यूको बैंक UCO BANK

UCO BANK
Honours your Trust

Head Office
Audit & Inspection Department
1st Floor, 10. B. T. M. Sarani,
Kolkata – 700 001

REQUEST FOR PROPOSAL (RFP)
FOR
Selection & Empanelment of
INFORMATION SYSTEMS AUDITOR

RFP REF NO. : UCO/INSP/ISSA/2018/1
Date : 23/03/2018

Cost of the RFP document:-Rs 5000/- (Rupees Five Thousands only)

Disclaimer

While the document has been prepared in good faith, no representation or warranty , express or implied, is or will be made, and no responsibility or liability will be accepted by UCO Bank or any of its employees, in relation to the accuracy or completeness of this document and any liability thereof expressly disclaimed. The RFP is not an offer by UCO Bank, but an invitation for bidder's responses. No contractual obligation on behalf of UCO Bank, whatsoever, shall arise from the offer process unless and until a formal contract is signed and executed by duly authorized officials of UCO Bank and the selected Bidder.

IN D E X

Table of Contents

Note: - UCO Bank reserves the right to change the contents/dates mentioned in the RFP. Changes if any, related to RFP will be communicated to the bidders or posted on Bank's web site. Vendors must check the website for updated information.

SECTION-I

INTRODUCTION TO PROJECT

UCO Bank, a public sector bank having its Head Office at Kolkata has implemented many key technology solutions like Core Banking (CBS), Internet Banking (e-banking), Mobile Banking, ATMs, Integrated Treasury System, RTGS, SFMS, NEFT, Security Operating Centre etc. The bank is using Finacle Software of M/s. Infosys Technologies Ltd. as the Core Banking Solution for both Domestic and International operation. Bank has got Primary Site at one location and Disaster Recovery Site at another location. It has also got CTS locations at three different locations for three different grids. Bank's Treasury and Payment Gateway site is located at its Treasury Branch at one location and Disaster Recovery site at another location. The ATM switch Centre of our bank, is hosted by a vendor is located at one location with DR site at another location. (Location details of DC-DR sites will be communicated to bidders who qualify the eligibility criteria)

The Bank intends to appoint Cert-In empanelled Information Systems Security Auditor to conduct Information Systems Security Audit.

To conduct IS audit at Bank's Data Center, Disaster Recovery Site, Integrated Treasury branch, Treasury DR Site, ATM Switch/Centre etc., providing independent reasonable assurance to the Bank on:

- Robust IT security.
- Mitigation of risks where there are significant control weaknesses.
- Safeguarding the information assets viz. hardware, network etc.
- Maintaining security, confidentiality, integrity and availability of data.
- Efficient utilization of IT resources.
- Ensuring compliance of IT Security Policy/IS Audit Policy and procedures defined by the Bank.
- Providing minimum domain wise baseline security standard / practices in a checklist format to be implemented to achieve a reasonably secure IT environment for technologies deployed at UCO Bank separately for Servers, Database Management System (**DBMS**), network equipments, security equipments etc.

1.1 BID CONTROL SHEET

CALENDAR OF EVENTS		
1	Tender Reference	**UCO/INSP/ISSA/2018/1 dated 23/03/2018**
2	Cost of Tender Document	**Rs 5,000/-** in the form of Demand Draft/Pay order in favour of **UCO BANK** payable at Kolkata. The DD/PO should be submitted along with the Technical Bid.
3	Date of commencement of RFP Process/ issue of Bidding Document	**23.03.2018**
4	Earnest Money Deposit (EMD)	**Rs 1,00,000/- (One Lacs Only) /-** Rs. 1,00,000/- in form of Bank Guarantee (**Annexure-13**)
5	Last date of Queries, if any, to be communicated by the bidders	**02.04.2018**
6	Date of Pre-Bid Meeting	**08.04.2018**
7.	Last date, time & Venue for submission of Bid Documents	Date**:** **23.04.2018** Time: **4. P.M.** **Tender Box placed at Venue**: UCO BANK Audit & Inspection Department Head Office, 1st Floor 10 B. T. M. Sarani Kolkata : 700001
8.	Date and Time for Opening Technical Bid	**Technical Bid-Opening** Date: **23.04.2018** Time: **4.30. P.M.** Venue: UCO BANK Audit & Inspection Department Head Office, 1st Floor 10 B. T. M. Sarani Kolkata : 700001
9	Opening of Commercial Bid	**Commercial Bid-Opening** **Date & time will be communicated to the Technically qualified bidders** **Venue**: UCO BANK Audit & Inspection Department Head Office, 1st Floor 10 B. T. M. Sarani Kolkata : 700001
10	Place of opening of Bids	UCO BANK Audit & Inspection Department Head Office, 1st Floor 10 B. T. M. Sarani Kolkata : 700001
11	Address for communication	UCO BANK Audit & Inspection Department Head Office, 1st Floor 10 B. T. M. Sarani Kolkata : 700001
12	Contact Person	Ajay Kumar, Chief Manager Audit & Inspection, Head Office (Contact Nos. 033-4455 7873)

ELIGIBILITY CRITERIA

The eligibility criteria (**Annexure-1**) to participate in bidding process are mentioned below. Only those bidders, who satisfy all the eligibility criteria as mentioned herein below, may respond. Document in support of all eligibility criteria are required to be submitted along with the Technical Bid. The General Bidder Details must be submitted in **Annexure-2** format.

1.1.1 The IS Audit firm/company should be in the business of Information System auditing (IS Auditing) in India at least for last three years as on 31.03.2017 (in case of mergers/acquisition/restructuring or name change, the date of establishment of the earlier/original Partnership Firm/Limited Company can be taken in to account).

1.1.2 The Bidder must be a profit making firm/company in any two of the last three years (supporting documents for the year 2014-15, 2015-16, 2016-17 to be submitted).

1.1.3 The Bidder must have a turnover of at least **Rs. 2 crore** in the last three financial years (2014-15, 2015-16, 2016-17).

1.1.4 The Bidder must be having on their rolls, on permanent employment basis, **a minimum of 10 (ten nos.)** professionals who hold professional certifications like CISA/DISA/CISSP/CISM/ISO 27001 with requisite experience to handle the work as per the Scope (valid as on date). The profile of the Core Audit team must be submitted in **Annexure 7** format.

1.1.5 The bidder should have Banks/ Financial Institutions as their clients for IS Audit. The bidder must have completed comprehensive System Audit, in last two financial years, for at least One (01) Public Sector Bank in India. (Documentary proofs must be provided as per format given in **Annexure-3** along with copies of Work Order etc.).

1.1.6 Bidder should submit an Undertaking regarding compliance of all Laws, Rules, Regulations, Bye-Laws, Guidelines, Notifications etc as per **Annexure-4.** Bidder shall also submit an undertaking in letter head in the format of **Annexure 5** for undertaking IS Audit Assignment.

1.1.7 Bidder is required to execute the Pre Contract Integrity Pact as per **Annexure-6**

1.1.8 To ensure audit independence, the bidder should not have been a vendor/Consultant of IT equipment/peripherals/software/Services to UCO Bank in the past 3 years.

1.1.9 The bidder must not have been blacklisted by any Public Sector Bank/ICAI. A declaration to this effect must be submitted by the bidder.

1.1.10 The Bidder should be an empanelled Security Auditing Firm with CERT-In as on RFP publication date and also during the course of Audit.

1.1.11 The Bidder must be an Indian firms **or Company** to be eligible to participate in the tendering process.

Note: Documentary evidence must be submitted for all the above criteria.

SECTION-II

2.1 SCOPE OF AUDIT WORK

Bank has a board approved IS Audit Policy which need to be adhered to while conducting the audit. A comprehensive Information Systems Audit has to be undertaken covering the various key Areas:

- Preparation of **IS Audit Plan** in Consultation with bank.
- Defining **Checklist for different applications/area** of audit in Consultation with bank.
- Preparing **IS Audit Checklist for branches** as per regulatory guidelines in consultation with the bank.
- Audit of all **Outsourced activities/services**.
- IT Act 2000-08 Compliance
- Registration Authority for Digital Signatures.
- Disaster Recovery & Business Continuity Plans
- Capacity Planning of IT Infrastructure of Critical Applications
- Audit of patch Management System for various applications
- Service Level Management
- **Cyber Security Framework as per Cyber Security Policy of the bank**

2.1.1 Audit Units/Areas

The Applications/Infrastructure and site audit under the IT Universe of the bank shall include the following Audit Units. Process Audit shall also cover the following units:-

i. Anti-Money Laundering (AML) – Domestic
ii. Anti-Money Laundering (AML) - Overseas
iii. Lending Automation Processing System (LAPS)
iv. Network Management Infrastructure
v. Alternate Delivery Channels including
   - E Banking
   - Mobile Banking Application with embedded **Bharat QR code (Standard)**
   - UCO Wallet with embedded QR Code (UCO bank specific)
   - UCO Smart Pay
   - UCO Rewardz
   - BHIM Aadhaar Pay
   - BHIM UCO UPI with embedded **Bharat QR code (Standard)** as well as **QR code** (UCO bank specific)
   - m-passbook
   - UCO Pay Plus
   - UCO Secure Applications
   - Debit Card
   - Prepaid Card
   - PoS machine
   - Automatic Teller Machine (ATM) installed at different locations in Metros, Urban and Rural areas (5 ATM in each location)
   - Bharat Bill Payment System (BBPS) by M/s Integra
   - On-Line account opening System
   - PFMS (Public Financial Management System) by M/s Mine Gate

vi. UCO Bill Pay (for **Rajasthan Beverages accessible from branches and interfaced with Customer's Database Server**)
vii. Email/Mail Messaging System
viii. RTGS/NEFT Infrastructure
ix. Core Banking System (CBS) including Connect 24 Interface and Central Stand in Application Server(CSIS) - Domestic Application

x. Core Banking System (CBS) including Connect 24 Interface and Central Stand in Application Server(CSIS)- Overseas Application
xi. Risk Based Internal Audit (RBIA)
xii. MIS & Automated Data Flow (ADF) Audit
xiii. Government Business Module (GBM) (DC & DR)
xiv. Central Plan Scheme Monitoring System (CPSMS)
xv. Integrated Treasury Management System (ITMS)
xvi. Cheque Truncation System (CTS) (Northern & Southern Grids)
xvii. Security Operating Centre (SOC) – (includes modules viz. WAF, PIMS, DAM, APT, NBA etc.) with ARC Sight as a single Window incident management, ticketing and reporting System. **The audit should include Review of rules of SoC Devices including Arc Sight**.
xviii. SWIFT Infrastructure
xix. Mobile Banking Switch Audit (hosted by M/s. Lcode Limited)
xx. Unified Payment Interface (UPI), Mobile Banking Application & m-passbook
xxi. Registration Authority (RA) Office Setup under IDRBT Set-up
xxii. Prepaid card by M/s Yellumchili
xxiii. MPLS Network Architecture, Management & Audit
xxiv. Micro ATM
xxv. Servers/public facing routers/firewalls
xxvi. Document Management System (DMS)
xxvii. Active Directory
xxviii. Proxy Application Server
xxix. Near DR Site
xxx. E-Surveillance Infrastructure
xxxi. Review of interface with approx 10 Payment Gateways used by the Bank viz. ATM, Mobile Banking, Internet Banking, Bill Desk, Citrus etc.
xxxii. ATM Reconciliation Audit, CBO Mumbai
xxxiii. SMS System Audit
xxxiv. Biometric Infrastructure incld. for Finacle Login, Attendance System, e-KYC.
xxxv. Anti Virus
xxxvi. **Cyber Security Framework Audit**

