implementation and operations during contract period

1.1.11.1. Scope of Work

- Review of SOC activity related to logs monitoring
- Review of alerts raising mechanism and closure for SOC related activity,
- Review of SOC activity related to Storage,
- Review of SIEM correlation rules and add-on tools
- Review of SOC alert Tracking & Closure of incidents

1.1.11.2. Deliverables

- Detailed Gap assessment report for SOC implementation, operational procedures followed with recommendation and industry best practices.

1.1.12. Information Security Awareness

1.1.12.1. Scope of Work

- General Information Security Awareness
- Specialised Information Security Training

1.1.12.2. Deliverables

- Content creation – presentations, audio, video, e-learning content, quizzes
- Conducting training sessions

1.1.13. Web and Application Security

1.1.13.1. Scope of Work for Web and Application Security Assessment

A. Technical Assessment

- The assessment should cover both business logic and technical risks
- 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
- The tester should attempt to identify and exploit vulnerabilities that include the latest OWASP Top 10, including:
 - Input validation
 - Injection
 - Cross site scripting
 - SQL and XSL injection
 - Cookie modification
 - Code execution
 - Buffer overflow
 - URL manipulation
 - Weak Authentication and Session Management / Authentication bypass
 - File upload vulnerabilities
 - Insecure Direct Object References
 - Sensitive Data Exposure
 - Missing Functional Level Access Control
 - Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA etc
 - Session hijacking
 - CSRF - Cross Site Request Forgery
 - Using Components with known Vulnerabilities
 - Privilege escalation
- The report should show risk to the business based on any exploits found.
- The assessment report should contain a test plan that shows what tests were conducted and its status.

B. Process Assessment

- 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)
- 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
 - 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 being 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

C. Others

- Review the audit trail features of the applications in scope, understand how the audit trail reports are reviewed by BANK to detect errors and understand how the reported errors are corrected in a timely manner.
- Review the maintenance and storage of audit trails and logs in order to assess whether the same can be used for forensic study if required by Bank
- Understand the legal and statutory requirements related to using the applications in scope

- Review other related procedures namely backup, change management, Escrow arrangement for source code and risk management processes for the applications in scope.

1.1.13.2. Deliverables

- Identified threats for each application.
- Report of findings and recommendations for each application.
- All the reports would be prepared module/functionality-wise keeping the following points in view:
 - The assurance that application functions as intended by Bank's information security policy
 - Identification of gaps/ deviancies/ deficiencies/ vulnerabilities/ risks and detailed observations and its potential impact on the business
 - Industry best practices
 - Specific recommendations for improvement o Adequate verifiable audit evidences
- Security and control review report of the applications in scope
- All observations will be thoroughly discussed with team/application owners before finalization of report and the user's views/explanations to be noted for deviations/recommendations. However this should not influence the independent views/observations of the auditors.
- All the documents and audit evidences, documentary or otherwise with screenshots/gist of discussion with stakeholders.

1.1.14. Code Review

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

1.1.14.1. Scope of Work

- 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 as per criticality of the code
- Use combination of tools like custom scripts, static code analyzers, process, file and registry usage monitors, disassemblers, de-compilers etc.
- Verify the findings reported by the tools and prioritize them based on their criticality and impact

1.1.14.2. Deliverables

The code review report should contain the following at minimum:

- Vulnerabilities identified
- Vulnerability ratings
- Threat Profile

- Test Plan
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible □ Solutions with details and additional resources.

1.1.15. Domain/Channel Process Audit

1.1.15.1. Scope of Work

Same as given above for Application Security Assessment. This assessment is to be done for specific area/application in the bank such as internet banking, ATM etc.

1.1.15.2. Deliverables

Same as given above for Application Security Assessment

1.1.16. BCP / DRP (ISO 22301) consulting

Bank is currently ISO 22301:2012 certified for its DC & DRC systems. To advance maturity levels further, Bank 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 Bank wide response plans.

1.1.16.1. Activities under BCM

A. Systems Study

- Read the existing BCP policy of Bank and review it against leading practices to identify gaps.
- Benchmark it with the requirements of standards such as ISO 22301:2012
- Discuss the recommendations with the Bank and assist in documenting the new policy and associated processes / documents based on the recommendations accepted by Bank

B. Assist in documenting a high level roadmap and timeframe for the BCP engagement

- Understand the business operations of Bank 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.

C. 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 well being;
 - 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.
- Discuss with management the approach for assessing the impact of disruption and present the findings and conclusions.
- Review the results of business impact assessment, recovery time objectives(RTO) for operations and recovery point objectives (RPO) 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);
 - supporting technology, plant and equipment (technology);
 - 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

D. BCM Strategy

- Determine and guide Bank officials 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 Bank and assist in determining the relative costs for implementing strategies and provide cost benefit analysis

E. 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.

F. 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.

G. Implementation and Training

- Create the teams and allocate responsibilities in line with BCP
- Conduct training and awareness sessions for end users
- Assist Bank officials in implementing procedural and technical measures as per plan

H. 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

I. Certification Support

1.1.16.2. Deliverables

- Project Plan
- Threat and Risk analysis document
- Impact scenarios
- BIA document
- BCM Strategy documents
- Plan and procedure documents
- Testing and Maintenance plan
- Training program and content document

1.1.17. Security solution consulting

1.1.17.1. 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.

1.1.17.2. Deliverables

Various reports capturing the analysis of solutions, evaluation reports, executive summary, management presentations.

1.1.18. 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.

1.1.18.1. Scope of Work

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.

1.1.18.2. Deliverables

Various reports capturing the analysis of projects, evaluation reports, executive summary, management presentations

1.1.19. 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 labelling product for effectively managing unstructured data
- Ensuring identification of granular rule sets for DLP and other solution implementation

1.1.19.1. Scope of Work

- A. Review of existing Data Asset Classification Policy and Methodology
- B. Perform data risk assessment to assess security loopholes from where data can get leaked
- C. Develop a robust data governance framework which encapsulates:
 - Data Identification
 - Data Classification
 - Records Management
 - Data Security control matrix
 - Secure Data disposal processes
- D. Develop Data Classification Guideline and Procedure document (encompassing complete data lifecycle including registration, maintenance, de-classifying and deregistration/ discarding process)
- E. To develop training presentations and relevant materials for different audiences such as, business users, technical teams, managers etc.
- F. Prepare the Data Classification Project Plan clearly identifying the milestones timelines, approach and resources required.
- G. Conduct Data Flow Analyses for the business units across the enterprise
- H. Identify key documents & data that need to be classified
- I. Identify the supporting applications and corresponding databases for classification and DLP protection.
- J. Identify the owner, custodian & authorized users (white listed users)
- K. Populating data in Data Classification Repository
- L. To create a granular matrix that defines DLP authorization for individual user (Employee) and DLP channels (such as USB, email, print etc.)
- M. Implement data labelling solution for classifying all unstructured data based on the data classification policy
- N. Data Disclosure, sharing, exchange with internal / external stakeholders and government / public agencies / legal requirements.

1.1.19.2. Deliverables

- Data Governance Framework

- Data Classification Policy, Standards, Procedures, Templates and Guidelines
- Records Management Policy, Procedures, Templates and Guidelines
- Secure Data Handling Policy & Procedures
- Data Workflow Assessment Report
- Recognised Data Values and Data Risk Assessment Report
- Data Labelling Product & Implementation Support
- Data Disclosure related guidelines / report.

1.1.20. Mobile Application Protection

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

1.1.20.1. Scope of Work

- 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 /or Malware Insertion, Spoofing of Mobile App to access sensitive data, 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, Regeneration, 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.

1.1.20.2. Deliverables

The mobile application security report should contain the following at minimum:

- Vulnerabilities identified
- Vulnerability ratings
- Threat Profile
- Test Plan
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible □ Solutions with details and additional resources.

1.1.21. Forensic Analysis/Investigations

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

1.1.21.1. Scope of Work

- The vendor should have skill set 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

1.1.21.2. Deliverables

Deliverables should include detailed analysis reports, summary reports with timelines, evidences collected in scientific manner, etc as required in forensic analysis activity.

1.1.22. PCI-DSS Services

1.1.22.1. Scope of Work

Ensure compliance to the following PCI DSS standard requirements:

- A. Build and Maintain a Secure Network and Systems
 - i. Setup secure processes for managing security devices including firewalls
 - ii. Implement the process for secure commissioning of servers, network devices, security devices and applications
- B. Protect Cardholder Data
 - i. Implement controls to mitigate the risks to card holder data
 - ii. Implement encryption across links including WAN, Internet to protect card holder data
- C. Maintain a Vulnerability Management Program
 - i. Setup processes for antivirus management
 - ii. Develop and maintain secure systems and applications.

D. Implement Strong Access Control Measures

- i. Identify and authenticate access to system components.

E. Regularly Monitor and Test Networks

- i. Implement controls for tracking and monitoring access to network resources and cardholder data.
- ii. Implement controls to enable periodic testing of IT infrastructure including wireless, applications

F. Maintain an Information Security Policy

- i. Define policies and procedures that addresses information security for employees and contractors

G. Guidance on PCI DSS compliance

- i. Provide guidance to implement controls and best practices to achieve compliance.

1.1.22.2. Deliverables

- Card Holder Data Matrix
- Card Holder Data Flow Diagram
- Card Data Discovery Report
- PCI-DSS Awareness workshop
- Gap Analysis Report
- Vulnerability Scanning Report
- Redesigned – Suggested network Architecture Diagram
- Enhanced Security Policies and Procedures
- Technology evaluation & recommendations
- Sample Security Configuration Assessment Reports
- Network Assessment Report
- Report on Compliance
- Card Brands Reporting Documents

1.1.23. Documentation – Policy, Processes, Procedure Creation/Review/Modification etc.

1.1.23.1. Scope of Work

- Drafting new Policy, Processes, Procedure for Bank as per Bank/ Regulatory requirement
- Reviewing/Modification of Existing policy as per industry best practices
- GAP assessment

1.1.23.2. Deliverables

- Drafted Policy, Process & Procedures
- GAP Assessment Reports

1.1.24. Threat Modelling for various Software/App Development

1.1.24.1. Scope of Work

- Analysis of Bank's various Business software/applications/mobile apps for attack simulation and threat analysis
- Model attack scenarios
- Calculate residual risks
- Identification of threats and assigning possibility to each threat
- Mapping of threat to security controls
- Development of threat assessment framework for Bank

1.1.24.2. Deliverables

- Threat assessment framework
- Threat analysis report with recommendations and threat mitigations controls

1.1.25. Security and Network Architecture Review

Consultant shall review the Data centre and Wide Area Network of Bank to identify single point of failures, network availability, logical segregation and deployment of security products/technologies etc. The assessment is to be carried out for Data centre LAN, DRLAN, network connectivity from branch office to Data centre, Sample branch networks and ATM networks etc.

1.1.25.1. Scope of Work

- Review for Network security architecture
- Review of DMZ Placement
- Review the appropriate segregation of network into various trusted zones
- Review the traffic flow in the network
- Review of routing protocols and security controls therein
- Review the security measures at the entry and exit points of the network
- SOC/ C-SOC Architecture review
- Configuration review of network and security devices including Firewall, IPS, IDS, Routers, Switches, etc
- Rule based review of firewall and IPS
- Review of security measures at entry and exit points of network
- Review of key processes related to network and information security
- Network vulnerability assessment

1.1.25.2. Deliverables

- Assessment methodology
- Detailed assessment report including recommendations (quick fix, short fix, etc)
- Executive summary report
- Presentations

1.1.26. Assess, Develop and Review Information Technology & Information Security Performance Dashboards focused on various measures such as effectiveness, ROI to convey value of investment on IS infrastructure across the Bank

1.1.26.1. Scope of Work

- Development of Information Technology/Information security dashboards

- Define Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) for assessing cyber security performance of Bank

1.1.26.2. Deliverables

- Dashboards, KPIs, KRIs
- Presentations and Short Videos for Management

1.1.27. Assess, Develop and Review Information Security Controls, Standards, Metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

1.1.27.1. Scope of Work

- Assessment of Information Security Controls, standard and metrics used in Bank against industry best practices
- Detailed GAP assessment as per Bank/Regulator guidelines

1.1.27.2. Deliverables

- Assessment Report with detailed supporting evidences
- Recommendation in terms of short term and long-term implementations
- Presentation and short videos for Management

1.1.28. Investigations of frauds (process related, cyber related etc.) reported by the bank/customers to find out the root cause and suggest remedial measures.

1.1.28.1. Scope of Work

- Investigation of modus operandi of the frauds and find the root cause for such frauds. Assessment of Information Security/process related Controls (deficiencies, improvements etc.)