Note:-

1. For the above, the Infrastructure at both DC & DR is to be covered under the Scope
2. For all Critical Processes where there is no Straight Through Processes (STP) are to be reviewed

2.1.2 Out Sourced Infrastructure Facilities

The Outsourced Infrastructure facilities shall include the following:-

i. ATM Switch Audit (hosted by M/s Euronet Limited)
ii. Data Centre Hosted by Tata Communications
iii. Near DR Site
iv. Cheque Truncation System (CTS) (Western Grids).
v. Prepaid Card Facility by M/s Yellamchili
vi. PoS Infrastructure Facility
vii. Security Operating Centre

2.1.3 In House Applications (Source Code Audit)

The in-house developed Software Packages includes the following:

- Aadhaar Pay Reconciliation
- Auto SWIFT Messaging

- Branch Visit Report (BVR)
- CMR13
- Credit Rating
- Customer Meet Module
- Empanelment of Concurrent Auditor
- Electronic Voucher Checking System (EVCS)
- GAD – Lease
- GAD – Bill Tracking
- HRMS Mobile App
- Human Resource Management System (HRMS)
- Iran Vostro Management System (IVMS)
- IT Procurement Management System
- Geevan Pramaan in GBM
- MIS DashBoard Mobile App
- MIS Portal
- Net Assist
- Recruitment Package
- UCO OnLine (ucoonline.co.in/ucoonline.in)

2.1.4 Vulnerability/Threat Assessment

The Vulnerability/Threat Assessment – Penetration Testing (**VA-PT**) for key IT infrastructure components shall cover a minimum of 350-375 devices on quarterly basis. A list of Servers/devices in different locations will be given to the selected vendor.

Scope of Vulnerability / Threat Assessment shall include, but not be limited to:

- Vulnerability assessment of all servers, ATM Switch, network equipments, security equipments installed
- Placement/ Deployment of security equipments, network equipments for securing database, application, web servers of various applications.
- Configurations and Monitoring of logs of Intrusion Detection/Prevention Systems, firewalls and response capabilities. Exercise will be carried out from the place where servers are placed. The same will also be carried out from a selected branch outlet for selected sample critical application/servers. Appropriate updated tools should be used for each phase of test

2.1.5 Penetration Testing

Penetration Testing shall include the following websites/URLs

- Bank's Websites viz.
  - www.ucobank.com,
  - www.ucobank.co.in,
  - www.ucobank.com.sg,
  - www.ucobankhongkong.com
  - http://www.ucombanking.com/ucomb/index.jsp
- E-Banking website (www.ucoebanking.com)
- Mobile Banking Application & Portal
- Bharat Bill Payment System
- HRMS application & portal

- Mail messaging system
- Aggregation Point (AP)/Base Stations.
- UCO ONLINE portals (ucoonline.co.in
- Public facing Routers & Firewalls

The final list of Public facing routers/URLs/IPs for Penetration Testing will be provided to the selected bidders. The Approximate Number of websites/URLs for Penetration Testing is 25-30.

Scope of External Penetration Testing should be designed to simulate a real world attack keeping in view prevailing RBI guidelines, IT acts 2000 & 2008 and other applicable regulations in India and shall at the minimum cover the following:--

- Port Scanning
- System Fingerprinting
- Services Fingerprinting
- Vulnerability Scanning
- Firewall & Access Control List Mapping
- Attempt to guess passwords using password-cracking tools.
- Session Hijacking
- Buffer Overflow
- SQL Injection
- Command Injection
- Cross Site Scripting
- Malicious Input Checks
- Checking Vulnerabilities for defacement and unauthorized modification of corporate websites.
- Search for back door traps in the programs.
- Attempt to overload the system using DDoS (Distributed Denial of Service) e.g. Botnet and DoS (Denial of Service) attacks.
- Check if commonly known bugs in the software, especially the browser and the email software exist.

Note: Any new addition/up-gradation in sites, hardware, software, new deliverables, change in architecture or due to regulatory requirement, during the contract period will also be covered in the scope of this audit without any additional cost to the bank.

2.2 CONTROLS TO BE COVERED UNDER AUDIT AREAS/UNITS

2.2.1 Site Audit for Various IT Infrastructure/Facilities

The Data Centre facilities Audit at the above mentioned sites shall cover following aspects:-

- Building Management Systems
- Power Supply, UPS & DG
- Physical Access Controls
- Environment Control
- Data centre infrastructure - network cabling, raceways, server/ Communication racks, Rack Power Distribution Units (PDU), KVM
- Fire & Smoke, Water leak Detection and suppression Systems

- Air-conditioning :-Temperature & Humidity control systems
- Assets safeguarding, Handling of movement of Man /Material/Media/ Backup / Software/ Hardware / Information.
- Surveillance systems.
- Pest prevention (rodent prevention) systems.
- Lightning Protection
- Training, Documentation, monitoring, duty list, storage management
- Asset Register, asset tracking, asset management

2.2.2 Operating System Audit

The Operating System audit shall cover following aspects for Servers, Databases, network equipments, Security Systems, Storage Area Networks.

- Set up and maintenance of system parameters
- Patch Management
- Change Management Procedures
- Logical Access Controls
- User Management & Security
- OS Hardening
- Performance, Scalability and Availability

2.2.3 Application Audit (Controls)

The Application audit shall cover following aspects:-

- Functionality implemented vis-à-vis the Bank's requirements.
- Input, processing and output controls across various schemes across the bank.
- Controls for performing/changing parameter setup of functionality across applications.
- Segregation of duties.
- Accuracy, adequacy and integrity of data in reports and MIS.
- Availability of necessary audit logs and its accuracy and effectiveness.
- Adherence of reporting to legal and statutory requirements.
- Automated batch processing, scheduled tasks, critical calculations etc.
- End of Day, Start of Day, period closure operations including End of Month, End of Quarter and End of Year operations.
- Integration with Delivery Channels including data and transaction integrity for the same
- Release of software governed by formal procedures-ensuring sign-off through testing, handover, etc.
- Formal procedure for change management being adopted.
- Impact analysis of changes made.
- Associated documents and procedures being/to be updated accordingly.
- Maintenance personnel have specific assignments and that their work is properly monitored. Their system access rights are controlled to avoid risks of unauthorized access to automated systems.
- Access log is monitored.
- Regular updation of job cards with new version releases.
- If outsourced, escrow arrangement with application vendors.

- Tracing of all High value transactions
- Verification of number of Branch Head (BH) and Asstt. Branch Head (ABH) for branches.
- Interfacing between Finacle &various Forex/ Treasury Applications.
- Controls for opening/modifications of Office Accounts /GL heads.
- Customization Source code review of all the important applications.

2.2.4 Database Audit

The Database audit shall cover following aspects:--

- Authorization, authentication and access control review.
- Audit of data integrity controls.
- Database Backup Management.
- Review of database privileges assigned to DBAs/Users.
- Security of Oracle systems files.
- Synchronization between DC & DR Databases for CBS/Alternate Delivery channels(ADC), between Treasury Primary Database & Treasury DR Database and between MISADF Database & MISADF DR Database etc..
- Patch Management.
- Review of control procedures for changes to parameter files.
- Review of Control procedures for sensitive DB passwords.
- Review of Control procedures for purging of Data Files.
- Review of Procedures for data backup, restoration, recovery and readability of backed up data.
- Maintenance/Monitoring/Review of Audit log and Archiving

2.2.5 Network Audit

The Network audit shall cover following aspects:--

- Overall Network management.
- Review of detailed Network architecture
- Network traffic analysis and base lining
- Virtual LANS (VLANs) & Routing.
- Evaluate procedures adopted for:
    i. Secured transmission of data through leased line/ISDN/VPN/VSATs/ MPLS, Wireless etc.
    ii. Bandwidth management
    iii. Uptime of network -- its monitoring as per SLA.
    iv. Fault management
    v. Capacity planning
    vi. Performance management.
    vii. Monitoring of logs.
- Verification of Network Devices for any security threats
- Configuration Checking vis-à-vis load and Access control audit for all the Networking Devices viz. Routers, Switches, IDS/IPS, Firewalls, Servers etc.
- Access list in networking devices for securing data transmission.
- Structured LAN cabling in DC and DR.
- Carry out "war driving" (or equivalent exercise) to identify rogue access points and mis-configured access points.
- Integration of various extranet with Bank's network.

2.2.6 Security Management Review

The **Security Management Review** shall cover following aspects:--

- Security Equipment Configurations & Policies.
- Penetration testing and Vulnerability Assessment (PT/VA) of various security zones/Networks/Delivery channels.
- Maintenance of necessary logs **including those of SOC Modules**

2.2.7 Delivery Channels Review/Audit

ATM Centre/Switch Audit shall cover following aspects:--

- ATM centre management :
    1. PIN Management
    2. Card Management
    3. Time Management in delivering ATM Card/PIN to Customers.
    4. Hot listing of cards.
- ATM helpdesk and monitoring.
- Branch procedures.
- Reconciliation:-Visa, Rupay, POS, NFS, Us-on-Us Chargeback procedures. (at ATM Transaction Banking Division, CBO Mumbai).
- Card Printing/Dispatch.
- ATM Switch setup, configuration, Security, control & Risk Management.
- ATM Switch operational controls, Consortium issues & Reconciliation/ Functional Managerial activities.
- Monitoring procedure of ATM's Status (Uptime/downtime).
- Processing of requests received through Debit Card Request (DCR) module in Finacle.
- Review of EWDIT Software of Euronet.
- Interface systems (Connect 24, Verified by Visa, Rupay etc.).
- Offsite Security Services.
- Status of required certifications as per International as well as regulatory stipulations.

2.2.8 Security System for Online Card Transaction (SSOCT) Audit

The SSOCT shall cover following aspects

- Detailed review of the SSOCT security architecture vis-à-vis the RBI, VISA/MASTER/Rupay card guidelines.
- Bank's SSOCT product line, transaction flow.
- Review on internal controls in place to minimize errors & frauds.
- Interface with ATM Switch & other applications.
- Process of creation/Activation/Resetting/delivery of PIN.
- Authentication controls.
- Compliance with industry standards of security such as, Payment Card Industry Data Security Standard (PCIDSS) etc.

2.2.9 E-Banking Audit

E-Banking Audit shall cover following aspects:--

- Detailed review of the Internet Banking security architecture vis-à-vis the

- RBI guidelines.
- Bank's internet Banking product line, transaction flow.
- Review on internal controls in place to minimize errors & frauds.
- Interface with other organizations for utility bill payments/share Trading
- etc.
- Interface with CBS & other applications.
- Process of creation/Activation/Resetting/delivery of internet banking
- User ids/ passwords.
- Password/PIN management.
- Authentication controls.
- Two Factor Authentication Solutions for E-Banking.
- Vulnerability/ Threat Assessment

2.2.10 Mobile Banking Audit

Mobile Banking Audit shall cover following aspects

- Detailed review of the Mobile Banking Security architecture vis-à-vis the RBI guidelines.
- Bank's Mobile banking product line, transaction flow.
- Review on internal controls in place to minimize errors & frauds.
- Interface with other organizations for utility bill payments & other purposes etc.
- Interface with CBS, Financial Transaction Switch & other applications.
- Parameterization & customization of Mobile Banking
- Process of creation/Activation/Resetting/delivery of M- PINS.
- Authentication controls.

2.2.11 Mail Messaging System Audit

The Mail Messaging audit shall cover following aspects:--

- Overall Mail Messaging System management.
- Architecture & design review of Mail Messaging System
- Performance of Mail Messaging Servers
- Configuration Audit for all servers, network devices (Routers, Firewall, Switches) used in Mail Messaging System
- Impact Analysis of Mail Servers

2.2.12 SMS System Audit

The SMS System Audit shall cover following aspects:--

- Overall SMS Management
- Architecture & design Review of SMS System
- Performance Analysis of SMS Servers
- Configuration Audit for all servers, network devices (Routers, Firewall, Switches) used in SMS System
- Impact Analysis of SMS Servers
- Adequacy of security features of the application implemented

2.2.13 Review of IT Processes and IT Management Tools

The review of IT Processes and Management tools shall cover following aspects:--

- IT Asset Management

- Enterprise Management System
- Help Desk
- Change Management
- Incident Management
- Network Management
- Backup & Media Management
- Anti-Virus Management
- Vendor & SLA Management
- **Cyber Security Management Plan**

2.2.14 IT Policies review

An assessment/review of all the important Policies/ Procedure Documents of the Bank such as

- Information Technology (IT) Policy
- ISMS Policy
- Cyber Security Policy
- ATM Policy
- E-Banking Policy
- Outsourcing Policy
- Any other policies of the bank which are not listed above

2.2.15 Payment Gateway Audit

Verification of controls for RTGS, NEFT, SFMS, SWIFT, NFS etc. at Payment Gateway, as per the regulator's policies and guidelines.

2.2.16 CTS-Chennai, Delhi, Mumbai

CTS-Chennai, Delhi & Mumbai shall cover following aspects:--

- Detailed review of the CTS architecture vis-à-vis the RBI guidelines.
- Review on internal controls in place to minimize errors & frauds.
- Interface with CBS & other applications.
- Authentication controls.
- Review of the Work Flow
- Vulnerability/ Threat Assessment

2.2.17 Registration Authority (RA) Office Audit

Registration Authority (RA) Office Audit shall cover following aspects:--

- Audit of all RA functions
- Compliance to the requirements of IT acts 2000 & 2008, Rules and Regulations.
- Compliance of RA functions as per IDRBT checklist.
- Reconciliation of digital signatures issued/revoked by RA with IDRBT.
- Digital Certificates details/record maintenance as per IDRBT requirements.

2.2.18 Call Centre Audit

Call Centre Audit shall cover following aspects:--

- Review of the call centre architecture.

- Vulnerability/ Threat Assessment
- Review on internal controls in place to minimize errors & frauds.
- Manageability of the solution implemented by means of administrative control such as administrative password.
- Adequacy of security features of the application implemented.
- Solution should not breach the security of any other installations of Bank in any way.
- Review of interfaces if any
- Authentication controls.

2.2.19 Risk Based Internal Audit (RBIA)

Risk Based Internal Audit shall cover following aspects:--

- Review of System Architecture of RBIA.
- Vulnerability/ Threat Assessment of the Servers and associated peripherals
- Review of risk based Internal Audit & Off-site Surveillance implemented in the System including work flow.
- Manageability of the solution implemented by means of administrative control such as administrative password.
- Adequacy of security features of the application implemented.
- Solution should not breach the security of any other installations of Bank in any way.
- Review of interfaces, particularly with Finacle & others, if any.
- Authentication controls.

2.2.20 Management Information System –Automated Data Flow to RBI (MIS-ADF)

MIS-ADF Audit shall cover following aspects:--

- Vulnerability/ Threat Assessment of the Servers and associated Peripherals
- Review of MIS ADF Architecture
- Review of DC-DR Replication
- IS Audit with respect to Data Integrity & Consistency
- Manageability of the solution implemented by means of administrative control such as administrative password.
- Adequacy of security features of the application implemented. (Testing for known vulnerabilities and configuration issues on Web Server & Web Application, Denial of Service Attack, Testing for SQL Injection Vulnerability etc.)
- Review of interfaces, particularly with Finacle & others, if any. Authentication controls (OS, Database, Storage and Application Security & Authentication.
- Controls for managing change, patch, Source Code and Sensitive DB password.
- Controls for performing/changing parameter setup of functionality across applications (also controls for impact analysis of changes made).

2.2.21 Internet Banking

Internet Banking Audit shall cover following aspects:--

- Information systems security framework
- Web server

- Logs of activity
- De-militarized zone and firewall
- Security reviews of all servers used for Internet Banking
- Database and Systems Administration
- Operational activities
- Application Control reviews for internet banking application
- Application security

2.2.22 Privacy and Data Protection

Privacy and Data Protection Audit shall cover following aspects:--

- Controls established for data conversion process
- Information classification based on criticality and sensitivity to business Operations
- Fraud prevention and Security standards
- Isolation and confidentiality in maintaining of Bank's customer Information, documents, records by banks
- Procedures for identification of owners
- Procedures of erasing, shredding of documents and
- Media containing sensitive information after the period of usage.
- Media control within the premises.

2.2.23 Business Continuity Management & Cyber Crisis Management

Business Continuity Management Audit shall cover following aspects:--

- Top Management guidance and support on BCP
- The BCP methodology covering the following:
  - Identification of critical business
  - Owned and shared resources with supporting function
  - Risk assessment on the basis of Business Impact Analysis ('BIA')
  - Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO')
  - Minimizing immediate damage and losses
  - Restoring of critical business functions, including customer-facing systems and payment settlement systems
  - Establishing management succession and emergency powers
- Addressing of HR issues and training aspects
- Providing for the safety and wellbeing of people at branch or location at the time of disaster
- Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.
- Independent Audit and review of the BCP and test result
- Participation in drills conducted by RBI for Banks using RTGS/NDS/CFMS Services
- Maintaining of robust framework for documenting, maintaining and Testing business continuity and recovery plans by Banks and Service Providers.

2.2.24 Asset Management

Asset Management shall cover following aspects:--

- Records of assets mapped to owners
- For Payment Card Industry (PCI) covered data, the following should be implemented:
  - Proper usage policies for use of critical employee facing technologies
  - Maintenance of Inventory logs for media
  - Restriction of access to assets through acceptable usage policies, explicit management approval, authorized use of technology, access control list covering list of employees and devices, labeling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
- Review of duties of employees having access to asset on regular basis.

2.2.25 Human Resources

Human Resource Management in IS Audit Context shall cover following aspects:--

- Formal Organization Chart and defined job description maintained and reviewed periodically.
- Proper segregation of duties maintained and reviewed regularly
- Assessment of Manpower and competency of Staff handling IT Infrastructure/ Application. Training need of the Staff handling IT Infrastructure/Application.
- Prevention of unauthorized access of IT Assets to Former employees
- Dismissed staff to be removed from premises on immediate effect. People on notice period moved in non-sensitive role and maintenance of such reports.
- Close supervision of staff in sensitive position

2.2.26 IT Financial Control

IT Financial Control shall cover the following aspects:-

- Comprehensive outsourcing policy
- Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract
- Periodic review of financial and operational condition of Service Provider with emphasis to performance standards, confidentiality and Security, business continuity preparedness
- Contract clauses for vendor to allow RBI or personnel authorized by RBI
- Access relevant information/ records within reasonable frame of time.

2.2.27 IT Operations

IT Operations shall cover the following aspects:-

- Application Security covering access control
- Business Relationship Management

- Customer Education and awareness for adaptation of security measures.
- Mechanism for informing banks for deceptive domains, suspicious emails
- Trade-marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
- Use of SSL and updated certification in website
- Informing client of various attacks like phishing

➢ Capacity Management

➢ Service Continuity and availability management

- Consistency in handling and storing of information in accordance to its classification
- Securing of confidential data with proper storage
- Media disposal
- Infrastructure for backup and recovery
- Regular backups for essential business information and software
- Continuation of voice mail and telephone services as Part of business contingency and disaster recovery Plans
- Adequate insurance maintained to cover the cost of Replacement of IT resources in event of disaster
- Avoidance of single point failure through contingency Planning

➢ Service Level Management.

2.2.28 Project Management

Project Management shall cover the following aspects:-

➢ Information System Acquisition, Development and maintenance

- Sponsorship of senior management for development projects
- New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
- Scrambling of sensitive data prior to use for testing purpose

➢ Release Management

- Access to computer environment and data based on job roles and responsibilities
- Proper segregation of duties to be maintained while granting access in the following environment
  - Live
  - Test
  - Development
- Segregation of development, test and operating environments for software.