1.1.28.2. Deliverables

- Investigation Report with detailed supporting evidences
- Recommendation in terms of short term and long-term implementations
- Presentation and short videos for Management

Required Skill Set:

The bidder should have adequate number of skilled resources to meet Bank's requirements as per the table given below:

Skill Set Level	Work Experience	Basic Requirements
Level-1	3 to 5 years	• Certificate CEH,ISO 27001LA/LI, CCNA/CCNP, Associate of CISSP, CISA, CISM, Specialized Product certifications • Experience Conduct of domain level assessment
Level-2	Above 5 years	• Certificate CISSP, CISA, CISM, CRISC, CHFI, Specialized Product/domain certifications • Experience previous experience in specialized services

The bidder will be expected to provide helpdesk–voice / email / portal based support for some of the services as desired by the Bank. This should include escalation matrix. The availability of this service should be commensurate with the type of service like 24*7 log monitoring.

The bidder should provide requisite report including dashboard etc for all Regulatory / Compliance and Security requirements.

All the services provided by the bidder should conform to the security best practices.

The bidder should comply with Bank's Information Security Policy & Cyber Security Policy and procedures (The policy may revise time to time) in key concern areas relevant to the RFP.

Section IV: Bid Guidelines

1. Bid Price

- 1.1 RFP document can be purchased against payment of Rs.5,000/- (Rupees Five thousands only) in the form of a demand draft/Pay Order issued by a scheduled commercial bank favouring Central Bank of India, payable at Mumbai.
- 1.2 In the event of non-payment of the fee of Rs.5,000/-towards the RFP document form before the submission of the offer, the offer will not be considered/opened.

2. Bid Security

- 2.1 Bid security of Rs.3,00,000/- (Rupees Three Lakh Only) in the form of a demand draft/ Pay Order or Bank Guarantee (BG) issued by a scheduled commercial Bank other than Central Bank of India favouring Central Bank of India, payable at Mumbai to be submitted along with the offer.
- 2.2 The bid security must be submitted along with technical offer. In the event of non-submission of the bid-security of Rs.3,00,000/-, the proposals will be rejected.
- 2.3 The Bid Security will be refunded to the unsuccessful bidders only after completion of the bid process.
- 2.4 No interest will be payable on the Bid Security amount.
- 2.5 The Bid security amount will be forfeited if the selected bidder refuses to accept assignment or having accepted the assignment, fails to carry out his obligations mentioned therein
 - If a bidder withdraws its bid during the period of bid validity and/or
 - In case of a successful Bidder, if the Bidder fails:
 - In the Contract within the stipulated time and/or
 - To furnish Performance Bank Guarantee as Security within the stipulated time and valid till the end of warranty period.
 - The Bidder refuses to accept purchase order or having accepted the purchase order, fails to carry out his obligations mentioned therein
- 2.6 Within Ten (10) days of the receipt of formal notification of award from the Bank, the successful Bidder shall submit the Performance Bank Guarantee (PBG) for the value equivalent to Rs.3,00,000/-. The PBG should be valid for the entire contract period i.e. 2 Years in this case (plus an additional grace period of 3 months) in the format prescribed in Annexure H.

- 2.7 **Integrity Pact-** Each Participating bidder/s shall submit Integrity Pact (as per attached Annexure N) duly stamped of Rs 500. Integrity pact should submit by all participating bidder at the time of submission of Bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time scheduled prescribed by Bank may be relevant ground of disqualification to participating in Bid process.

3. Technical Bid

- 3.1 The offer will be in one part i.e. Technical Bid.
- 3.2 Technical Bid must be submitted giving full particulars as per the prescribed formats, in sealed cover duly super-scribed.

“TECHNICAL BID FOR EMPANELMENT OF INFORMATION TECHNOLOGY / CYBER SECURITY SERVICE PROVIDERS FOR CENTRAL BANK OF INDIA”

- 3.3 The envelope must be addressed to the Asst. General Manager (DIT), Central Bank of India, DIT, 1st floor, Sec.11, Plot No.26, Opp. Belapur Rly. Station, CBD Belapur, Navi Mumbai 400 614 and submitted on or before the prescribed time schedule of this RFP.
- 3.4 Technical bid should contain the proof for the eligibility criteria, technical solution and un-priced Technical bid and should contain all information asked for in these documents. It should not contain any price information. However there should be a confirmation that all required rates have been quoted in Price bid, without showing the actual amounts.
- 3.5 It is mandatory to submit all the details in the prescribed pro-forma (Annexure-B) duly filled in, along with the offer. The Bank, at its discretion, may not evaluate a Technical Bid in case of non-submission or partial submission of technical details.
- 3.6 Technical Bid must be submitted in an organized and structured manner. No brochures/leaflets etc. should be submitted in loose form.
- 3.7 The Technical Bid should comprise of following:
1. Covering letter on the prescribed format (Annexure-A).
 2. Complete details with all the columns filled in (Annexure-B).
 3. Compliance to Eligibility Criteria (Annexure - C)
 4. Statement of Bidder (For last 3 years) (Annexure C1)
 5. Specific Work Experience of Vendor during past three years in BANKS (Annexure C2)
 6. List of Experienced Staff working in the Company (Annexure C3)
 7. Priority list of Services and Assignments by the ITCSSPs in BFSI Sector (Annexure C4)
 8. Reference site details (Annexure-D) duly filled in with photocopies of required certificates / documents / proof should be attached.
 9. Undertaking for providing Performance Bank guarantees as and when required (Annexure-F)
 10. Undertaking that they have not been blacklisted by the Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response as per Annexure-G
 11. Bank guarantees (Annexure- H)
 12. Compliance to RFP terms and condition (Annexure-I)
 13. Pre Bid Query Format (Annexure J)

14. Undertaking of KYE (Annexure K)
15. Format of Bank Guarantee For EMD (Annexure - L)
16. Confidentiality/ Non-Disclosure Agreement (Annexure M)
17. Integrity Pact (Annexure N)
18. Expertise in Methodologies (Documents on Information Technology/Cyber Security services/framework/tools/templates & utilities to be provided)

4. Offer Validity Period

The offer should remain valid for a period of at least 180 days from the date of opening of technical bids.

Opening of Offers

1. TECHNICAL BID – Empanelment of Information Technology / Cyber Security Service Providers for Central Bank of India will be opened as per the schedule of this RFP.
2. One representative of the bidder may be present for the opening of the Technical Offers.
3. No separate intimation will be given in this regard to the bidders, for deputing their representatives.

5. Bidding Document:

All pages of the Bid document should be serially numbered and shall be signed by the authorize person(s) only. The person(s) signing the bid shall sign all pages of the bid and rubber stamp should be affixed on each page except for a no amended printed literature. The bidder should submit a copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document.

The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not substantially responsive to the bidding documents in every respect will be at the Bidder's risk and may result in the rejection of its bid.

6. Erasures or Alterations

The original offer (Technical Offer and Indicative Commercial Offer); shall be prepared in indelible ink. There should be no hand-written material, corrections or alterations in the offer. Any such corrections must be initialled by the persons or person who sign(s) the proposals Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the forms using terms such as "OK", "accepted", "noted", "as given in brochure/manual" are not acceptable to the Bank. The Bank may treat non-adherence to these guidelines as unacceptable.

7. Right to Alter Quantities / Repeat orders

- 7.1. The Bank will be free to either reduce or increase the quantity of services to be availed on the same terms and conditions. The Bank reserves the right to alter quantities.
- 7.2. The Bank also reserves right to place further order on same terms and conditions within a period of twelve months from the date of first purchase order / letter of intent.

- 7.3. No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the contract shall be made by the successful bidder except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the contract, by notice in writing to instruct the successful bidder to make any variation without prejudice to the contract. The finally selected bidders shall carry out such variation and be bound by the same conditions as far as applicable as though said variations occurred in the contract documents. If any suggested variations would, in the opinion of the finally selected bidders, if carried out, prevent him from fulfilling any of his obligations under the contract, he shall notify Bank thereof in writing with reasons for holding such opinion and Bank shall instruct the successful bidder to make such other modified variation without prejudice to the contract. The finally selected bidders shall carry out such variation and be bound by the same conditions as far as applicable as though said variations occurred in the contract documents. If Bank confirms its instructions, the successful bidder's obligations shall be modified to such an extent as may be mutually agreed, if such variation is substantial and involves considerable extra cost. Any agreed difference in cost occasioned by such variation shall be added to or deducted from the contract price as the case may be.
- 7.4. In any case in which the successful bidders have received instructions from Bank as to the requirement of carrying out the altered or additional substituted work which either then or later on, will in the opinion of the finally selected bidders, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.
- 7.5. If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of change in contract price, before the finally selected bidder(s) proceeds with the change. In all the above cases, in the event of a disagreement as to the reasonableness of the said sum, the decision of Bank shall prevail.
- 7.6. The Bank reserves the right to alter the number of locations specified in the tender, and to delete/substitute items from the ones specified in tender. Bank may also place order for various services which are only part of this RFP in addition to the quantities mentioned in this tender at the same rate terms and conditions including the cost agreed upon.

8. Bidder Queries

- 8.1. All queries with regards to this bid, if any, must be sent to the Asst. General Manager -IT, Central Bank of India, DIT, CO, Mumbai on or before the scheduled time given for Queries (Email id smitpurchase@centralbank.co.in & sminfosec@centralbank.co.in).
- 8.2. The Bank is not obliged to divulge the nature and configuration of its IT / IT Security Infrastructure.
- 8.3. The Bank at its sole discretion, reserves the right whether or not to respond to queries raised by bidders or provide written clarifications. No oral responses to a clarification request shall be constructed as amending this RFP document. No extension of any deadline will be granted on the basis grounds that the Bank has not responded to any question or provided any clarification.
- 8.4. All the queries should be as per defined format by banks in Annexure- J.

9. Amendment of bidding documents:

- 9.1. At any time prior to the date for submission of bids, the bank may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the Bidding documents by amendments.
- 9.2. Amendments, if any will be notified through Bank's web site to all prospective Bidders, which have received the Bidding documents and will be binding on them.
- 9.3. In order to provide, prospective Bidders, reasonable time to take the amendment into account for preparing their bid, the Purchaser may, at its discretion, extend the last date of submission of bids

10. Terms of execution of work:

- 10.1. Empanelled Bidder/Bidders shall start the services within 2 weeks from the date of the Purchase order in a time bound manner as required/stipulated by the Bank. In case of delay in start of services or meeting timelines/deadlines stipulated by Bank, penalty will be charged as mentioned in Liquidated Damages clause.

11. Overview of Evaluation Process (Two Part Offer):

- 11.1. In the first stage, only TECHNICAL BID will be opened and evaluated. Those bidders satisfying the eligibility criteria and the technical requirements as determined by the Bank and accepting the terms and conditions of this document shall be short-listed.
- 11.2. The Bank will evaluate the technical offers of the bidders in terms of the eligibility criteria and proposals meeting the criteria will only be taken up for further technical evaluation.
- 11.3. THE PROPOSALS WHICH DO NOT CARRY POINT WISE DETAILS OF MEETING THE ELIGIBILITY CRITERIA AND SUPPORTING DOCUMENTS WILL BE REJECTED.
- 11.4. The products evaluation will be done on the basis of the information provided in the responses information available in the brochure attached and OEM's details (wherever applicable).
- 11.5. Only proposals meeting the products requirements will be taken up for further commercial evaluation. Proposals quoting the products not meeting the requirement may be rejected. After completion of technical evaluation, the Commercial Bid of only eligible bidders, whose bids are short-listed, will be opened.
- 11.6. The offers should either be hand delivered or dropped in the Tender box at the given address before the stipulated date and time. In case designated date of bid submission is declared to be public holiday, the same may be extended to next working day.

12. No Commitment to Accept Lowest or Any Tender

The Bank shall be under no obligation to accept the lowest or any other offer received in response to this notice and shall be entitled to reject any or all offers without assigning any reason whatsoever.

13. Late Bids

Any bid received by the Bank after last date and time of submission of bid prescribed by the Bank, may be rejected and/or returned unopened to the Bidder. Bank reserve right to accept or reject any such bids without assigning any reason thereof.

14. Evaluation Criterion:

14.1. Evaluation of Technical Bids:

The Bank's evaluation of the technical bids will take into account the following factors and based on such evaluation the technically qualified bidders will be shortlisted:

- a) Scrutiny of minimum Eligibility Criteria as given in Annexure – C, C1, C2 C3 & C4 for proposed services, reference calls and site visits, if required.
- b) Compliance of terms and conditions stipulated in the RFP duly supported by certified documentary evidence called for therein.
- c) Submission of duly signed compliance statement as stipulated in Annexure I. Details / Brochures containing data centre infrastructure facilities are to be enclosed.
- d) Review of written reply, if any, submitted in response to the clarification sought by the Bank, if any.
- e) The Bank reserves the right to evaluate the bids on technical & functional parameters including possible visit to inspect live site/s of the Service providers and witness demos, presentations or undertake a POC exercise of the system and verify functionalities, response times, users acceptability etc.

14.1.1. Bank reserves the right to reject an offer under any of the following circumstances:

- a) Bid security is not submitted.
- b) Document fees are not paid, if required.
- c) Offer is incomplete and/or not accompanied by all stipulated documents.
- d) Offer is not in conformity with the terms and conditions stipulated in this document.
- e) Requirement compliance stipulated in Annexure-H is not met. However, deviations resulting in higher/superior configuration will be accepted.
- f) Unpriced commercial offer is not submitted along with Technical Offer.
- g) Format of commercial offer differs from unpriced commercial Offer.

14.1.2. The evaluation will also take into account:

- a) State of the art services offered by the bidder to any noticeable Bank in India. The bidder should furnish the details.
- b) Capability of the proposed services to meet future requirements not outlined in the RFP
- c) In house capability of tools / utilities development
- d) Bidder support facilities

Technical Bid Evaluation:

S.No.	Activities related to IT / Cyber Security	Maximum Marks	Marks Scored	Remarks

1.	Turnover of the bidder- minimum annual turnover of Rs.50 Crores in the last three financial years (i.e. 2014-15 & 2015-2016 & 2016-17) (For scoring purpose, average of three years turnover will be considered) More than 500 Crore : 25 Marks	25		
----	---	----	--	--

	250-500 Crore Turnover : 20 marks 50-250 Crore Turnover : 15 marks <i>(Minimum required marks -15)</i>			
2.	Total Number of Assignment carried out in BFSI related Information Technology/Information Security/ Cyber Security Activities in India in last three years (from 01.04.2015) as declared in Annexure – C to be submitted by the bidder. One mark per assignment /purchase Order [Max 5 marks for same/similar activity] for different activities in different organization. <i>(Minimum required marks -10)</i>	30		
3.	Total Number of Assignment carried out in BFSI related Information Technology/Information Security/ Cyber Security Activities for Global Client to be submitted by the bidder. One mark per assignment /purchase Order after 01.04.2015. <i>(Minimum required marks –N.A.)</i>	10		
4.	Total Number of special information security incident response/IT investigation/ Digital Forensics related services performed for Banks in India. 1-2 assignment : 10 Marks 3-5 Assignment : 15 Marks More than 5 Assignment : 20 Marks <i>(Minimum required marks -10)</i>	20		

5.	Total No. of Skilled Employees / Resources available as per the enclosed list of Employees with their Credentials / Certifications related to Information Technology/Information Security/ Cyber Security Activities given in the Annexure C. 22 to 50 Employees -- 10 Marks 51 to 100 Employees --15 Marks 101 and above Employees -- 20 Marks (Minimum required marks -10)	20		
6.	No. of Years" Existence/Establishment in Information Technology/Information Security/ Cyber Security related activities in INDIA in BFSI Sector. Evidence of the 1st Assignment to be enclosed as a proof of Experience. – One Mark per year prior to 01.04.2013. (Minimum required marks –N.A.)	5		
7.	Technical Skill Credentials (extra ordinary activities) – Proprietary Tools Developed, R&D Work Done, Papers Published, Other Value added Services and Additional Deliverables, Proprietary Tools, Dashboards, Training, Knowledge sharing, etc. Attach Evidences as a proof. Each activity will carry 1 mark and subject to Max of 15 marks. (Minimum required marks –N.A.)	10		
8.	Presentation and Methodologies , Procedures, Tools, Utilities, Templates Developed /used during execution of previous assignments and arrangements for BCPDR infrastructure proposed etc presented by bidder. Marks will be given by Bank Team based on Presentations *Bidder fulfilling the eligibility criteria will be called for presentation and product demonstration, in accordance with the responses given for identified requirements, any time after the date of submission of bid. The Bank will communicate the date and time to the bidder. (Minimum required marks -20)	30		
	Total Marks	150		
Total Marks are to be calculated and filled by the Bidders for item Nos. 1 to 7 and submit together with the Technical Bid Cover				

Bidders will be shortlisted and grouped as follows:

Group of top 10 bidders scoring 75% and above , subject to the minimum scoring as mentioned in the above table.

Bidders scoring less than 70% will not be considered for further stages of evaluation. In case during Technical evaluation, all the bidders fail to score more than 75% marks, or less than ten bidders obtain 75% or more marks, then in that case top ten bidders (if available) will be considered for the Group provided marks obtained by them are more than 70%. The decision of the Bank in this regard shall be final.

Allocation / Distribution of activities/ assignments will be solely at the discretion of the bank. On completion of evaluation process of Technical bids, the Bank reserves the right to opt for checking references provided bidders to establish quality of services rendered by them.

Bank will notify successful bidder(s) in writing by letter in duplicate or email / fax that bid has been accepted. The Selected bidder(s) has/have to return the duplicate copy to the Bank within 7 working days duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.

The successful bidder(s) shall be required to enter into a contract / Service Level Agreement (SLA) with the Bank, within 15 days of the award of the tender or within such extended period as may be decided by the Bank along with the letter of acceptance, Non-Disclosure Agreement (NDA) and other terms and conditions as may be determined by the Bank to be necessary for the due performance of the work in accordance with the Bid and acceptance thereof.

Copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted. In case of failure to accept the empanelment within 7 days from the date of receipt of the communication, the Bank will be at liberty to cancel / drop the empanelment offer for that vendor.

The contract/agreement will be based on bidders offer document with all its enclosures, modifications arising out of negotiation / clarifications etc. and will include Service Level Agreement (SLA), project plan – phases & milestones and schedule as applicable, copies of all necessary documents, licenses, certifications etc.

The Bank reserves the right to stipulate, at the time of finalization of the contract, any other document(s) to be enclosed as a part of the final contract.

15. Awarding of Assignment

This is an empanelment only, the actual job allocation or Scope of Work will be a dynamic time to time activity and in any areas of IT/Cyber Security related activities as required by Bank; payments will be based on actual work mutually agreed at the time awarding an assignment / contract.

Based on the requirements, Bank at its discretion will call quotations from the empanelled bidders for awarding assignments. Decision of the Bank in this regard will be final.

16. Order Cancellation:

16.1. The Bank, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Supplier/bidder, may terminate this Contract in whole or in part.

- 16.2. The Bank reserves its right to cancel the order in the event of delay in delivery of the deliverables.
- 16.3. If the Bidder / Service provider fails to perform any other obligation(s) under the Contract.
- 16.4. In the event the Bank terminates the Contract in whole or in part, the Bank avail services from any empaneled vendor with Bank, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered services and the Supplier shall be liable to the BANK for any excess costs for such similar Services performed by other empaneled vendor in the course of completion of the Assignment. However, the Supplier shall continue performance of the Contract to the extent not terminated.
- 16.5. In addition to the cancellation of contract and Purchase order, the Bank also reserves the right to invoke the Bank Guarantee given by the Vendor to recover the damages and to recover compensation from the vendor on account of wastage of time, money and services.16.5. The Bank shall have the right to cancel the contract with the empaneled vendor at any time during the contract period, by giving a written notice of at least 3 (three) months, for any valid reason, including but not limited to the following reasons:
- a) Laxity in following security standards given by the Bank
 - b) Excessive delay in execution of orders placed by the Bank
 - c) Discrepancies/deviations in the agreed processes and / or products
 - d) Violation of terms & conditions stipulated in this RFP at any point of time during the contract period.

17. Liquidated Damages:

- 17.1. Notwithstanding the Bank's right to cancel the order, liquidated damages at 2% of the cost of undelivered service/s per site per week or part thereof will be charged for every week's delay in delivery subject to maximum 25% of order price.
- 17.2. The Vendor shall start the work related to availed services within 2 weeks from date of Purchase Order . Any delay beyond stipulated period will attract additional penalty @ 2% per week or part thereof of order value maximum 25%.
- 17.3. Maximum penalty is of 25% of order value excluding applicable taxes.
- 17.4. The Bank reserves its right to recover these amounts by any mode such as adjusting from any payments to be made by the Bank to the vendor/company.
- 17.5. Part of week will be treated as a week for this purpose.
- 17.6. However, the Bank may, at its discretion, waive the liquidated damages in case the delay is not attributable to the Bidder.
- 17.7. Once the Liquidated damages is reached on the maximum, Bank may also consider termination of Contract/empanelment/Assignment.
- 17.8. The empanelled Service Provider may be penalized or counter part of legal action against misguidance, if any.

18. Inspections & Tests:

- 18.1. The Bank or its representative shall have the right to inspect and/or to test the services/Solution/Technology/hardware/software to check their conformity to the contract specifications at no extra cost to the Bank.

18.2. The inspections and test may be conducted on the premises of the supplier/vendor or its subcontractor(s), at point of delivery and/or at the final destination. If conducted on the premises of the supplier/vendor or its subcontractor(s), all reasonable facilities and assistance as required by the Bank officials/representative, including access to services/Solution/Technology/ Drawings, system start/boot and production data, shall be furnished to the inspectors at no charge to the Bank.

19. Media & Documentation:

The vendor is expected to provide Media & Documentation for all the services provided. Latest copy of the required document of availed service may be submitted along with an undertaking on company's letter head stating that it contains valid and legal copy as required by the Bank.

20. Supplier's Obligations:

20.1. The Bidder / Supplier is responsible for managing the activities of its personnel or and will hold itself responsible for any misdemeanours.

20.2. The Bidder's / Supplier's representative and local office at Mumbai will be the contact point for the Bank and all the authentic status of delivery, Progress and installation should be made available in writing at least twice in a week

20.3. The Bidder / Supplier will treat as confidential all data and information about the bank, obtained in the execution of its responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank. In case of any breach of trust, the Bank may initiate any action as deemed fit entirely at the cost and responsibility of the supplier.

20.4. Bidder / Supplier has to undertake and agree to save defend and keep harmless and indemnified the Bank against all loss, cost, damages, claims, penalties expenses, legal liability because of noncompliance of KYE and or misconduct of the employee deployed by the bidder / supplier to Bank. Bidder / Supplier to undertake the same as per Annexure-K.

21. Delays in the Suppliers Performance:

Delivery of the goods and performance of the Services shall be made by the supplier in accordance with the time schedule specified by Bank. Any delay in performing the obligation/services by the supplier will result in imposition of liquidated damages and/or termination of contract for such default.

22. Termination and Consequences of termination including Exit Option-

Termination

22.1. The Bank, without prejudice to any other remedy for breach of Contract, by written notice of 30 days default sent to the Bidder, may terminate this Contract in whole or in part, if the Bidder fails to perform any obligations(s) under the Contract at no cost to the bank.

22.2. In the event of the Bank terminating the Contract in whole or in part, the Bank may avail services from any empaneled vendor , upon such terms and in such manner, as it deems appropriate, services similar to those undelivered/non submission, and the Vendor shall be liable to the Bank for any excess costs for such similar services.

22.3 If the Successful Bidder, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract. Corrupt practice means the offering, giving, receiving or soliciting of anything of value or influence the action of a public official in the procurement process or in contract execution; and "fraudulent practice" means a

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

- 22.4. In the event, the Bank terminates the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Successful Bidder shall be liable to the Bank for any excess costs for such similar Goods or Services. However, the Successful Bidder shall continue performance of the Contract to the extent not terminated when the value of the liquidated damages exceed 10% of the contract value.
- 22.5. In case the contract is terminated then all undisputed payment will be given to vendor, but disputed payment shall be adjusted by way of penalty from invoices or PBG.
- 22.6-If the Bidder becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Bidder is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Bidder takes or suffers any other analogous action in consequence of debt; then the Bank plans to, at any time, terminate the contract by giving written notice to the Bidder. If the contract is terminated by the Bank in terms of this Clause, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Bank. In case, the termination occurs before implementation in all the locations in terms of this clause, the Bank is entitled to make its claim to the extent of the amount already paid by the Bank to the Bidder.
- 22.7- The Bidder shall have right to terminate only in the event of winding up of the Bank. Bank will specify the period for remedying any defect.

B- CONSEQUENCES OF TERMINATION :

- a) In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], Bank shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.
- b) In the event that the termination of the Contract is due to the expiry of the term of the Contract, a decision not to grant any (further) extension by Bank , the Vendor herein shall be obliged to provide all such assistance to the next successor Vendor or any other person as may be required and as Bank may specify including training, where the successor(s) is a representative/personnel of Bank to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination hereof.
- c)The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come

into or continue in force on or after such termination.