2.2.29 Record Management

Record processes and controls shall cover the following aspects:-

➢ Policies for media handling, disposal and transit

- Periodic review of Authorization levels and distribution lists
- Procedures of handling, storage and disposal of information and media
- Storage of media backups
- Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement.

2.2.30 Technology Licensing

Technology Licensing shall cover the following aspects:-

- Periodic review of software licenses
- Legal and regulatory requirement of Importing or exporting of software.

2.2.31 IT outsourcing related controls

The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.

- **Compliance:** Assess the third-party's ability/control framework in place to comply with laws/regulations.
- **Information Security & Privacy:** Assess third party controls over the Availability, confidentiality, and integrity of third party data.
- **Physical Security:** Assess facility access and security measures implemented by the third party.
- **Country Risk:** Assess political, geographic, regulatory, legal, and economic risks of sourcing to a country or region.
- **Business Continuity & Resiliency:** Assess the third parties ability to perform in the event of a process failure or catastrophic event.
- **Financial:** Assess financial stability for the third party to continue provide the product/service.
- **Technology:** Assess the adequacy and appropriateness of the third parties systems and applications to provide the product/service
- **Subcontractor:** Assess the risk management processes surrounding the use of subcontractors by third parties.
- **Operational Competency:** Assesses the ability of the third party to deliver the contracted products/services.

2.2.32 IT Architecture

IT Architecture shall cover the following aspects:-

- **Acquisition and Implementation of Packaged software**
  - Requirement Identification and Analysis
  - Product and Vendor selection criteria
  - Vendor selection process
  - Contracts
  - Implementation

- Post Implementation Issues

- **Development of software- In-house and Out-sourced**
  - Audit framework for software developed in house, if any
  - Software Audit process
    – Audit at Program level
    – Audit at Application level
    – Audit at Organizational level
  - Audit framework for software outsourcing
- **Operating Systems Controls**
  - Adherence to licensing requirements
  - Version maintenance and application of patches
  - Network Security
  - User Account Management
  - Logical Access Controls
  - System Administration
  - Maintenance of sensitive user accounts
- **Application Systems and Controls**
  - Logical Access Controls
  - Input Controls
  - Processing Controls
  - Output Controls
  - Interface Controls
  - Authorization Controls
  - Data Integrity/ File Continuity controls
  - Review of logs and audit trails
- **Database Controls**
  - Physical access and protection
  - Referential Integrity and accuracy
  - Administration and Housekeeping
- **Network Management audit**
  - Process
  - Risk acceptance (deviation)
  - Authentication
  - Passwords
  - Personal Identification Numbers ('PINS')
  - Dynamic password
  - Public key Infrastructure ('PKI')
  - Biometrics authentication
  - Access Control
  - Cryptography
  - Network Information Security
  - E-mail and Voicemail rules and requirements
  - Information security administration
  - Microcomputer/ PC security
  - Audit trails
  - Violation logging management
  - Information storage and retrieval
  - Penetration testing

2.2.33 Maintenance

The IS Asset maintenance shall cover the following aspects:-

- **Change Request Management**
  - Software developed in-house
- **Version Control**
- **Software procured from outside vendors**
- **DC Operations (KDC & BDC) both Internal and External**
- **Software trouble-shooting**
  - Helpdesk
- **File/ Data reorganization**
- **Backup and recovery**
  - Software
  - Data
  - Purging of data
- **Hardware maintenance**
- **Training**

2.2.34 Others

- Privileges available to Systems Integrator and Outsourced Vendors.
- Evaluate role, responsibility and accountability of IT Process owners.
- Review of DR Drills undertaken for CBS/ADC & other delivery channels at Treasury branch and reports thereof Comments on sufficiency and periodicity etc. of DR Drills undertaken and planned.
- Audit of anti virus protection at host and at desktop levels, procedure of antivirus updates at DC, Servers and Desktops, Gateway level AV protection etc
- Alignment of IT strategy with Business strategy.
- IT Governance related processes.
- Long term IT strategy and Short term IT plans.
- Information security governance, effectiveness of implementation of Security policies and processes.

2.3 AUDIT APPROACH

Information Systems Security Audit approach includes the following:

- Auditing around the computer
- Auditing through the computer
- Auditing with the computer
- Through preparation of IS audit checklists based on globally accepted standards and RBI guidelines/ Circulars / IT Acts.
- Based on the audit findings risk assessment to be classified as Low, Medium and High in each specific audit areas.

The selected auditors must understand the business and IT environment, risks and internal control framework. During audit, auditors shall obtain evidences, perform test procedures, appropriately document findings, and conclude a report. Guidance on executing the IS Audit may entail the following steps:

- Refining the understanding of business process and IT environment
- Refining the scope and identifying internal controls

- Testing Control Design
- Testing the outcome of the control objectives
- Collecting audit evidence
- Documenting test results
- Concluding tests performed
- Considering use of audit accelerators
- Considering the use of Computer-Aided Automated Tools (CAATs)
- Considering the work of others
- Considering third-party review by service providers

2.4 AUDIT METHODOLOGY

IS Auditors can use an appropriate combination of manual techniques and CAATs/automated tools for audit purpose. To increase efficiency and effectiveness (and also for consistency) IS Auditors may also use testing accelerators i.e. tools or techniques such as CAATs, Network Analysis tools, Hacking tools, Application Security tools or any other tools that will help support IS Audit procedures.

There shall be a Scoring Model used to define the Criticality (Critical, High Medium, Low) of a particular Audit Unit/Application. The scoring model shall be based on various controls of the System/application/devices and the criticality of the System/application/devices. The criticality (Critical, High Medium, Low) of the audit observations shall be arrived at by adopting suitable scoring model of Industry Standard such as **OWASP**, **CVSS**, and **ISO 31000** etc.

A brief description of the **Audit Methodology and Work Plan** is to be submitted in format as per **Annexure-15**. The Audit Methodology and Work Plan shall be discussed with the bank's team before the start of Audit.

2.5 AUDIT PHASES AND SCHEDULE

2.5.1 The empanelled bidders have to undertake the audit (except VA/PT/Firewall audit) within 2 weeks from date of issue of Work Order, in the following phased manner:

Srl No	PHASE	ACTIVITY	TIMELINES
1	**PHASE – I** [PLANNING & CONDUCT OF AUDIT]	1. Conduct of IS audit as per scope 2. Risk rating of Servers/Devices based on any Industry Standard Methodology 3. Conduct Gap Analysis of the Banks compliance vis-à-vis legal, regulatory, statutory and Govt. of India guidelines in the relevant areas. 4. Submission of preliminary draft audit report of IS audit findings.	10 weeks* from the date of undertaking the assignment.
2	**PHASE – II** [REPORTING & REVIEW]	1. Review of Audit Report with Risk rated (Critical, High, Medium, Low) observations 2. Assigning an Overall risk score and Risk rating (Critical, High Medium, Low) for a particular Audit Unit/Server/Device 3. Submission of final reports and Acceptance of the same by the Bank.	2 weeks from the date of completion of **Phase I**.

3	**PHASE – III** [COMPLIANCE & CLOSURE]	1. Compliance review 2. Submission of Review Report with Risk rated (Critical, High Medium, Low) observations vis-à-vis compliance by bank. 3. Issuance of Closure Certificate on completion of the compliance audit.	Within **4 months** from the date of completion of Phase II. Exact date of commencement of Review Audit will be intimated by the Bank.

Note:-

- Application Audit, Migration Audit (if any), Process audit, Network Architecture Review, Source Code Audit, Operating System Audit, Database Audit etc. should be completed and draft report submitted **within 10 weeks** from the date of issue of Work Order to the empanelled bidders. The Review report should be submitted before the end of the relevant Financial Year Audit period. For example, if the Audit period pertains to FY2018-19, then the Audit should be completed by 15th June, 2018 and Post Audit Compliance report should be submitted latest by 31st March, 2019. The review of each Audit Units should be completed and report submitted as and when bank completes the compliance of the audit observations, on intimation by the bank.

2.5.2 The empanelled bidders have to undertake the VA/PT/Firewall audit within 2 weeks from date of issue of Work Order.

Srl No	PHASE	ACTIVITY	TIMELINES
1	**PHASE – I** [PLANNING & CONDUCT OF AUDIT]	1. Risk rating of Servers/Devices based on Industry Standard Methodology 2. Conduct of Audit as per scope	4 weeks* from the date of undertaking the assignment.
2	**PHASE – II** [REPORTING of Findings]	1. Submission Audit Report with Risk rated (Critical, High Medium, Low) observations 2. Assigning an Overall risk score and Risk rating (Critical, High Medium, Low) for a particular Server/Device	2 weeks from the date of completion of **Phase I**.
3	**PHASE – III** [COMPLIANCE & CLOSURE]	1. Compliance review 2. Submission of Review Report with Risk rated (Critical, High Medium, Low) observations vis-à-vis compliance by bank. 3. Issuance of Closure Certificate on completion of the compliance audit.	Within 4 **Weeks** from the end of relevant quarter. Exact date of commencement of Review Audit will be intimated by the Bank.

- VA, PT & Firewall Rule Review should be completed and final Report submitted **within 4 weeks** from the date of issue of Work Order to the empanelled bidders and Post Audit compliance should be completed within two weeks after the end of the relevant quarter. For example, if the VA/PT pertains to June, 2018 Quarter, then the Post Audit Compliance report should be submitted by 15th of July, 2018**.** However,

the exact date for commencement of Post Audit Compliance Audit shall be communicated by bank.

An Audit Area/Unit Round will be closed only after the submission of Compliance Review Report of **Critical, High, Medium & Low Risk** observations of each Audit Unit/Area. The Audit Report as well as the Compliance Review reports must be submitted in Hard Copy as well as Soft Copy.