(C)Exit Option and Contract Re-Negotiation

a. The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:

i. Failure of the successful bidder to accept the contract and furnish the Performance

Guarantee within specified time of receipt of purchase contract;

ii. Delay in delivery, performance or implementation of the solution beyond the specified period;

b. In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Vendor.

c. The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Vendor at more favorable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.

Notwithstanding the foregoing, the Vendor shall continue to have the same obligations as contained in this RFP in relation to such equipment procured from third party suppliers. As aforesaid The Bank would procure the equipment from the third party only in the event that the equipment was available at more favourable terms in the industry, and secondly,

The Equipment procured here from third parties (if any) is functionally similar, so that the Vendor can maintain such equipment. The modalities under this right to re-negotiate /re-procure shall be finalized at the time of contract finalization.

d. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Vendor will be expected to continue the facilities management services and the Bank will continue to pay for services that are accepted by it provided that all products and services as serving satisfactory, as per satisfaction of the Bank.

The Bank, reserve its right to terminate the Agreement/Empanelment without assigning any reason after serving written notice of 30(thirty) days to the Vendor at no cost to the bank.

23. Audit by Third Party

23.1. Bank at its discretion may appoint third party for auditing the activities of ON-SITE Services and operations of entire services provided to the Bank.

23.2. Bank or its regulator (i.e. Reserve Bank of India) reserves the right to audit the Bidder in terms of services offered by bidder or may ask for compliance reports. This includes security related compliance also.

24. Confidentiality

24.1. The Vendor will be exposed by virtue of the contracted activities to internal business information of Bank, affiliates, business partners and /or customers. The vendor must safe guard the

confidentiality of the banks business information, applications and data. Vendor shall execute the NDA(Non disclosure Agreement) with Bank as per attached format under this RFP.

Confidential obligation imposes on the vendor in its nature shall so survive even after termination or expiry of the Agreement/Empanelment.

- 24.2. Disclosure of any part of the above mentioned information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law or other Statutory Authorities, could result in pre mature termination of the contract. The bank may initiate legal action against the vendor for breach of trust alongwith other remedy available under applicable law for time being inforced.

Section V: Terms and Conditions

1. Terms of execution of work

- 1.1. Time, being an essence of the contract, the empanelled vendor are expected to complete the assignment as and when awarded within the stipulated time frame of starting of the assignment, the Bank reserves its right to levy liquidated damages as prescribed hereunder.
- 1.2. The duration of contract for empanelment will be initially for a period of 2 year from acceptance of letter of empanelment. During the validity period of contract Bank may assign the task/work as per requirement time to time any or more than one empanelment Vendor as norms laid down by the BANK, after expiry of the empanelment contract no vendor shall be in empanelment at all.
- 1.3. Non-Disclosure Agreement: In the event of the Vendor getting the assignment of the project under empanelment , an authorized official of the Vendor should execute a NDA with the Bank in the attached format.
- 1.4. The bidder shall be responsible in the event of security incidents.
- 1.5. Escalation Matrix shall be worked out at the time of placing orders from both sides.
- 1.6. Empanelled bidder/bidders shall guarantee that all the software and aligned components used to service to bank are licensed and legal.

2. Indemnity

a)The empanelled bidder/bidders shall, at its own expense, defend and indemnify the Bank against any or losses, claim, damage resulting from the failure of the contractual obligation including all third party claims for infringement of patent, trademark, design or copyright arising from use of proposed product/products or any part thereof.

b)Empanelled bidder/bidders will provide infringement remedies and indemnities for third party Products, on a pass through basis. If the Bank is required to pay compensation to a third party resulting from such infringement, the Bidder shall be fully responsible to pay such compensation along with all costs, damages and attorney's fees and other expenses that a court may finally award, in the event of the matter being adjudicated by a court or that be included in a Bidder approved settlement. The Bank will issue notice to the Bidder of any such claim without delay and provide reasonable assistance to the Bidder in disposal of such claim, and shall at no time admit to any liability for, or express any intent, to settle the claim. The Bidder shall also reimburse all incidental costs, which the Bank may incur in this regard.

c)If such a claim is made or appears likely to be made, the Bank agrees to permit Bidder to enable the Bank to continue to use the Product, or to modify it, provided no order otherwise has been passed by a court or replace it with one that is at least functionally equivalent. If Bidder determines that none of these alternatives is reasonably available, the Bank agrees to return the Product to Bidder on its written request, upon which the Bidder will then give the Bank a credit equal to:

For equipment, its invoice value as paid by the Bank to the Bidder;

For Materials, the amount the Bank paid to Bidder for the creation of the Materials i.e. application, related software, solution, technology etc.

This Section stipulates Bidder's entire obligation to the Bank regarding any claim of infringement.

Bidder has no obligation regarding any such claim based on:

- I. Anything the Bank provides which is incorporated into a Product or Bidder's compliance with any designs, specifications, or instructions provided by the Bank or by a third party on the Bank's behalf;
- II. Bank's modification of a Product's use in other than its Specified Operating Environment;
- III. The combination, operation, or use of a Product with other products not provided by Bidder as a system, or the combination, operation or use of a Product with any product, data, apparatus, or business method that Bidder did not provide, or the distribution, operation or use of a Product for the benefit of a third party outside the Bank;

d)The Bidder shall also indemnify the Bank against all losses, damages, claims, counter claims, suits, penalties and costs which the Bank may face on account of –

- I. Bodily injury (including death) and damage to real property and tangible personal property caused by Bidder's negligence on the part of the Bidder's employees, agents or representatives.
- II. Any claim or proceeding brought by a third party against the Bank as a consequence of the above.
- III. Any claim made upon and any action taken against the Bank by any statutory authority or Court on account of the Bidder's failure to comply with any laws, orders and regulations applicable to the performance by Bidder of its obligations under this Agreement.

e)In the event of the Bidder not fulfilling its obligations under this Section within the period specified in the notice issued by the Bank, Bank has the right to recover the amounts due to it under this provision from any amount payable to the Bidder under the RFP and subsequent Agreement for AMC/Facility Management/ Support Services etc.

f). Additionally, the Vendor shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings,

a. that the Deliverables and Services delivered or provided under this RFP infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in any country where the Deliverables and Services are used, sold or received; and/or

b. resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements under any laws including the Copyright Act,1957 or Information Technology Act, 2000 in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Vendor in writing as soon as practicable when the Bank becomes aware of the claim however,

i. the Vendor has sole control of the defense and all related settlement negotiations.

ii. the Bank provide the Vendor with the assistance, information and authority reasonably necessary to perform the above and

iii. Vendor aware the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.

However indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

5. Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

6. The Vendor shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.

Bidder shall be liable for any breach or any non-performance by the Bidder of any of its undertakings, warranties, covenants, representations or obligations under this Agreement

3. Publicity

Any publicity by the Service Provider in which the name of the Bank is to be used, will be done only with the explicit written permission of the Bank.

4. Patents Rights:

4.1. The supplier shall indemnify the Bank against all Intellectual Property Rights including third party claims of infringement of patent, Copy Rights, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.

4.2. The supplier shall, at their own expense, defend and indemnify the Bank against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.

4.3. The supplier shall expeditiously extinguish any such claims and shall have full rights to defend it there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible for, including all expenses and court and legal fees.

4.4. The Bank will give notice to the Supplier of any such claim without delay, provide reasonable assistance to the Supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.

4.5. The Supplier shall grant to the bank a fully paid-up, irrevocable, non-exclusive license throughout the territory of India or abroad to access, replicate and use software (and other software items) provided by the supplier, including-all inventions, designs and marks embodied therein in perpetuity.

4.6- The Bank shall not be held liable for and is absolved of any responsibility or claim/Litigation or penal liability arising out of the use of any third party software or modules supplied or otherwise by the Vendor as part of this RFP.

5. Force Majeure:

1. For the purpose of this clause, “Force Majeure” shall mean an event beyond the control of the parties, due to or as a result of or caused by acts of God, wars, insurrections, riots, earthquake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.

- II. The Bidder or the Bank is not responsible for delays or non-performance of any contractual obligations arising out of blockade caused by war, revolutions, insurrection, civil commotion, riots, mobilizations, strikes, acts of God, plague or other epidemics, fire, flood, obstructions of navigation by ice of port of dispatch, acts of Govt. or public enemy or any other event beyond the control of either party which directly, materially and adversely affect the performance of any contractual obligation.
- III. If a force majeure situation arises, the bidder shall promptly notify the Bank in writing of such conditions and the change thereof immediately within five calendar days. Unless otherwise directed by the Bank, in writing, the bidder shall continue to perform his obligations under the contract and shall seek all reasonable alternative means for performance not prevented by the force majeure event.
- IV. The bidder or the bank shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the Service Provider or the bank, i.e. Force Majeure.
- V. In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of one month, the Bank and the Service Provider shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the Bank shall be final and binding on the Service Provider.

6. Limitation of Liability

The Vendors aggregate liability in connection with obligations undertaken as a part of the Project regardless of the form or nature of the action giving rise to such liability (in contract), shall be at actuals and limited to the contract value. The Vendors liability in case of claims against the Bank resulting from , misconduct or gross negligence of the Vendor, its employees and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited. The Bank shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third party software or modules supplied by the Vendor under this project and operated according to the Vendor's advice and same confirmed by Bank's officials. In no event shall either party be liable for any indirect, incidental damages, under or in connection with or arising out of this agreement.

7. Compliance with Laws

Compliance with all applicable laws: The Bidder shall observe, adhere to, abide by, comply with and notify the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this RFP and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees/officers/staff/ personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

Compliance in obtaining approvals/permissions/licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Bank and its employees/ officers/ staff/ personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and the Bank will give notice of any such claim or demand of liability within reasonable time to the Bidder.

All necessary compliances relating to the transaction such as disclosure in the returns to be filed, Tax Collected at Source(if applicable) etc. shall be duly undertaken by the supplier and in case of any non-compliance or delayed compliance, the Bank shall have right to recover interest and/or penalty that may be levied including liquidated damages @10 % of the value of supplier.

This indemnification is only a remedy for the Bank. The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

8. Corrupt and Fraudulent practice

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:

“Corrupt Practice” means the offering, giving, receiving or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution

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

The Bank reserves the right to reject a proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

9. Information ownership All information transmitted by successful Bidder belongs to the Bank. the Bidder does not acquire implicit access rights to the information or rights to redistribute the information unless and until written approval sought in this regard. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately, which is proved to have caused due to reasons solely attributable to bidder.

Any information considered sensitive by the bank must be protected by the successful Bidder from unauthorized disclosure, modification or access. The bank's decision will be final if any unauthorized disclosure have encountered.

Types of sensitive information that will be found on Bank system's which the Bidder plans to support or have access to include, but are not limited to Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

The successful Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any of the Bank location. The Bidder will have to also ensure that all sub-contractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.

10-Privacy and security safeguards

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

ii. The Vendor hereby agrees and confirms that they will disclose, forthwith, instances of security breaches.

iii. The Vendor hereby agrees that they will preserve the documents.

11-Sensitive Information:

Any information considered sensitive must be protected by bidder from unauthorized disclosure, modification or access. Types of sensitive information that will be found on Bank systems which the Service provider may support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc

12. Arbitration

10.1. All disputes and differences of any kind whatever arising out of or in connection with the purchase order shall be referred to arbitration. The arbitrator may be appointed by both the parties or in case of disagreement each party may appoint an arbitrator and such arbitrators shall appoint an Umpire before entering on the reference. The decision of the Umpire shall be final. Such arbitration to be governed by the provisions of Indian Arbitration and Conciliation Act 1996 or any statutory modifications or re-enactments thereof and the rules made there under and for the time being in force, shall apply to the arbitration proceedings. The arbitrator shall be appointed with the mutual consent of both the parties. Any appeal will be subject to the exclusive jurisdiction of the courts in Mumbai.

- 10.2. Notwithstanding anything contained herein above, in case of any dispute, claim and legal action arising out of this RFP, the parties shall be subject to the jurisdiction of courts at Mumbai, India only.
- 10.3. The vendor shall continue to work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or the umpire, as the case may be, is obtained.
- 10.4- The bidder acknowledges that if bidder fails to comply with any of its obligations hereunder, if Bank suffers any or all immediate, irreparable harm for which monetary damages may not be adequate. The bidder agrees that, in addition to all other remedies provided at law or in equity, the Bank shall be entitled to injunctive relief, restraining order, right of recovery, specific performance, or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the vendor from committing any violation or enforce the performance of the covenants, obligations and representation contained in the RFP/Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages..