PHASE – I: PLANNING & CONDUCT OF AUDIT

- The Bank will call upon the vendor, on placement of the order, to carry out demonstration and/ or walkthrough, and/or presentation and demonstration of all or specific aspects of the IS Audit at the Bank's desired location or, for a walkthrough, at a mutually agreed location. All the expenses for the above will be borne by the concerned vendor
- **Audit schedule to be provided 7 working days prior to the start of audit along with the name of the auditors who will be conducting the audit**. Resumes of the auditors assigned above task for the project to be provided to the Bank beforehand and they should be deputed to the assignment only after Bank's Consent.
- Commencement of IS Audit of IT Setups as per the scope of Audit.
- Study of the existing systems, processes and meeting with the stakeholders and making them aware of the Audit methodology, checklists etc.,
- **Conduct of Information Systems (IS) Audit, risk based, as per the scope.**
- Conduct Gap Analysis of the Banks compliance vis-à-vis legal, regulatory, statutory and Govt. of India guidelines in the relevant areas.
- Execute Vulnerability Assessment/External Attack Penetration testing of the entire network, conduct application security etc., as per the scope of Audit, with prior intimation to the Bank Officials.
- Identify the security gaps i.e. vulnerability, security flaws, loopholes, etc. during the course of the review of the CBS & other IT infrastructure of the Bank, categorize the identified security gaps based on their criticality and provide recommendations for those gaps along with the resource/effort requirement to address them.
- Suggest changes/modifications in the Security Policies and Security Architecture including Network and Applications to address the same.
- Submission of Preliminary Draft Report of the IS Audit Findings

PHASE – II: REPORTING & REVIEW of Audit Findings

- Vendor has to discuss the preliminary report findings/observations/ recommendations/suggestions with the Bank prior to acceptance of the same. Subject to the acceptance of the preliminary report by the bank, the vendor has to submit the Final report. **All observations should have specific references to standards, guidelines and industry best practices along with detailed analysis and justification.** Those points need to be thoroughly discussed with process owners before finalization of report.

  The final report (Soft as well as Hard Copy) should contain

  a. Executive Summary
  b. Detailed findings / Checklists along with Risk Analysis

c. In Depth Analysis of findings / Corrective Measures & Suggestions

d. **Risk Score Matrix** (Critical, High, Medium, Low) for each Audit Unit viz. Applications/Servers/ Devices.

- Acceptance of the Final Report by the Bank.

PHASE – III: COMPLIANCE & CLOSURE

- An exercise to review the compliance with the findings and recommendations of IS Audit observations are to be undertaken by the empanelled bidder.
- The final date for the start of Compliance Audit will be intimated by the bank.
- This exercise would encompass evaluation of the general/overall level of compliance undertaken by the Bank against the shortcomings reported in the IS Audit Reports.
- A Summarized Audit Type wise Review report is required to be submitted for all the audit findings for different units/area. The reporting format shall be discussed with bank.
- A summary of Audit Unit/Area wise Risk Score & Rating is also to be provided.
- On completion of the compliance review and before final sign off by the Bank, the empanelled bidders to whom work order is issued, have to provide the separate certificates for Bank's Compliance Level vis-à-vis IS Audit and also the Closure Certificate.

2.6 TYPE OF AUDIT & FREQUENCY OF AUDIT:

The IS Auditor shall cover broadly cover following Audit Types (but not limited to) at defined frequency per **Audit Round**.

SL No.	Type of audit	Description	Details Description	Frequency of Audit
1	Penetration Testing	Penetration testing (PT) to be conducted mandatorily on all the public facing application exposed to the internet.	It is a type of testing where the penetration tester/ auditor should not have knowledge on the auditee system, to be conducted by external agency empanelled by CERT_in. Please also refer section 2.1.2 on page 9 for scope of Audit.	**Quarterly** (Conduct of Audit & Compliance Review)
2	Vulnerability Assessment	Vulnerability Assessment (VA) to be carried out on all production critical assets deployed in datacenter and DR, like Network Intrusion prevention system(NIPS), IDS, Routers, Switches, Web servers, Operating Systems, Database systems, IOSs etc. (Threat Vulnerability and Risk Assessment (TVRA) for Data Centre as per scope of Monitoring Authority of Singapore (MAS) & Hong Kong Monitoring Authority (HKMA) shall also be covered)	The auditor should check whether the authorized users have access rights, if so, what infringement can be caused to the system. Auditor has to study the current configuration by individually logging into the system or prepare scripts which can read the parameter and prepare an output to be required for VA report. Such scripts can be tested on UAT before running on the production system. Please also refer section 2.1.1 on page 9 for scope of Audit.	**Quarterly** (Conduct of Audit & Compliance Review)
3	Application Audit (Controls) & Migration Audit	Application testing to be conducted on all critical applications, generally it should be conducted on UAT system by using various tools.	Auditor should have the complete understanding of the data flow on the system, which can be collected by interviewing business owner. **OWASP Top 10 Application Security**	**Once in a year** (Conduct of Audit & Compliance Review)

		Data Migration audit also would be verified and scrutinized by the appointed auditor.	**should be covered viz.** ➢ SQL/Command Injection ➢ Broken Authentication and Session Management ➢ Cross-Site Scripting (XSS) ➢ Insecure Direct Object References ➢ Security Mis-Configuration ➢ Sensitive Data Exposure ➢ Insufficient Attack Protection ➢ Cross-Site Request Forgery (CSRF) ➢ Using Components with Known Vulnerabilities ➢ Under-protected APIs **SAN top 25 threats should also be covered**	
4	Process audit	Process audit is to be conducted for Data Centre, DR Centre any critical location where bank's critical infrastructure is hosted.	➢ Physical/ Logical security of infrastructure ➢ Various controls deployed to safeguard the physical assets ➢ Various process adopted to perform day to day critical activity like data backup, restoration ➢ Licensing checking of all the critical systems like OS, database, web servers, IOs. ➢ Signature/patch deployment on critical asset like firewall/ IPs/ IDs/ iOS/OS and database systems ➢ End to End Process Audit should be covered	**Once in a year** (Conduct of Audit & Compliance Review)
5	Network architecture Review	Network design of critical architecture and infrastructure performance controls shall be reviewed.	To be discussed with network and IT security business owner, and updated network diagram to be taken to deeply study the flow of traffic. Please also refer section 2.2.5 of this document.	**Once in a year** (Conduct of Audit & Compliance Review)
6	Firewall Rule base Review	It can be considered as Vulnerability assessment (VA) testing, all the configuration output of the firewall policy to be captured and to be studied policy wise manually or using the tools, so that any mis-configuration residing which may be mitigated.	Auditor has to study the current configuration by individual logging into the firewall system or take the configuration output from at backend for analyzing. Auditor should give Suggestion on removing archaic rules to avoid clogging of the firewall	**Quarterly** (Conduct of Audit & Compliance Review)
7	Source Code Audit	Source code audit review of in-house developed packages and Version Control. **For outsourced software, assurance shall from respective vendors** regarding source code audit compliance in the form of Audit Certificate from respective vendors.		**Once in a year** (Conduct of Audit & Compliance Review)
8	Operating System Audit	For detail Refer section 2.2.2 of this Document.		**Once in a year** (Conduct of Audit & Compliance Review)
9	Database Audit	For detail Refer section 2.2.4 of this Document.		**Once in a year** (Conduct of Audit & Compliance Review)

2.7 GENERAL GUIDELINES FOR AUDIT

a) The Audit should be conducted only by experienced, skilled and certified Auditors.

b) External Penetration Testing/ Vulnerability & Threat Assessment etc. and other critical audit activities must be conducted only by highly skilled and experienced ethical hackers/auditors.

c) External Penetration Testing/ Vulnerability & Threat Assessment etc. or any Audit activity should not disrupt Bank's services.

d) The auditor has to take prior approval of proposed Test cases from the Bank before any testing.

e) Destructive Test cases should not be selected for External Penetration Testing/ Vulnerability & Threat Assessment etc.

f) All Audit activities must comply with all prevalent Statutory and Regulatory Guidelines, Laws, Bye-Laws, Rules, Regulations, Notifications etc.

g) During the course of the audit, if the Auditor observes any major deficiencies, he should immediately bring such observations, deficiencies, areas of improvement and suggestions for improvement to the notice of the concerned persons. The Auditor should also discuss with, guide/help the Bank staff in implementation of critical and important suggestions.

2.8 AUDIT FINDINGS, REPORTS & DELIVERABLES

In respect of the security audit assignment proposed by the bidders, they must submit to the bank the methodology, tools & techniques, as well as Interim and end-of-audit Reports (Executive Summary, Detailed technical findings, Recommendations etc) for each of the major segment covered under the scope of work under the RFP.

The broad deliverable types are given below:

Srl. No	DELIVERABLES	DELIVERABLE TYPE
1	Verification and submission of compliance to previous audit as per format given in **Annexure- 16 & 17.**	Service & Documentation
2	Audit Plan for conduct of Audit Units under IT Universe/Scope of Work should be prepared in consultation with the bank before conduct of audit of a particular Type of Audit.	Service & Documentation
3	Risk Matrix of all the Information Systems (Audit Units) of the Bank mentioned under 2.5 above, based on Risk Analysis along with the Gap Analysis document as per the guidelines issued by RBI, Govt. of India & other regulatory authorities. (Hard & Soft copies). All audit units to be risk rated as either Critical Risk, High Risk, Medium Risk or Low Risk)	Service & Documentation
4	Finalization and submission of Check Lists for Individual Audit Units in consultation with the Bank	Service & Documentation
5	Conduct of IS Audit as per the scope	Service
6	IS Audit Report (Preliminary Draft & Final) (Hard & Soft copies), including Review Report.	Documentation
7	A presentation to the targeted group of officials of the Bank, broadly explaining the ➢ methods of assessment followed, ➢ weaknesses / vulnerabilities observed, and ➢ Recommended course of action for rectification	Service & Documentation

	The IS Auditor must also provide Technical assistance in compliance of VA/PT/Firewall rule base/Network Architecture Review etc as required/ desired by bank.	
9	Post Compliance review cum closure report. Compliance Certificate and Closure Certificate. (hard & soft copies)	Documentation

Upon successful delivery of all the deliverables and closure of all the three phases (section 2.5) of the **audit Round**, Bank will issue Audit Completion Certificate (ACC) for the particular year to the vendor.

2.8.1 IS AUDIT REPORT

i. Broadly, the IS Audit Report for each application (refer section 2.1 on page 8 for list* of application) should contain the following points:
(the list may increase as per banks requirement)*

a) Identification of Auditee (Address & contact information), Dates and Location(s) of audit, Terms of reference (as agreed between the Auditee and auditor), including the standard for audit, if any, Audit plan, Explicit reference to key Auditee organization documents (by date or version) including policy and procedure documents, Additional mandatory or voluntary standards or regulations applicable to the Auditee.
b) Personnel involved in the audit.
c) Report on audit covering compliance status of the previous IS Audit.
d) Risks associated with Gaps, deficiencies, vulnerabilities and Analysis of the same.
e) Detailed report of network, application audit including VAPT with recommendations and suggestions.
f) Summary of audit findings including identification tests, tools used, results of tests performed during IS Audit and recommendations for corrective action.

ii. In case of VA/PT, IP-wise/application-wise/location-wise reports are desired and the same should be provided in soft copy in excel sheet. For hard copy, Location-wise, Application-wise, IP-wise observations should be provided.

iii. For Network architecture Review & Firewall Rule base Review, a separate report may be provided.