13. Assignment

Bank may assign the Project and the solution and services provided therein by Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the facilities management services to any of the Contractor/sub-contractor, at its sole option, upon the occurrence of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with Bidder for any reason whatsoever; (iii) expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against Bidder. Bidder shall ensure that the said sub-contractors shall agree to provide such services to the Bank at no less favourable terms than that provided by Bidder and shall include appropriate wordings to this effect in the agreement entered into by Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of Bidder to perform or termination/expiry of the contract.

14-Independent Contractor:

Nothing herein contained will be construed to imply a joint venture, partnership, principal-agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified

that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/NDA(Non Disclosure Agreement) irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labour laws for its employees and sub-contractors or as the case may be. Bidder should take bank's prior written permission before subcontracting/ resource outsourcing of any work related to the performance of this RFP or as the case may be.

15-Statutory and Regulatory Requirements

The services must comply with all applicable requirements defined by any regulatory, statutory or legal body which shall include but not be limited to RBI or other Regulatory Authority, judicial courts in India and as of the date of execution of Agreement. This requirement shall supersede the responses provided by the Vendor in the technical response. During the period of Empanelment/Agreement, Bidder / Vendor should comply with all requirements including any or all reports without any additional cost, defined by any regulatory authority time to time and which fall under the scope of this RFP / Agreement. All mandatory requirements by regulatory / statutory bodies will be provided by the bidder under change management at no extra cost to the bank during the tenure of the contract.

16-FIXED PRICE AND TAXES

(A)The commercial offer shall be on a fixed price basis, exclusive of all taxes and levies. No price variation relating to increases in applicable taxes customs duty, excise tax, dollar price variation etc. will be permitted. The Bidder shall pay any other Tax being applicable after placement of order, during currency of the project only.

(B)Taxes:

1- The consolidated fees and charges required to be paid by the Bank against each of the specified components under this RFP shall be all-inclusive amount with currently (prevailing) applicable taxes. The service provider shall provide the details of the taxes applicable in the invoices raised on the Bank. Accordingly, the Bank shall deduct at source, all applicable taxes including TDS from the payments due/ payments to service provider. The applicable tax shall be paid by the service provider to the concerned authorities.

2- In case of any variation (upward or down ward) in Government levies / taxes / etc. up-to the date of providing services , the benefit or burden of the same shall be passed on or adjusted to the Bank. If the service provider makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines

and proceed accordingly.

3- Goods and Services Taxes(GST) and its Compliance

(i) Goods and Services Tax Law in India is a Comprehensive, multi-stage, destination-based tax that will be levied on every value addition. Vendor shall have to follow GST Law as per time being enforced along with certain mandatory feature mentioned hereunder-

(a) TDS (Tax Deducted on Source) is required to deduct as per applicable under GST Law on the payment made or credited to the supplier of taxable goods and services. It would enhance the tax base and would be compliance and self-maintaining tax law based on processes. The statutory compliances contained in the statutes include obtaining registration under the GST law by the existing assesses as well as new assesses, periodic payments of taxes and furnishing various statement return by all the registered taxable person.

(b) It is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit (ITR) to the Bank by way of commensurate reduction in the prices under the GST Law.

(c) If vendor as the case may be, is backlisted in the GST (Goods and Services Tax) portal or rating of a supplier falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract.

4- Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Service provider shall pay any other taxes separately or alongwith GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

17-Bank Property -

All data or information supplied by the Bank to the bidder in connection with the services being provided by bidder ('the software and Hardware if any ') shall remain the property of the Bank or its licensors. All deliverables/services to the extent prepared by bidder hereunder for delivery/services to the Bank ('the Deliverables') shall be the property of the bidder and the bidder shall grant to the Bank a worldwide, non-exclusive, fully paid, royalty-free license to use, display, execute, reproduce, and distribute copies of the Deliverables for its internal use only, to the extent necessary for the intended use of the Deliverables. Except as otherwise provided herein above, if the bidder discloses any data or information to any unauthorized party the bidder agrees to indemnify and hold harmless the Bank against all claims, causes of action, liabilities, losses, damages, costs, and resulting from such disclosure.

18-Survival and Severability: Any provision or covenant of the RFP/ subsequent Agreement, which expressly, or by its nature, imposes obligations on bidder shall so survive beyond the expiration, or termination of this Agreement. The invalidity of one or more provisions contained in this Agreement shall not affect the remaining portions of this Agreement or any part thereof; and in the event that one or more provisions shall be declared void or unenforceable by any court of competent jurisdiction, this Agreement shall be construed as if any such provision had not been inserted herein.

19-AMENDMENTS

Any change made in any clause of the contract which shall modify the purview of the contract within the validity and currency of the contract shall be deemed as an Amendment. Such an amendment can and will be made and be deemed legal only when the parties to the contract provide their written consent about the amendment, subsequent to which the amendment is duly signed by the parties and shall be construed as a part of the contract.

12. RFP Ownership:

The RFP and all supporting documentation are the sole property of Bank and should NOT be redistributed without prior written consent of Bank. Violation of this would be a breach of trust and may, inter-alia cause the bidders to be irrevocably disqualified. The aforementioned material must be returned to Bank when submitting the proposal, or upon request; however, bidders can retain one copy for reference.

13. Proposal Ownership:

The proposal and all supporting documentation submitted by the bidders shall become the property of Bank unless the Bank agrees to the bidders' specific requests, in writing, the proposal and documentation to be returned or destroyed.

14. Tender / RFP Cancellation:

The Bank reserves the right to cancel the Tender/RFP at any time without assigning any reasons whatsoever.

15. Other Terms and Conditions:

- 15.1. Empanelment does not confer any rights on the vendors to necessarily receive assignments/jobs.
- 15.2. Empanelment by the Bank does not constitute any right on the vendor to receive assignments / activities / work orders
- 15.3. This allocation of assignments/jobs will be at the sole discretion of the Bank. This would be subject to annual review.
- 15.4. Bank reserves the right to de-empanel any empanelled **ITCSSPs**.
- 15.5. All the details pertaining to this procurement will be displayed on our website after the placement of the purchase order on the selected Bidder.

15.6. Clarifications needed on any of the points mentioned in the RFP, if any, may be sought from the Bank as per the timelines specified in Bid details and after which no request will be entertained / replied.

16. Language and Currency of BIDs:

The bid shall be in English Language and all prices shall be expressed in Indian Rupees.

17. Penalty

All deliverables including reports need to be submitted within 15 days from the actual deliverable date / completion of the activity. Bank may impose penalty on concern Vendor for nonperformance of the contractual obligation in time schedule/ during currency of the contract. A penalty will be imposed on delay on account of the Consultant on submitting the necessary reports or non performance of the contractual obligation as per time schedule @ 2.5% of order value per month and part thereof subject to maximum 10% of order value.

Section VI: Annexure

Annexure-A: Acceptance of terms and conditions

(LETTER TO THE BANK ON THE BIDDER'S LETTERHEAD)

To,

The Asst. General Manager,
Central Bank of India,
DIT, 1st floor, Sec.11,
Plot No.26, Opp. Belapur Rly. Stn.,
CBD Belapur,
Navi Mumbai 400 614.

Sir / Madam,

Subject: RFP for Empanelment of IT and Cyber Security Service Provider for Bank

The details submitted in the format above are true and correct to the best of our knowledge and if it is proved otherwise at any stage of execution of the contract, Central bank of India has the right to summarily reject the proposal and disqualify us from the process.

We hereby acknowledge and confirm having accepted that bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP and related documents, in short listing of vendors for providing the services.

We also acknowledge the information that this response of our Company for the Banks' RFP process is valid for a period of 180 Days, for the selection purpose, from the date of expiry of the last date for submission for response to RFP and related enclosures.

We also confirm that we have noted the contents of the RFP including various documents forming part of it and have ensured that there is no deviation in submitting our offer in response to the tender. The Bank will have the option to disqualify us in case of any such deviations.

We also confirm that we will abide by the Terms & Conditions mentioned as given in the Tender Document in full and without any deviation.

Signatory

Authorised Signatory

Seal of company

Date

Place

Annexure – B (Technical Proposal)

Firm's Profile:

S. No.	Particulars		Response		
1	Name of the Firm/company/Individual				
2	Address				
3	Brief description of the nature of the business and profile of the company with particular reference to IT & CSSP				
4	Year of commencement of the kind of services (copy of commencement certificate may be enclosed) and number of years in this service industry.				
5	Turnover, Annual Income, Profit/Loss for the Year 1 three years in crores (enclose relevant copies of audited financial statements)	last	T.O.	AI	Profit
6	Total number of certified professional permanent staff (please submit the curriculum vitae (CV) for the professional staff like Name, Key qualification, designation, experience, their domain etc. separately)				
7	Team composition and task assignment for the proposed assignment.				
8	Description of the methodology and activity (work) schedule for performing the assignment				
9	Number of banks / Financial Institutions to which this kind of services are being given. *				
10	*Name and address of the banks / financial institutions to whom this kind of services was given with brief description, Location, etc.				
11	Number of other institution to which this kind of services were given. *				
12	*Name and address of other institutions to whom this kind of services was given with brief description.				
13	PAN Number				
14	GST Number				

***Note: The relevant support documents should be attached without which the offer is liable for rejection.**

SIGNATURE

Annexure-C: Eligibility criteria**(ELIGIBILITY COMPLIANCE)**

Sl. No.	Pre-Qualification	Compliance (Yes/No)	Supporting document Required
1.	The bidder should be a registered company /partnership firm / LLP in India and should be in existence for minimum of Five years as on the date of RFP		Attach Copy of Certificate of incorporation with full address of registered office and
2.	The bidder should be empanelled by CERT-IN.		Current Certificate by CERT-In
3.	The bidder should have minimum annual turnover of Rs.50 Crores during each of the last three financial years (i.e. 2014-2015, 2015-16 & 2016-17).		Please provide audited annual reports, Balance Sheet, Profit & Loss accounts for the same.
4.	The bidder should have net profit during the last three financial years (i.e. 2014-2015, 2015-16 & 2016-17).		Please provide audited Balance Sheet, Profit & Loss accounts for three Financial Years (i.e. 2014-2015, 2015-16 & 2016-17).
5.	The Bidder should have experience & expertise in handling Assignments / Services related to comprehensive security review of Data Centre/Enterprise Network, Active Directory, Application Security, Security review/ IS or IS-IT Audit (including Vulnerability Assessment and Penetration Testing (VAPT)) in India of BFSI Sectors during last three Financial years (i.e. 2014-2015, 2015-16 & 2016-17).		Attach copies of Purchase Order/reference, contract, installation certificate for software supplied and services provided.
6.	Bidder must have carried out Minimum Two Information Security and/or IS Audit related Assignments in BFSI during the last Financial year i.e. on or after 01.04.2017		Attach copies of Purchase Order/reference, contract.

7.	The Bidder should have experience in & expertise in handling Assignments / Services related to providing guidance in implementation of ISO 27001:2013 and/or ISO 22301:2012 in India in Minimum TWO BFSI during last three financial years (i.e. 2014-2015, 2015-16 & 2016-17)		Attach copies of PO/reference, contract/agreement / Work Order.
8.	The Bidder should have minimum three each of CISA, CISSP, ISO 27001 LA/LI, CEH certification holder as permanent employees in their organization. In addition to this, Bidder should also have minimum TEN staff with any of the following qualifications / Certifications. I. Certified PCI DSS professional II. CISM III. COBIT Certificate Holder IV. CCNA / CCNP V. CHFI VI. GIAC VII. CRISC VIII. SSCP IX. ECSA X. Offensive Security Certified Professional XI. ECIH XII. ISO 22301:2012 LA/LI		Provide exact number of certified officials and total no. of officials avoiding double count as per Annexure – C3
9.	The companies or firms, bidding for tender, should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs). The bidder shall give an undertaking (on their letter head) that they have not been black listed by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was black listed by any of the Govt. Authority or PSUs, the name of the company or organization must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered. Please refer Annexure-G		Undertaking as per Annexure - G

10.	The bidder should not be declared as NPA by any of the Banks in India.		The bidder shall give an undertaking to this effect (on their letter head).
-----	--	--	---

Signature

Authorised Signatory

Seal of company

Annexure C1- Statement of Bidder (For last 3 years from 01.04.2015)

(Scheduled Commercial Bank clients should appear at top, followed by BFSI (nonbanking), Govt.

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 at 1.1 service type, 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

Depts., etc)

- Assignments done during the financial years 01.04.2015 to 31.03.2018 shall only be mentioned.
- Supporting documents shall be Work Orders; letters from clients on their letter head, contacts of clients etc. shall be enclosed. Only such assignments should be described in above table which are directly related to Scope of Work of this RFP.
- Brochures / emails attached shall not be considered for evaluation.

Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the bidder. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted.

Signature

Seal of Company

Annexure C2 - Specific Work Experience of Vendor during past three years in BANKS

Activities (As per Annexure C4)	CBS	ATM	Internet Banking	Mobile Banking	Treasure operations/ SWIFT	Network/ Security	Various Certification	Outsourced Activities	Any Other

Mention only No. of assignments under the respective head.

Signature

Seal of Company

Annexure C3 List of Experienced Staff working in the Company

S.No.	Name of the Employee	Designation	Professionals / Technical / Qualifications / Certifications	Date of Joining	No. of Completed Years as on 31.03.2018	No. of IT/IS/CS Projects Handled	Activities [as per Annexure C4]

- a. Employee should be on permanent Pay Roll of the company.
- b. Ad-hoc / Temporary staff or other outsources / organisation should not be included.

Signature

Seal of Company

Annexure C4 Priority list of Services and Assignments by the ITCSSPs in BFSI Sector

S.No.	Services/Assignments	Capability (Yes//No)	If Yes, indicate priority of interest levels on scale of 1-4, where scale-1 is top priority	Total No. of Assignments
1.	Vulnerability Assessment [VA].			
2.	Penetration Testing [PT].			
3.	Secured Configuration, & Hardening Documents Review - [Technical Standards Updation].			
4.	Mobile Application Review and Security related Work.			
5.	Risk Assessment, Asset Classification, Review, Compliance of NDAs, SLA with Vendors / Third Party Outsourcing Agencies.			
6.	SMS and All Middleware Security Review and related work.			
7.	Network Security, Access Control, Review of NAP Locations, Switches and Routers and LAN - WAN NW.			
8.	General Controls Review / Audit Review and related Work.			
9.	Anti-Phishing, Anti-Malware and Brand Monitoring Services etc.			
10.	PCI DSS Certification and Compliance related Work.			
11.	COBIT – Advisory Services and related Work			
12.	ISO 22301 Certification, Automated Score ISMS Score Board and related Work.			
13.	ISO 27001 Certification and related Work.			
14.	ISO 27001 Audit and Compliance related Work.			
15.	Review, Update Gaps of IS Audit Policies, IS Audit Manual, and IS Audit Procedures, Metrics and related Work.			
16.	Review, Update Gaps of Information Security Policy, Procedures, Metrics, Controls			
17.	IS Audit - Internal Control Guidelines of Treasury Branch, Dealing Room Activities Review and related Work.			
18.	IS Audit of ATMs of Banks under Section PSS Act 2007 of RBI and related Work.			
19.	IS Audit of ATMs of Bank's Network, Gaps and related Work.			
20.	Concurrent Audit of Data Center			

21.	Forensic Audit / Analysis / Special Reviews / Scrutinize / Cyber Crime – Investigations and related Work.			
22.	Green Process Audit [GPA], Configuration Audit and related Work.			
23.	Project Management Office [PMO] – Security Solution Assessment, Identification, Requirements for Pre Implementation of IS Projects, Production Evolution for Monitoring of IS Projects and related Work.			
24.	Application [SW] Security Assessment / Review of Domain / Channel Process Audit including Associated Infrastructure [Including WEB]			
25.	Evaluation of New Technology/Products against Industry Best practices and Information Security Controls			
26.	Assess, Develop and Review Information Security Performance Dashboards focused on various measures such as effectiveness, ROI to convey value of investment on IS infrastructure across the Bank			
27.	Assess, Develop and Review Information Security Controls, Standards, Metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.			
28.	Threat Modeling for Software/App Development			
29.	Change Request Review (Monthly/Quarterly/Half-Yearly)			
30.	Application Code Audit - Review – Gap Analysis, Post Compliance Audit and related Work.			
31.	Data Governance, Data Protection Strategy Framework and Development related Work.			
32.	GAP Analysis of Requirements of Local Regulator/s of Foreign Centers including Threat and Vulnerability Risk Assessment [TVRA].			
33.	Conducting IS Audit of IT Infrastructure at DC / DR / NR Site / Treasury / RRBs / CBS / Service Branches – CTS etc. Quality Assurance, GAPs, Compliance Audit/s and related Work.			
34.	Quality Assurance, Conducting GAP Analysis, Compliance Audit/s of RBI / G. G. Committee Recommendations, IT Act 2008, Guidelines of other Foreign Regulators & GoI Guidelines etc. Automation of Compliance requirements and related Work.			
35.	Development and Implementation of IT Governance, Risk and Compliance [IT – GRC], most suitable IS Solutions and Tool/s and related Work.			
36.	Assisting in Selection of suitable tool, solution for ISC / ISAC related work.			

37.	Review of BCP/DR System, strategy and related Work.			
38.	Review, Development, Selection, Implementation of various Tools for Data Privacy, Data Protection Data Classification, Data Governance Strategy, and Framework of the Bank in pursuance of the various Regulatory and Government Guidelines in vogue from time to time.			
39.	Develop, Implement, Training IS Awareness, E-Learning Modules related to InfoSec related areas and Issues.			
40.	Review of Post - Implementation of various IS initiatives and Project/s			
41.	Assisting in Log Management – Revamping and up gradation of our SOC Operations, Monitoring, Assessment of SIEM Solution, Optimization technical process, correlation review for existing DLP, DAM, SIEM, IPS / IDS etc., Identify and assistance in implementation of recommend IS Tools such as IAM, IRM etc. and other related Work.			
42.	Any other relevant Assignment (Please mention)			

NOTE:

- In case of capability, experience and expertise vendors shall mention “YES” In case of “Capability” column kept blank, respective item no will be considered as NO.
- Kindly mention the No. of Assignments carried out in past three years (From 01.04.2013) against respective Sr. No.
- In case of ANY other related Activities NOT included in the above list, but related assignment/s carried out by the Bidder, may be added and included in the list after avoiding duplication along with the priority no. of such additional items.
- The information provided in the list must be supported by documentary evidence. Non submission or incomplete documentary evidence will be considered as Non-conformity for particular line item and it will not be considered. Bank’s decision in this regards will be final.
- In case the Bidder has carried out any other assignments over and above list they may add these assignments together with evidence and PRIORITY for that assignment. The Bidder should give and list out all their ISC and ISAC related Assignments and Services.

Signature

Seal of Company

Annexure – D (Reference Site Details)

We give below the reference site details. *

Name of the Bank / Financial Institution (Client Name)	
Address of the Bank / Financial Institution	
Brief description of the nature of business / process handled.	
Contact Details (At least two contacts details of senior staff of the client are to be provided for each reference).	Contact 1
Contact1	
Name:	
Designation:	
Landline No.:	
Mobile No.:	
E-mail id:	
Contact2	
Name:	
Designation:	
Landline No.:	
Mobile No.:	
E-mail id:	
Description of the services provided	
Duration of assignment including start date and end date.	
Approximate value of service	

Signature
Company Seal

*Note: One reference as per in scope activity whichever is carried out by bidder is to be provided in form of Annexure -D

Annexure - F Undertaking for providing Performance Bank guarantee

To

Central Bank of India
DIT, 1st floor, Sec.11,
Plot No.26, Opp.CBD Belapur Rly. Stn.,
CBD Belapur,
Navi Mumbai 400 614.

Dear Sir,

Sub: Undertaking for providing Performance Bank Guarantee—Request for Proposal (RFP) for empanelment of IT and Cyber Security Service Providers.

We undertake to provide the Bank with a suitable Bank Guarantee in the format prescribed by the Bank for maintaining the systems supplied, installed and maintained under the RFP for Request for Proposal (RFP) for empanelment of IT and Cyber Security Service Providers.

Yours faithfully,

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

Date:

Annexure –G (Undertaking)

Place:

Date:

To:

The Asst. General Manager
Central Bank of India
DIT, 1st floor, Sec.11,
Plot No.26, Opp. Belapur Rly. Stn.,
CBD Belapur,
Navi Mumbai 400 614.

Undertaking (To be submitted by all Bidders' on their letter head)

We _____ (bidder name), hereby undertake that-

- We have not been blacklisted by the Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response.
- We also undertake that, we were never involved in any legal case that may affect the solvency / existence of our firm or in any other way that may affect capability to provide / continue the services to bank.

Yours faithfully,

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

Date:

Annexure H: Performance Bank Guarantee

TO,
CENTRAL BANK OF INDIA
CHANDRAMUKHI BUILDING
NARIMAN POINT
MUMBAI

In consideration of M/s Central Bank of India having Registered Office at Chandermukhi Building, Nariman Point, Mumbai 400 021 (hereinafter referred to as "Bank") having agreed to purchase ----- (hereinafter referred to as "Goods") from M/s ----- (hereinafter referred to as "Vendor") on the terms and conditions contained in their agreement/purchase order No----- dt.----- (hereinafter referred to as the "Contract") subject to the Vendor furnishing a Bank Guarantee to the Bank as to the due performance of the-----, as per the terms and conditions duly stipulated in the aforesaid contract, to be supplied by the Vendor and also guaranteeing the maintenance, by the Vendor , ----- ----- --as per the terms and conditions of the said contract;

We, ----- (detail address of Guarantor Bank) (hereinafter called "Guarantor Bank"), in consideration of the premises and at the request of the Vendor, do hereby guarantee and undertake to pay to the Bank, forthwith and immediate on mere written demand and without any demur, at any time within the validity date up to ----- any money or moneys not exceeding a total sum of Rs----- (Rupees-----only) as may be claimed by the Bank to be due from the Vendor by way of loss or damage caused to or would be caused to or suffered by the Bank by reason of failure of Performance ----- as per the said contract, and also failure of the Vendor to maintain the ----- as per the terms and conditions of the said contract.

Notwithstanding anything to the contrary, the decision of the Bank as to whether Vendor has failed to perform as per the Terms and conditions of the said contract, and also as to whether the Vendor has failed to maintain the ----- as per the terms and conditions of the said contract will be final and binding on the Guarantor Bank and the Guarantor Bank shall not be entitled to ask the Bank to establish its claim or claims under this Guarantee but shall pay the Guarantee amount to the Bank forthwith on mere demand without any demur, reservation, recourse, contest or protest and/or without any reference to the Vendor. Any such demand made by the Bank on the Guarantor Bank shall be conclusive and binding notwithstanding :-

Any dispute that might have cropped up between the Bank and the vendor, or

Any dispute might have been pending , between the Bank and the vendor, before any court, Tribunal , Arbitrator or any other authority or

Any variation of the contract or any other act, omission or promise made by the Bank and agreed by the Bank and the Vendor, the effect of which, is the discharge of the Guarantor Bank.

This Guarantee shall expire on -----; without prejudice to the Bank's claim or claims demanded from or otherwise notified to the Guarantor Bank in writing on or before the said date i.e. ----- (this date should be date of expiry of Guarantee).

The Guarantor Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the Bank in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the Bank under or by virtue of the said contract have

been duly paid and its claims satisfied or discharged or the Bank certifies that the terms and conditions of the said contract have been fully carried out by the Vendor and accordingly discharges the Guarantee.

In order to give full effect to the Guarantee herein contained you shall be entitled to act as if we are your principal debtors in respect of all your claims against the Vendor hereby Guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

The Guarantor Bank agrees with the Bank that the Vendor shall have the fullest liberty without affecting in any manner the Guarantor Bank's obligations under this Guarantee to extend the time of performance by the contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the Bank against the Vendor and either to enforce or forbear to enforce any of the terms and conditions of the said contract, and the Guarantor Bank shall not be released from its liability for the reasons of any such extensions being granted to the Vendor for any forbearance, act or omission on the part of the Bank or any other indulgence shown by the Bank or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision have the effect of so relieving the Guarantor Bank.

The Guarantee shall not be affected by any change in the constitution of the Vendor or the Guarantor Bank nor shall it be affected by any change in the constitution of the Bank by any amalgamation or absorption or with the Vendor, Guarantor Bank or the Bank, but Guarantor Bank will ensure that this guarantee shall be available to and enforceable by the absorbing or amalgamated company or concern.

This guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by Guarantor Bank (whether singly or jointly with other banks) on behalf of the Vendor heretofore mentioned for the same contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing un-cancelled and we the Guarantor Bank further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by us on behalf of the Vendor heretofore mentioned for the same contract referred to heretofore and for the same purpose for which this guarantee is issued.

Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax or registered post to our local address as mentioned in this guarantee.

The expression "Bank", "Guarantor Bank" and "Vendor" hereinbefore used shall include their respective successors and assigns.

Notwithstanding anything contained herein:-

Our liability under this Bank Guarantee shall not exceed Rs.------(Rupees-----only);

This Bank Guarantee shall be valid up to -----; and

We are liable to pay the Guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before ----- (date of expiry of Guarantee).