Both the preliminary draft and final Audit report should contain the following sections:

1. Executive Summary
    a. An executive summary of the Audit findings should form a part of this section
2. Detailed findings
    a. The detailed findings of the IS Audit would be brought out in this report viz. identification of flaws/ gaps /vulnerabilities in the systems (specific to equipments/resources – indicating name and IP address of the equipment with Office & Department name), identification of threat sources, identification of Risk, Identification of inherent weaknesses, details of Servers/Resources affected etc.

b. Report should classify the Audit Units into Critical / Non Critical category and assess the category of Risk Implication OF Audit Observations as CRITICAL/HIGH/MEDIUM/LOW risk based on the impact. The various checklist formats, designed and used for conducting the IS Audit as per the scope, should also be included in the report separately for Servers (different for OS, RDBMS, Network equipments, security equipments etc), so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed in Bank. The Reports should be substantiated with the help of snap shots/evidences /documents etc. from where the observations were made.

3. Critical Analysis & Recommendation

   a. The findings of entire IS Audit Process should be critically analyzed and controls should be suggested as corrective / preventive measures for strengthening / safeguarding the IT assets of the Bank against existing and future threats in the short / long term.

   b. All **observations/recommendation** should have specific references to standards, guidelines and industry best practices along with detailed analysis and justification

   c. Report should contain recommendations for improvement in the systems wherever required along with alternate solutions, if recommendations could not be implemented due to technical feasibility/business constraint. Also recommendations should be as per the industry best practices, standards, guidelines etc.

All the IS Audit reports (Hard & Soft copies) should be submitted in English only.

a) **HARD COPY**: Three sets which are neatly and robustly bound on good-quality paper of A-4 size.

b) **SOFT COPY**: CD/DVD containing the IS Audit reports in MS-Word/MS-Excel/PDF formats should be necessarily password protected/encrypted.

2.8.2 PRESENTATION to the Targeted Group:

Before presenting the report after each stage of assessment, a presentation must be made to the targeted group of officials of the Bank, broadly explaining the methods of assessment followed, weaknesses/vulnerabilities observed, and recommended course of action for rectification

The selected bidder should also provide the customized material (PPT/ANIMATED/PDF etc.) in a precise and lucid manner for circulation in the Bank, so that it creates awareness about the information security and audit among the employees of the Bank.

SECTION III

3.1 INVITATION FOR BIDS

UCO BANK invites separate sealed Technical & Commercial bids from the experienced bidders empanelled by Cert-In for **Information Systems (IS) Audit.**

3.2 COST OF TENDER DOCUMENT

Prospective Bidders are required to pay the cost of the Tender Document as mentioned in the **Bid Control Sheet** by Demand Draft/Pay Order favoring UCO Bank payable at Kolkata at the time of submission of the Technical & Commercial bids, failing which the bid of the concerned Bidder will be rejected. The Tender Document cost is non-refundable. The tender document may also be downloaded from The Bank's official website www.ucobank.com.

3.3 EARNEST MONEY DEPOSIT (EMD)

The bidder is required to deposit Earnest Money of Rs 1 lac (Rupees One lac only) as mentioned in the **Bid Control Sheet** along with their Technical & Commercial Bids in the form of a Bank Guarantee (as per format furnished in **Annexure–13**) valid for a period of **180 days** together with a claim period of **30 days** issued by a Scheduled commercial Bank in India, failing which the bid of the concerned bidder will out-rightly be rejected.

Non-submission of Earnest Money Deposit will lead to outright rejection of the Offer. The EMD of unsuccessful bidders will be returned to them on completion of the procurement process without any interest thereon. The EMD of successful bidder(s) will be returned to them on submission of Performance Bank Guarantee (s) (as per format furnished in **Annexure–14**) either at the time of or before the execution of the Master Contract.

The Earnest Money Deposit may be forfeited under the following circumstances:-

- If the Bidder withdraws its bid during the period of bid validity (180 days from the date of opening of the Technical bid).
- If the Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading at any time prior to signing of contract and / or conceals or suppresses material information; and / or
- In case of the successful Bidder, if the Bidder fails:
    - To sign the Master Contract in the form and manner to the satisfaction of the Bank.
    - To furnish performance Bank Guarantee in the form and manner to the satisfaction of the Bank either at the time of or before the execution of Master Contract.

3.4 REJECTION OF THE BID

The Bid is liable to be rejected if:

3.4.1 The document doesn't bear signature of authorized person on each page signed and duly stamp.

3.4.2 It is received through Telegram/Fax/E-mail.

3.4.3 It is received after expiry of the due date and time stipulated for Bid submission.

3.4.4 The bidder submits Incomplete Bids, including non-submission or non-furnishing of requisite documents / Conditional Bids / Bids not conforming to the terms and conditions stipulated in this Request for proposal (RFP).

3.4.5 Bidder should comply with all the points mentioned in the Scope of work. Noncompliance of any point will lead to rejection of the bid.

3.4.6 Any form of canvassing/lobbying/influence/query regarding short listing, status etc. will be a disqualification.

3.5 PRE-BID MEETING:

3.5.1 The prospective bidders may like to attend a pre-bid meeting to be held at the venue and time as indicated in the "Calendar of Events" in **Bid Control Sheet** after publication of RFP and well before the last date for receipt of bids. Up to a **maximum of 2 (two) authorized representatives** of each prospective bidder will be permitted to attend the pre-bid meeting.

3.5.2 Bidders may send their queries relating to RFP to our office by e-mail / fax / speed post / courier, well in advance, so that the same could be addressed during the Pre-Bid meeting with interested Bidders or clarifications will be given by way of addendum to RFP and placed on Bank's web-site www.ucobank.com as additions/corrigendum to RFP.

3.5.3 The Bank will have liberty to invite its Technical Consultant or any outside agency, wherever necessary, to be present in the pre-bid meeting to reply to the Technical Queries of the bidders in the meeting.

3.5.4 Non-attendance at the Pre-bid Meeting will not be a cause for disqualification of a bidder.

3.5.5 Bank will not contact the prospective bidders separately.

3.5.6 No Queries/clarifications would be entertained over phone by the bank.

3.6 Modification and Withdrawal of Bids

No bid can be modified by the bidder subsequent to the closing date and time for submission of bids. In the event of withdrawal of the bid by bidders, Bank shall be entitled to forfeit the EMD.

3.7 INFORMATION PROVIDED

The RFP document contains statements derived from information that is believed to be reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Bank in relation to the provision of services. Neither Bank nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied as to the accuracy or completeness of any information or statement given or made in this RFP document.

3.8 FOR RESPONDENT ONLY

The RFP document is intended solely for the information to the party to whom it is issued ("the Recipient" or "the Respondent") and no other person or organization.

3.9 CONFIDENTIALITY

The bidder must undertake that they shall hold in trust any Information received by them, under the Contract/Agreement, and the strictest of confidence shall be maintained in respect of such Information. The bidder has also to agree:

- To maintain and use the Information only for the purposes of the Contract/Agreement and only as permitted by BANK;
- To only make copies as specifically authorized by the prior written consent of Bank and with the same confidential or proprietary notices as may be printed or displayed on the original;
- To restrict access and disclosure of Information to such of their employees, agents, strictly on a "need to know" basis, to maintain confidentiality of the Information disclosed to them in accordance with this Clause and
- To treat all Information as Confidential Information.
- Conflict of interest: The Vendor shall disclose to BANK in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Vendor or the Bidder's team) in the course of performing the Service(s) as soon as practical after it becomes aware of that conflict.
- The successful Bidder is required to enter into a *Non Disclosure Agreement* with the bank as per bank's format before or at the time of execution of the Master Contract.

3.10 COSTS BORNE BY RESPONDENTS

All costs and expenses incurred by Recipients / Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by Bank, will be borne entirely and exclusively by the Recipient/Respondent.

3.11 NO LEGAL RELATIONSHIP

No binding legal relationship will exist between any of the Recipients / Respondents and Bank until execution of a contractual agreement.

3.12 ERRORS AND OMISSIONS

Each Recipient should notify Bank of any error, omission, or discrepancy found in this RFP document.

3.13 ACCEPTANCE OF TERMS

A Recipient, by responding to Bank RFP, will be deemed to have accepted the terms as stated in the RFP.

3.14 RFP RESPONSE

If the response to this RFP does not include the information required or is incomplete or submission is through Fax mode or through e-mail, the response to the RFP is liable to be rejected. All submissions will become the property of Bank. Recipients shall be deemed to license and grant all rights to Bank to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients who have registered a submission and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or Banking documents.

3.15 NOTIFICATION

Bank will notify the Respondents in writing as soon as practicable about the outcome of the RFP evaluation process, including whether the Respondent's RFP response has been accepted or rejected. Bank is not obliged to provide any reasons for any such acceptance or rejection.

3.16 LANGUAGE OF BIDS

The bid, correspondence and supporting documents should be submitted in English.

3.17 Performance Bank Guarantee

The successful bidder shall be required to provide a Performance Bank Guarantee (as per format furnished in **Annexure–14**) for 10% of the Total Cost of Ownership/Order Value (**proportionate Share of Total Order Value in case two or more bidders are empanelment as per the terms of the RFP**) issued by any scheduled commercial bank (other than UCO Bank) valid for the tenure of the **contract period (36 months) plus a claim period of 3 (three) months**, indemnifying any loss to the Bank. The bank guarantee shall be provided to the bank either before or at the time of execution of the Master Contract. Bank reserves the right to invoke the PBG for any non-compliance of the terms & conditions of this RFP or the Master Contract to be

executed between the selected bidder and the Bank at any point of time without prejudice to its other rights and remedies available under the Contract and/or the Law (s) for the time being in force. In case the contract period is extended by the Bank, the selected bidder shall be responsible to extend the validity period and claim period of the Performance Bank Guarantee.

3.18 INDEMNITY

The selected Bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights.

The selected Bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.

The selected Bidder agrees to indemnify and keep indemnified Bank at all times against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfill obligations by the selected bidder or its employees/personnel.

All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the Vendor shall continue to be liable under the indemnities.

Selected Bidder is required to furnish a separate Letter of Indemnity (Format whereof to be supplied by the Bank) in Bank's favour in this respect before or at the time of execution of the Master Contract.