The Guarantor Bank has power to issue this Guarantee under the statute/constitution and the undersigned has full power to sign this Guarantee on behalf of the Guarantor Bank.

Date this ----- day of ----- 2018 at Mumbai.

For and on behalf of ----- Guarantor Bank.

sd/- -----

Annexure –I Compliance to RFP terms & conditions

S.No	Clause Details	Vendor's compliance (Yes / No)
1	<u>Summarized scope of work</u>	
	Vendor's acceptance to all the points mentioned under the summarized scope of work	
2	Single Part Tender	
	Vendor's acceptance to the procedure and all terms and conditions mentioned under this clause	
3	Bid validity	
	Vendor's acceptance to keep the bid validity for 180 days from the last date of submission of bid documents	
4	Right to alter RFP	
	Vendor's acceptance for Bank's right to alter terms of RFP	
5	No Commitment to Accept Lowest or Any Tender	
	Vendor's acceptance to the Bank's right of no commitment to accept lowest or any Tender	
6	Locations to be covered	
	Vendor's acceptance to the locations that are proposed to be covered under this Tender	
7	Bid Security	
	Vendor's acceptance to all the terms and conditions mentioned under this clause and to submit bid security	
8	Support/Service Details	
	Vendor's acceptance for providing logistic and other support services as required by the Bank	
9	Audit for Security Services by third party or Bank	
	Vendor's acceptance to conduct network audit as specified	
10	Quality Requirement for equipment	
	Vendor's acceptance to meet the quality requirement of equipment as mentioned	
11	No Alternatives	
	Vendor's acceptance to the clause	

12	Project period	
	Vendor's acceptance to the clause	
13	Payment terms	
	Vendor's acceptance to all the payment terms of the Bank	
14	Technological Up gradation	
	Vendor's acceptance to Bank's Technological upgradation	
15	Scope of work	
	Vendor's acceptance to scope of work	
16	Order Cancellation	
	Vendor's acceptance for the clause	
17	Training	
	Vendor's acceptance for the clause	
18	Guarantees	
	Vendor's acceptance for the clause	
19	Resolution of Disputes/Arbitration	
	Vendor's acceptance for the clause	
	Disaster Recovery & Business Continuity	
20	Planning (BCP)	
21	Process	
	Vendor's acceptance to abide by all the terms and conditions as specified in RFP	

These are the mandatory conditions. Each bidder has to provide the compliance for the above.

Signature:

Name:

Date:

Seal of company:

Annexure – J: Pre Bid Query Format

S. No.	Section and Clause Reference No.	Page No.	RFP Text	Query	Response to query (to be left blank by the vendor)

Annexure – K (Know Your Employee)

(To be submitted by all bidders on their letter head)

To

The Asst. General Manager
Central Bank of India
DIT, 1st floor, Sec.11,
Plot No.26, Opp. Belapur Rly. Stn.,
CBD Belapur,
Navi Mumbai 400 614.

UNDERTAKING

1. We _____(name of the company) hereby confirm that all the resource (both on-site and off-site) deployed/to be deployed on Bank's project for _____ (Name of the RFP) have undergone KYE (Know Your Employee) process and requisite checks have been performed prior to employment of said employees as per our policy and Bank reserves the rights to ask for background check documents of resources.
2. We further undertake and agree to save defend and keep harmless and indemnified the Bank against all loss, cost, damages , claim penalties expenses, legal liability because of non compliance of KYE and of misconduct of the employee deployed by us to the Bank.

Signature of Competent Authority with company seal _____

Name of Competent Authority _____

Company / Organization _____

Designation within Company / Organization _____

Date _____

Name of Authorized Representative _____

Designation of Authorized Representative _____

Signature of Authorized Representative _____

Verified above signature

Signature of Competent Authority Date _____

Annexure - L: Format of BANK GUARANTEE FOR EMD

Date:

To
The General Manager,
Central Bank of India,
DIT, 1st floor, Sec.11,
Plot No.26, Opp. Belapur Rly. Stn.,
CBD Belapur,
Navi Mumbai 400 614.

Dear Sir/Madam,

In response to your invitation to respond RFP for empanelment of IT and Cyber Security Service Provider for Bank, M/s _____ having their registered office at _____ (hereinafter called the Bidder) wish to respond to the said Request for Proposal (RFP) and submit the proposal for the same. Whereas the Bidder has submitted the proposal in response to RFP, we, the _____ Bank having our head office _____ hereby irrevocably guarantee an amount of Rs./- (Rupees only) as Bid security as required to be submitted by the Consultant as a condition for participation in the said process of RFP.

The Bid security for which this guarantee is given is liable to be enforced/ invoked:

- 1) If the Bidder withdraws his proposal during the period of the proposal validity; or
- 2) If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the terms and conditions of the RFP or the terms and conditions mutually agreed subsequently.
- 3) If the Bidder, if selected for awarding the Contract, fails to renew this Bank Guarantee as decided by Central Bank of India. We undertake to pay immediately on demand to Central Bank of India, the said amount of Rs. (Rupees only) without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any demand made by Central Bank of India which shall be conclusive and binding on us irrespective of any dispute or difference raised by the Bidder.

Notwithstanding anything contained herein:

- 1) Our liability under this Bank guarantee shall not exceed Rs./- (Rupees only).
- 2) This Bank guarantee will be valid up to 180 days and
- 3) We are liable to pay the guaranteed amount or any part thereof under this Bank guarantee only upon service of a written claim or demand by you on or before _____. In witness whereof the Bank, through the authorized officer has sets its hand and stamp on this _____ day of the month of _____ 2018 at _____.

Signature

Name (In Block letters)

Designation (Staff Code No.).....

Official address:

(Bank's Common Seal)

Attorney as per power of Attorney No.:

Date:

WITNESS:

1..... (Signature with Name, Designation & Address)

2..... (Signature with Name, Designation & Address)

Annexure –M: Non-Disclosure Agreement

This Agreement made at, on this_ day of 2018, BETWEEN
_____, a Company
incorporated under the Companies Act, 1956 having its registered office at
_____ (hereinafter referred to as “-----” which expression
unless repugnant to the context or meaning thereof be deemed to include its successors and
assigns) of the ONE PART;

AND

CENTRAL BANK OF INDIA, a body corporate constituted under the Banking Companies
(Acquisition & Transfer of Undertakings) Act, 1970 and having its head Office at Central Office,
Chander Mukhi, Nariman Point, Mumbai – 400 021 (hereinafter referred to as “CBI” which
expression unless repugnant to the context or meaning thereof be deemed to include its
successors and assigns) of the OTHER PART

And CBI are hereinafter individually referred to as party and collectively referred to as “the
Parties”. Either of the parties which discloses or receives the confidential information is
respectively referred to herein as Disclosing Party and Receiving Party.

WHEREAS:

The Parties intend to engage in discussions and negotiations concerning the establishment of a
business relationship between them. In the course of such discussions and negotiations, it is
anticipated that both the parties may disclose or deliver to either of the Parties certain or some of
its trade secrets or confidential or proprietary information, for the purpose of enabling the other
party to evaluate the feasibility of such business relationship (hereinafter referred to as “the
Purpose”).

NOW, THEREFORE, THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED
BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. Confidential Information: “Confidential Information” means all information disclosed/
furnished by either of the parties to another Party in connection with the business transacted/to be
transacted between the Parties and/or in the course of discussions and negotiations between them
in connection with the Purpose. Confidential Information shall include customer data, any copy,
abstract, extract, sample, note or module thereof.

Either of the Parties may use the Confidential Information solely for and in connection with the
Purpose.

Notwithstanding the foregoing, “Confidential Information” shall not include any information
which the Receiving Party can show: (a) is now or subsequently becomes legally and publicly
available without breach of this Agreement by the Receiving Party, (b) was rightfully in the
possession of the Receiving Party without any obligation of confidentiality prior to receiving it
from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other
than the disclosing Party without any obligation of confidentiality, or (d) was developed by or for
the Receiving Party independently and without reference to any Confidential Information and
such independent development can be shown by documentary evidence.

1. Non-disclosure: The Receiving Party shall not commercially use or disclose any Confidential Information or any materials derived there from to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Receiving Party may disclose Confidential Information to consultants only if the consultant has executed a Non-disclosure Agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these. The Receiving Party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing Party's Confidential Information in violation of the terms of this Agreement. Further, any breach of non-disclosure obligations by such employees or consultants shall be deemed to be a breach of this Agreement by the Receiving Party and the Receiving Party shall be accordingly liable therefore.
2. Provided that the Receiving Party may disclose Confidential information to a court or governmental agency pursuant to an order of such court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.
3. Publications: Neither Party shall make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the other Party.
4. Term: This Agreement shall be effective from the date hereof and shall continue till establishment of business relationship between the Parties and execution of definitive agreements thereafter. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease any and all disclosures or uses of Confidential Information; and at the request of the Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

Notwithstanding anything to the contrary contained herein the confidential information shall continue to remain confidential until it reaches the public domain in the normal course.

5. Title and Proprietary Rights: Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain title and all intellectual property and proprietary rights in the Confidential Information. No license under any trademark, patent or copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface or otherwise interfere with any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall

not add or emboss its own or any other any mark, symbol or logo on such Confidential Information.

6. Return of Confidential Information: Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all copies, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.
7. Remedies: The Receiving Party acknowledges that if the Receiving Party fails to comply with any of its obligations hereunder, the Disclosing Party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The Receiving Party agrees that, in addition to all other remedies provided at law or in equity, the Disclosing Party shall be entitled to injunctive relief hereunder.
8. Entire Agreement, Amendment, and Assignment: This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.
9. Governing Law and Jurisdiction: The provisions of this Agreement shall be governed by the laws of India. The disputes, if any, arising out of this Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.
10. General: The Receiving Party shall not reverse-engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder. All Confidential Information is provided "as is". In no event shall the Disclosing Party be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by the parties constitutes any representation, warranty, assurance, guarantee or inducement by either party to the other with respect to the fitness of such Confidential Information for any particular purpose or infringement of trademarks, patents, copyrights or any right of third persons.
11. Indemnity: The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party etc., officers, employees, agents or consultants.

IN WITNESS WHEREOF, the Parties hereto have executed these presents the day, month and year first hereinabove written.

For and on behalf of

Name of Authorized signatory:

Designation:

For and on behalf of CENTRAL BANK OF INDIA

Name of Authorized signatory:

Designation:

INTEGRITY PACT

Between

Central Bank of India hereinafter referred to as “**The Principal**”,

And

..... hereinafter referred to as “**The Bidder/ Contractor**”

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for.....The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Principal

(1.) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

a. No employee of the Principal, personally or through family members, will in connection with the tender for , or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/ contractor(s)

(1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal’s employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the

“Guidelines on Indian Agents of Foreign Suppliers” shall be disclosed by the Bidder(s)/Contractor(s).Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the “Guidelines on Indian Agents of Foreign Suppliers” is placed at (page nos. 6-7

)

e. The Bidder(s)/ Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

(2) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3- Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the “Guidelines on Banning of business dealings”. Copy of the “Guidelines on Banning of business dealings” is placed at (page nos. 8-17).

Section 4 – Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Bank in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in “Guidelines on Banning of business dealings”.

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

- (1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.
- (2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.
- (3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

- (1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
- (2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman & Managing Director, CENTRAL BANK OF INDIA.
- (3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality.
- (4) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
- (5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
- (6) The Monitor will submit a written report to the Chairman & Managing Director, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the *Principal* and, should the occasion arise, submit proposals for correcting problematic situations.
- (7) If the Monitor has reported to the Chairman & Managing Director CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the Chairman & Managing Director CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to

proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(8) The word „**Monitor**“ would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Chairman & Managing Director of CENTRAL BANK OF INDIA.

Section 10 – Other provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. Mumbai.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.”

(For & On behalf of the Principal)

For & On behalf of the Principal
Bidder / Contractor

(Office Seal)

(Office Seal)

Place_____

Place_____

Date_____

Date_____

Witness1:

Name & Address

Witness 2:

Name & Address

Witness1:

Name & Address

Witness 2:

Name & Address

GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

1.0 There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with CENTRAL BANK OF INDIA shall apply for registration in the prescribed Application –Form.

1.1 Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by CENTRAL BANK OF INDIA.

1.2 Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e. Principal) before finalizing the order

2.0 DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA. IF ANY.

2.1 Tenderers of Foreign nationality shall furnish the following details in their offer:

2.1.1 The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Bank, it shall be confirmed whether it is real substantial Bank and details of the same shall be furnished.

2.1.2 The amount of commission/remuneration included in the quoted price(s) for such agents/representatives in India.

2.1.3 Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/representatives in India, may be paid by CENTRAL BANK OF INDIA in Indian Rupees only.

2.2 Tenderers of Indian Nationality shall furnish the following details in their offers:

2.2.1 The name and address of the foreign principals indicating their nationality as well as their status, i.e, whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.

2.2.2 The amount of commission/remuneration included in the price (s) quoted by the Tenderer for himself.

2.2.3 Confirmation of the foreign principals of the Tenderer that the commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by CENTRAL BANK OF INDIA in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items .

2.3 In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission /remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4 Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by CENTRAL BANK OF INDIA. Besides this there would be a penalty of banning business dealings with CENTRAL BANK OF INDIA or damage or payment of a named sum.

Guidelines on Banning of Business Dealing

SNo	CONTENTS	PAGE(S)
1.	INTRODCUTION	9
2.	SCOPE	9
3.	DEFINITIONS	10-11
4.	INITIATION OF BANNING / SUSPENSION	11
5.	SUSPENSION OF BUSINESS DEALING	11-12
6.	GROUND ON WHICH BANNING OF BUSINESS DELINGS CAN BE INITIATED	12-13
7.	BANNING OF BUSINESS DEALINGS	13-14
8.	REMOVAL FROM LIST OF APPROVED AGENCIES –SUPPLIERS/CONTRACTORS	15
9.	SHOW-CAUSE NOTICE	15
10.	APPEAL AGAINST THE COMPETENT AUTHORITY	15
11.	REVIEW OF THE DECEISION BY THE COMPETENT AUTHROTIY	16
12.	CIRCUALTION OF NAMES OF AGENCIES WITH WHOM BUSINESS DEALINGS HAVE BEEN BANNED	16

1. Introduction

1.1 Central Bank of India, being a Public Sector Enterprise and ‘State’, within the meaning of Article 12 of Constitution of India, has to ensure preservation of rights enshrined in Chapter III of the Constitution. CENTRAL BANK OF INDIA has also to safeguard its commercial interests. CENTRAL BANK OF INDIA deals with *Agencies*, who have a very high degree of integrity, commitments and sincerity towards the work undertaken. It is not in the interest of CENTRAL BANK OF INDIA to deal with Agencies who commit deception, fraud or other misconduct in the execution of contracts awarded / orders issued to them. In order to ensure compliance with the constitutional mandate, it is incumbent on CENTRAL BANK OF INDIA to observe principles of natural justice before banning the business dealings with any Agency.

1.2 Since banning of business dealings involves civil consequences for an Agency concerned, it is incumbent that adequate opportunity of hearing is provided and the explanation, if tendered, is considered before passing any order in this regard keeping in view the facts and circumstances of the case.

2. Scope

2.1 The General Conditions of Contract (GCC) of CENTRAL BANK OF INDIA generally provide that CENTRAL BANK OF INDIA reserves its rights to remove from list of approved suppliers / contractors or to ban business dealings if any Agency has been found to have committed misconduct and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated.

2.2 Similarly, in case of sale of material there is a clause to deal with the Agencies / customers / buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

2.3 However, absence of such a clause does not in any way restrict the right of Bank (CENTRAL BANK OF INDIA) to take action / decision under these guidelines in appropriate cases.

2.4 The procedure of (i) Removal of Agency from the List of approved suppliers / contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5 These guidelines apply to all the Units and subsidiaries of CENTRAL BANK OF INDIA.

2.6 It is clarified that these guidelines do not deal with the decision of the Management not to entertain any particular Agency due to its poor / inadequate performance or for any other reason.

2.7 The banning shall be with prospective effect, i.e., future business dealings.

3. Definitions

In these Guidelines, unless the context otherwise requires:

i) *'Party / Contractor / Supplier / Purchaser / Customer/Bidder/Tenderer'* shall mean and include a public limited Bank or a private limited Bank, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. *'Party / Contractor / Supplier / Purchaser / Customer/*

Bidder / Tenderer' in the context of these guidelines is indicated as *'Agency'*.

ii) *'Inter-connected Agency'* shall mean two or more companies having any of the following features:

a) If one is a subsidiary of the other.

b) If the Director(s), Partner(s), Manager(s) or Representative(s) are common;

c) If management is common;

d) If one owns or controls the other in any manner;

iii) *'Competent Authority'* and *'Appellate Authority'* shall mean the following:

a) For Bank (entire CENTRAL BANK OF INDIA) wide Banning Executive Director (GAD) shall be the „Competent Authority“ for the purpose of these guidelines. Chairman & Managing Director, CENTRAL BANK OF INDIA shall be the „Appellate Authority“ in respect of such cases except banning of business dealings with Foreign Suppliers of imported coal/coke.

b) For banning of business dealings with Foreign Suppliers of imported goods, CENTRAL BANK OF INDIA Executive Directors“ Committee (EDC) shall be the „Competent Authority“ . The Appeal against the Order passed by EDC, shall lie with Chairman & Managing Director, as First Appellate Authority.

c) In case the foreign supplier is not satisfied by the decision of the First Appellate Authority, it may approach CENTRAL BANK OF INDIA Board as Second Appellate Authority.

d) For Zonal Offices only

Any officer not below the rank of Deputy General Manager appointed or nominated by the Head of Zonal Office shall be the *'Competent Authority'* for the purpose of these guidelines. The Head of the concerned Zonal Office shall be the *'Appellate Authority'* in all such cases.

e) For Corporate Office only

For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Head of GAD shall be the

Competent Authority” and concerned Executive Director (GAD) shall be the “Appellate Authority”.

e) Chairman & Managing Director, CENTRAL BANK OF INDIA shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.

iv) '*Investigating Department*' shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.

v) '*List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers*' shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers, etc.

4. Initiation of Banning / Suspension

Action for banning / suspension business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of each Unit /Corporate Vigilance may also be competent to advise such action.

5. Suspension of Business Dealings

5.1 If the conduct of any Agency dealing with CENTRAL BANK OF INDIA is under investigation by any department (except Foreign Suppliers of imported goods), the Competent Authority may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the Competent Authority, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to the Investigating Department. The Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2 The order of suspension shall be communicated to all Departmental Heads within the Plants / Units. During the period of suspension, no business dealing may be held with the Agency.

5.3 As far as possible, the existing contract(s) with the Agency may continue unless the Competent Authority, having regard to the circumstances of the case, decides otherwise.

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of CENTRAL BANK OF INDIA, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to ED (GAD), CENTRAL BANK OF INDIA Corporate Office alongwith the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the Units and Subsidiaries of CENTRAL BANK OF INDIA to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the Units by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue.

5.5 For suspension of business dealings with Foreign Suppliers of imported goods, following shall be the procedure :-

i) Suspension of the foreign suppliers shall apply throughout the Bank including Subsidiaries.

ii) Based on the complaint forwarded by ED (GAD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, GAD to place it before Executive Directors Committee(EDC) with ED (GAD) as Convenor of the Committee. The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, GAD.

iii) If EDC opines that it is a fit case for suspension, EDC may pass necessary orders which shall be communicated to the foreign supplier by ED, GAD.

5.6 If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7 It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6. Ground on which Banning of Business Dealings can be initiated

6.1 If the security consideration, including questions of loyalty of the Agency to the State, so warrants;

6.2 If the Director / Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public sector enterprises or CENTRAL BANK OF INDIA, during the last five years;

6.3 If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of tenders, interpolations, etc;

6.4 If the Agency continuously refuses to return / refund the dues of CENTRAL BANK OF INDIA without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5 If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6 If business dealings with the Agency have been banned by the Govt. or any other public sector enterprise;

6.7 If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts and / or fudging /forging /tampering of documents;

6.8 If the Agency uses intimidation / threatening or brings undue outside pressure on the Bank (CENTRAL BANK OF INDIA) or its official in acceptance / performances of the job under the contract;

6.9 If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10 Wilful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-despatch inspection was carried out by Bank (CENTRAL BANK OF INDIA) or not;

6.11 Based on the findings of the investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Bank (CENTRAL BANK OF INDIA) or even otherwise;

6.12 Established litigant nature of the Agency to derive undue benefit;

6.13 Continued poor performance of the Agency in several contracts;

6.14 If the Agency misuses the premises or facilities of the Bank (CENTRAL BANK OF INDIA), forcefully occupies, tampers or damages the Bank's properties including land, water resources, forests / trees, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent Authority may decide to ban business dealing for any good and sufficient reason).

7 Banning of Business Dealings

7.1 A decision to ban business dealings with any Agency should apply throughout the Bank including Subsidiaries.

7.2 There will be a Standing Committee in each Zone to be appointed by Head of Zonal Office for processing the cases of "Banning of Business Dealings" except for banning of business dealings with foreign suppliers of goods. However, for procurement of items / award of contracts, to meet the requirement of Corporate Office only, the committee shall be consisting of General Manager / Dy. General Manager each from Operations, Law & GAD. Member from GAD shall be the convener of the committee. The functions of the committee shall, inter-alia include:

- i) To study the report of the Investigating Agency and decide if a prima-facie case for Bank-wide / Local unit wise banning exists, if not, send back the case to the Competent Authority.
- ii) To recommend for issue of show-cause notice to the Agency by the concerned department.
- iii) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.
- iv) To submit final recommendation to the Competent Authority for banning or otherwise.

7.3 If Bank wide banning is contemplated by the banning Committee of any Zone, the proposal should be sent by the committee to ED (GAD) through the Head of the Zonal Office setting out the facts of the case and the justification of the action proposed along with all the relevant papers and documents. GAD shall get feedback about that agency from all other Zones and based on this feedback, a prima-facie decision for banning / or otherwise shall be taken by the Competent Authority. At this stage if it is felt by the Competent Authority that there is no sufficient ground for Bank wide banning, then the case shall be sent back to the Head of Zonal Office for further action at the Zone level. If the prima-facie decision for Bank-wide banning has been taken, ED (GAD) shall issue a show-cause notice to the agency conveying why it should not be banned throughout CENTRAL BANK OF INDIA.

After considering the reply of the Agency and other circumstances and facts of the case, ED (GAD) will submit the case to the Competent Authority to take a final decision for Bank-wide banning or otherwise.

7.4 If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show-cause notice may be issued to the Agency as per paragraph 9.1 and an enquiry held accordingly.

7.5 Procedure for Banning of Business Dealings with Foreign Suppliers of imported goods.

- ☐ Banning of the agencies shall apply throughout the Bank including Subsidiaries.
- ☐ Based on the complaint forwarded by ED (GAD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, GAD to place it before Executive Directors" Committee (EDC) with ED (GAD) as Convenor of the Committee.
- ☐ The committee shall expeditiously examine the report , give its comments/recommendations within twenty one days of receipt of the reference by ED, GAD.
- ☐ If EDC opines that it is a fit case for initiating banning action, it will direct ED (GAD) to issue show-cause notice to the agency for replying within a reasonable period.
- ☐ On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by ED (GAD) to EDC for consideration & decision.
- ☐ The decision of the EDC shall be communicated to the agency by ED (GAD).

8 Removal from List of Approved Agencies - Suppliers / Contractors, etc.

8.1 If the Competent Authority decides that the charge against the Agency is of a minor nature, it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2 The effect of such an order would be that the Agency would not be disqualified from competing in Open Tender Enquiries but Limited Tender Enquiry (LTE) may not be given to the Agency concerned.

8.3 Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9 Show-cause Notice

9.1 In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or misbehaviour may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defence.

9.2 If the Agency requests for inspection of any relevant document in possession of CENTRAL BANK OF INDIA, necessary facility for inspection of documents may be provided.

9.3 The Competent Authority may consider and pass an appropriate speaking order:

- a) For exonerating the Agency if the charges are not established;
- b) For removing the Agency from the list of approved Suppliers / Contractors, etc.
- c) For banning the business dealing with the Agency.

9.4 If it decides to ban business dealings, the period for which the ban would be operative may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10 Appeal against the Decision of the Competent Authority

10.1 The Agency may file an appeal against the order of the Competent Authority banning business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2 Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11 Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Competent Authority upon disclosure of new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee/EDC as the case may be for examination and recommendation.

12 Circulation of the names of Agencies with whom Business Dealings have been banned

12.1 Depending upon the gravity of misconduct established, the Competent Authority of the Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public Sector Enterprises, etc. for such action as they deem appropriate.

12.2 If Government Departments or a Public Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3 If business dealings with any Agency has been banned by the Central or State Government or any other Public Sector Enterprise, CENTRAL BANK OF INDIA may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its inter-connected Agencies.

12.4 Based on the above, Zonal Offices may formulate their own procedure for implementation of the Guidelines and same be made a part of the tender documents.