3.19 AUTHORIZED SIGNATORY

The selected bidder shall indicate the authorized signatories who can discuss, sign negotiate, correspond and any other required formalities with the bank, with regard to the obligations. The selected bidder shall submit, a certified copy of the resolution of their Board, authenticated by Company Secretary, authorizing an official or officials of the company to discuss, sign with the Bank, raise invoice and accept payments and also to correspond. The bidder shall furnish proof of signature identification for above purposes as required by the Bank.

3.20 RIGHTS OF UCO BANK

The Bank further reserves the right to:

- Cancel the entire RFP process without assigning any reasons whatsoever and without any cost or compensation therefor at any stage of the RFP process.
- Cancel or Modify any terms, conditions and specifications of the RFP by publishing a notice to such effect on website of UCO Bank without assigning any reasons whatsoever and without any cost or compensation therefor.
- Obtain revised price Bids from the Bidders with regard to modifications/ changes in RFP.

- Place repeat orders.
- Issue the amendments to the RFP at anytime, prior to the deadline for the submission of Bids. From the date of issue, amendments to RFP Document shall be deemed to form an integral part of the RFP Document.
- The Bank also reserves the right to get the IS audit done for some of the Systems only. In the event of change of quantities, the Total Professional Cost (TPF) would be worked out after normalizing the Commercial Offer to suit the required systems.
- The Bank also reserves the right to get the feedback from the organizations mentioned in the clients lists

3.21 FORCE MAJEURE

Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidder or the Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have been foreseen and which substantially affect the performance of the Contract, such as:

- Natural calamities, including but not limited to floods, earthquakes, epidemic,
- Acts of any Government, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes, terrorist attacks, and public unrest in work area.

Provided **either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes**. The Selected bidder or the Bank shall not be liable for delays in performing their obligations resulting from any Force Majeure cause as referred to and/or defined above.

3.22 CLARIFICATIONS OF BIDDER'S OFFERS

To assist in the scrutiny, evaluation and comparison of offers/bids, Bank may, at its sole discretion, ask some or all bidders for clarification of their offer/bid. The request for such clarifications and the response will necessarily be in writing. Any decision of Bank in this regard shall be final, conclusive and binding on the bidder/ renderer.

3.23 Order Cancellation (Termination)

UCO BANK reserves the right to cancel the work/purchase order or terminate the Master Contract by giving **One Month (30 days) prior notice** in writing and recover damages, costs and expenses etc., incurred by Bank under the following circumstances: -

a) The selected bidder commits a breach of any of the terms and conditions of this RFP or the Master Contract to be executed between the Bank and the selected Bidder.

b) The selected bidder goes into liquidation, voluntarily or otherwise.

c) The selected bidder violates the Laws, Rules, Regulations, Bye-Laws, Guidelines, Notifications etc.

d) An attachment is levied or continues to be levied for a period of seven days

upon effects of the bid.

e) The selected bidder fails to complete the assignment as per the time lines prescribed in the Work Order/ Master Contract and the extension, if any allowed.

f) Deductions on account of liquidated damages exceed more than 10% of the total work order.

g) In case the selected bidder fails to deliver the resources as stipulated in the delivery schedule, UCO BANK reserves the right to procure the same or similar resources from alternate sources at the risk, cost and responsibility of the selected bidder.

h) After award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, UCO BANK reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which UCO BANK may have to incur in executing the balance contract. This clause is applicable, if the contract is cancelled for any reason, whatsoever.

i) UCO BANK reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the adjustment of pending bills and/or invoking the Performance Bank Guarantee under this contract.

The rights of the Bank enumerated above are in addition to the rights/remedies available to the Bank under the Law(s) for the time being in force.

3.24 Consequences of termination

In the event of termination of the Contract due to any reason, whatsoever, [whether consequent to the expiry of stipulated term of the Contract or otherwise], UCO 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 steps to minimize loss resulting from the 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.

In the event that the termination of the Contract is due to the expiry of the term of the Contract and the Contract is not further extended by UCO BANK, the Vendor herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as UCO BANK may specify including training, where the successor(s) is a representative/personnel of UCO 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.

Nothing herein shall restrict the right of UCO BANK to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Letter of Indemnity and pursue such other rights and/or remedies that may be available to UCO BANK under law or otherwise.

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.

3.25 DISPUTE RESOLUTION MECHANISM

The Bidder and the Bank shall endeavor their best to amicably settle all disputes arising out of or in connection with the Contract in the following manner:

a. The Party raising a dispute shall address to the other Party a notice requesting an amicable settlement of the dispute within seven (7) days of receipt of the notice.

b. The matter will be referred for negotiation between General Manager (Audit & Inspection Department) of UCO BANK and the Authorized Official of the selected Bidder. The matter shall then be resolved between them and the agreed course of action shall be documented within a further period of 15 days.

In case the dispute(s)/difference(s) between the Parties is/are not settled through negotiation in the manner as mentioned above, the same may be resolved by arbitration and such dispute/difference shall be submitted by either party for arbitration within 15 days of the failure of negotiations. Arbitration shall be held in Kolkata and conducted in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof. Each Party to the dispute shall appoint one arbitrator each and the two arbitrators shall jointly appoint the third or the presiding arbitrator.

The "Arbitration Notice" should accurately set out the disputes between the parties, the intention of the aggrieved party to refer such disputes to arbitration as provided herein, the name of the person it seeks to appoint as an arbitrator with a request to the other party to appoint its arbitrator within 30 days from receipt of the notice. All notices by one party to the other in connection with the arbitration shall be in writing and be made as provided in this tender document.

The arbitrators shall hold their sittings at Kolkata. The arbitration proceedings shall be conducted in English language. Subject to the above, the courts of law at Kolkata alone shall have the jurisdiction in respect of all matters connected with or arising out of the Contract even though other Courts in India may also have similar jurisdictions. The arbitration award shall be final, conclusive and binding upon the Parties and judgment may be entered thereon, upon the application of either party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides.

The Bidder shall not be entitled to suspend the Service/s or the completion of the job, pending resolution of any dispute between the Parties, rather shall continue to render the Service/s in accordance with the provisions of the Contract notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.

3.26 GOVERNING LAWS & JURISDICTION OF THE COURT:

The provisions of this RFP and the Master Contract to be executed shall be governed by the laws of India for the time being in force and the Rules made thereunder from time to time and all the dispute(s) or difference(s) arising out of or in connection with the contract shall be subject to the exclusive jurisdiction of the courts at KOLKATA.

3.27 IMPORTANT DATES

The important dates related to this RFP are given in Calendar of events.

3.28 ACCEPTANCE OF WORK ORDER:

The selected bidder must convey to the bank, in writing, their acceptance of the assignment within 2 working days from the date of receipt of the Work Order through fax/Speed-Post/Courier.

3.29 COMMENCEMENT OF AUDIT WORK:

The empanelled bidders must commence the work/assignment within Two Weeks from the date issuance of Work Order.

3.30 SAFETY OF PERSONNEL

The selected Bidder shall take all steps to ensure safety of their as well as the bank's personnel during execution of the contract and also be liable for any consequences due to omission or act of the selected bidder or their members.

3.31 SUBCONTRACTING:

The selected Bidder will not subcontract or delegate or permit anyone other than the Bidder personnel to perform any of the work, service or other performance required of the Bidder under this agreement without the prior written consent of the Bank and the bank's decision in this regard will be final and acceptable to the bidder.

3.32 SINGLE POINT OF CONTACT

The selected bidder must designate a Single Point of Contact for all aspects of this assignment and also inform the details of such designated person to the Bank.

3.33 GENERAL TERMS & CONDITIONS OF BIDDING

- Each offer should meet the tender specification and should not include any alternatives.
- The Bidder shall bear all costs associated with the preparation and submission of its bid, attending Pre-Bid meeting etc. and Bank will in no case be responsible or

liable for these costs, regardless of the conduct or outcome of the bidding process.

- Bid shall remain valid for 180 days after the date of opening of Technical Bid prescribed by Bank. **The Earnest Money will have to be submitted for a period of 180 days from the date of opening of the bid with a claim period of 30 days.** A bid valid for a shorter period may be rejected by Bank as non responsive.
- In exceptional circumstances, Bank may solicit the Bidders' consent to an extension of the period of validity. The request and the responses thereto shall be made in writing or by fax/email. The Earnest Money provided shall also be suitably extended. A bidder granting the request will not be required nor permitted to modify its bid.
- No Bidder shall contact Bank on any matter relating to its Bid, from the time of the bid opening to the time of final selection of the bidder.
- Any effort by a Bidder to influence Bank in Bank's bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's bid.
- Bank reserves the right to modify any terms, conditions and specifications of the RFP which will be communicated at least 7 working days before last date of submission of the Bid by e-mail/fax.
- In the event of any claim asserted by the third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the Goods or any part thereof in India, the Bidder shall act expeditiously to extinguish such claims. If the Bidder fails to comply and Bank is required to pay compensation to a third party resulting from such infringement, the Bidder shall be responsible for the compensation including all expenses, court costs and lawyer fees. Bank will give notice to the Bidder of such claims, if it is made, without delay by fax/e-mail/registered post.
- The services to be availed from the selected bidder are on a principal to principal basis and do not create any employer- employee relationship. No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the selected bidder, for any assignment under the purchase contract to be issued for this RFP. All remuneration, claims, wages, dues etc. of such employees, agents, contractors, subcontractors etc. of selected bidder shall be paid by selected bidder alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of selected bidder's employee, agents, contractors, and subcontractors, etc. The selected bidder shall hold the Bank, its successors, Assignees and Administrators fully indemnified and harmless against loss or liability, claims, actions or proceedings, if any, that may arise from whatsoever nature caused to the Bank through the action of its employees, agents, contractors, subcontractors etc. However, the selected bidder would be given an opportunity to be heard by the Bank prior to making of a decision in respect of such loss or damage.
- The selected bidder is responsible for managing the activities of its personnel or the personnel of its subcontractors/franchisees and will be accountable for both. The selected bidder shall be vicariously liable for any acts, deeds or things

done by their employees, agents, contractors, subcontractors, and their employees and agents, etc. which is outside the scope of power vested or instructions issued by the Bank. Selected bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc. engaged by selected bidder and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of power , or outside the scope of power, vested under the purchase contract to be issued for this Tender.

- UCO BANK shall be under no obligation to accept the lowest or any other offer received in response to this offer notice and shall be entitled to reject any or all offers without assigning any reason whatsoever. UCO BANK has the right to re-issue tender/bid. UCO BANK reserves the right to make any changes in the terms and conditions of purchase that will be informed to all bidders. UCO BANK will not be obliged to meet and have discussions with any bidder, and/or to listen to any representations once their offer/bid is rejected. Any decision of UCO BANK in this regard shall be final, conclusive and binding upon the bidder.

SECTION-IV

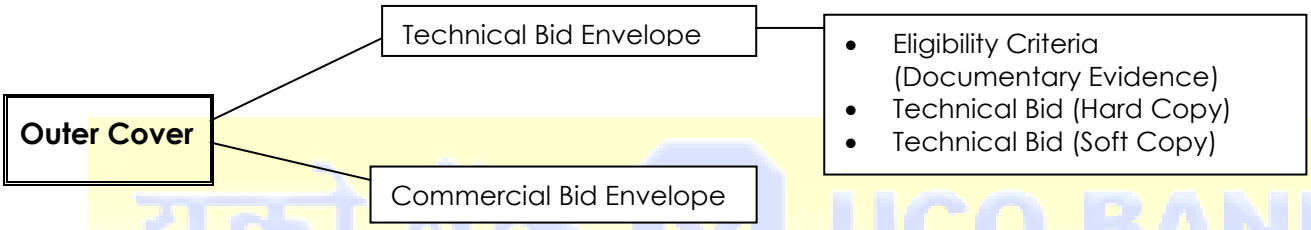
4.1 BIDDING PROCESS

4.1.1 The Technical & Commercial Bids should be duly sealed and superscribed as "Technical Bid for Information Systems Audit" and "Commercial Bid for Information Systems Audit" with outer envelope duly sealed and superscribed "Bid for Selection of IS Auditor for conducting Information Systems Audit" as per bid details given in the RFP.

4.1.2 The bids shall be dropped / submitted at UCO Bank's address given in this RFP, on or before the last date & time as mentioned under calendar of items in the **Bid Control Sheet**. Any Bid received by the Bank after deadline for submission of prescribed Bids, will be rejected and returned unopened to Bidder at the risk of Bidder.

4.1.3 All envelopes must be superscribed with the following information:

- Name of Bidder
- Offer Reference
- Type of Offer (Technical or Commercial)



The Technical Offer should be complete in all respects and contain all information asked for in the exact format (Hard Copy & Soft Copy – CD) of technical specifications given in the RFP. Bank, at its sole discretion, may not evaluate a Technical Offer in case of non-submission or partial submission of technical details. Any decision of Bank in this regard shall be final, conclusive and binding upon the bidder.

Note:

- If the outer cover/envelope are not sealed & superscribed as required, the Bank will assume no responsibility for bid's misplacement or premature opening.
- If any inner envelope of a bid is found to contain both technical & commercial bids then that bid will be rejected summarily.
- In case the specified date of submission of RFP is declared a holiday in West Bengal, the bids will be received till the specified time on the next working day.

4.2 TWO BID SYSTEM

4.2.1 The bidder should take care of submitting the bid properly filed & paginated so that the papers are not lost.

4.2.2 The Bids, which are not sealed as indicated above or open tenders sent through Fax /e-mail will summarily be rejected.

4.2.3 The Bid should contain no alterations, erasures or overwriting except as

necessary to correct errors made by the Bidder, in which case corrections should be duly stamped and initialed / authenticated by the person/(s) signing the Bid. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required in the bidding documents or submission of a bid not substantially responsive to the requirement of the RFP in every respect, will be at the Bidders risk and may result in rejection of the bid.

4.3 BID OPENING AND EVALUATION CRITERIA

The Bank will open the technical bids, in presence of bidders' representative(s) who choose to attend, at the Venue, Date and time mentioned in Bid Control Sheet. The bidder's representatives who are present shall sign the register evidencing their presence/attendance.

4.3.1 TECHNICAL BID

The technical bid will be evaluated for technical suitability as well as for other terms and conditions.

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

4.3.1.2 The Technical Bid should not contain any price information.

4.3.1.3 The Proposal shall be organized and submitted as per **Annexure 18**.

4.3.2 EVALUATION OF TECHNICAL BIDS

Technical offer will be opened on the date and time mentioned in the **Bid Control Sheet** in the presence of the Bidders who choose to attend on the said date and time. The Bank will evaluate the technical responses to the RFP submitted by bidders on the basis of following criteria:--

4.3.2.1 The Bank will evaluate the technical response to the RFP of the Bidders who are found eligible as per the eligibility criteria mentioned in the RFP. There will be no scoring involved in the eligibility evaluation.

4.3.2.2 Completeness of the Technical bid in all respects and availability of all information/details asked for as per **RFP document** & **Annexure-9**.

4.3.2.3 All the details asked in **Annexure-9** are mandatory and if not complied then the bid is liable for rejection.

4.3.2.4 Capabilities/past experience of the bidder to meet the scope & specifications prescribed.

4.3.2.5 Point to point conformity of the services offered as against the required scope & specifications as mentioned by bidder in the Project schedule/approach/methodology.

The technical evaluation will be done by a team constituted by the Bank and Bank may decide to include an External Consultant/Advisor in the

evaluation process. To qualify in Technical evaluation, the bidder has to comply with all the criteria are given in the **Annexure-9.**

4.3.3 COMMERCIAL BID

4.3.3.1 The Commercial Bid should give all relevant price information and should not contradict the Technical Bid in any manner. All prices should be quoted in Indian Rupees only. Bidders will be required to quote Commercial for all Type of Audits (line-Item-wise) in **Annexure-10**. **The bids where Commercial for all Type of Audits is not quoted in Annexure-10 will be summarily rejected.**

4.3.3.2 The Commercial Bid shall comprise of the following documents:

i. Covering Letter in Bidder's Letter head duly signed by Authorized signatory (As per format given in **Annexure-11**)

ii. Commercial Bid with price details (As per **Annexure–10**)

4.3.3.3 After opening the Commercial Offers of the short-listed Bidders, if any discrepancy is noticed between words and figures, the amount indicated in words shall prevail.

4.3.3.4 The Commercial quoted shall be valid for the period of empanelment i.e. three years.

Note: Taxes, if any applicable, at present rate should be quoted in the column "Taxes" mentioned in **Annexure-10**. The Bank will pay the taxes ruling at the time of presentation of the invoices.

4.3.4 EVALUATION OF COMMERCIAL BIDS

Commercial Bids of only technically qualified Bidders will be opened and evaluated. **Commercial evaluation will take into account the following factors for determination of L-1 bidder**:

4.3.4.1 The Commercial Bid should include all travel, boarding, local conveyance and all other incidental expenses and halting allowances for the bidder's personnel proposed to be engaged in the bank's assignment covered under this RFP. UCO Bank will not pay any additional amount other than the amount mentioned in the Commercial Bid for this Security Audit assignment.

4.3.4.2 The Prices quoted must include all taxes, duties, fees, and all levies prevalent under the applicable law at present. All the above charges are deemed to have been included by the bidders in their Commercial Bid (**Annexure-10**).

4.3.4.3 For arriving at (L1), Total Professional Fee (as per **Annexure-10**) will be the basis of comparison amongst Bidders to determine the lowest evaluated offer.

4.3.5 EMPANELMENT of AUDITORS

4.3.5.1 Bank will empanel a maximum of Three (03) firms for three years from the Technically Qualified bidders. If L2 & L3 bidders are agreeable to match the item-wise Commercial of L1 bidder as per **Annexure 10**, they will be empanelled along with L1 for three years. However, if L2 and/or L3 are not agreeable to match the item-wise Commercial of L1 bidder, then L4 and/or L5 and so on, will be asked to match the Commercial of L1 bidder for empanelment.

4.3.5.2 The bidders other than L1, agreeing to match the item-wise Commercial of L1 bidder as per **Annexure 10**, shall submit a revised commercial on their Letter Head. The revised commercial shall be submitted **within One week's time** of the opening of the Commercial bid.

4.3.5.3 The Scope of Audit work will be split between the lowest two bidders (the lowest two bidders are derived from initial Total Commercial quoted in **Annexure 10**) by value every year in the ratio of 60:40 in case only two bidders are empanelled. **For example**, if only L2 is willing to match the price of L1 (and other bidders are not willing) the work distribution between L1 & L2 will be 60 % and 40% (approximately) respectively every year by value of the **initial commercial quote of L1 bidder**.

4.3.5.4 In case three bidders are empanelled, the Scope of Work will be split between the lowest three bidders (the lowest three bidders are derived from initial Total Commercial quoted in **Annexure 10**) by value every year in the ratio of 50:30:20. **For example**, if L2 and L4 (in case L3 is not willing to match the price of L1) are willing to match the item-wise Commercial of L1, the work distribution among L1, L2 and L4 bidders will be in the ratio of 50%, 30% & 20% (approximately) respectively every year by value of the **initial commercial quote of L1 bidder**.

4.3.5.5 Bank may decide to split the Total Audit Scope into two or three groups by clubbing different audit types mentioned in **Annexure 10**. While splitting the work among empanelled bidders in the aforesaid ratio, bank will have its discretion in putting any Type of Audit (**Annexure 10**) under a particular group of work, and assigning a particular group of work to any of the empanelled bidder.

4.3.5.6 The empanelled bidder shall start conduct of Audit Process within **Two week's** time as and when a particular Type of Audit falls due or from the date of intimation by bank to the concerned bidder vide email/letter etc. In case any of the bidders fails to meet the timeline to start conduct of audit assignment, bank will have its own discretion to decide to give the work of the bidder failing to adhere to the timeline, to any other empanelled bidders.

4.3.5.7 A bidder, who is granted a particular group of audit work, shall not be given the same group of audit work in the next Audit Round i.e. there will

be cooling period of one Round for any group of audit work and/or Type of Audit work, for any of the empanelled bidder.

An Audit Unit Round will be said to be complete when the Audit Plan, Conduct of Audit, Review of Compliance of Audit Observations and submission of all relevant Reports & documentations is completed for one complete Round in case of any Type of Audit listed in **Annexure 10.**

4.3.5.8 The tenure for empanelment of Auditor will be for a period of 3 (three) years effective from the date of execution of the Master Contract unless terminated earlier by the Bank by serving **One month notice** (1 Month) days prior notice in writing to the Vendor at its own convenience without assigning any reason and without any cost or compensation therefor. However, after the completion of initial period of 3 (three) years, the contract may be extended/renewed for such further period as would be decided by the Bank on the same terms and conditions as mentioned herein.

The performance of the selected bidder shall be reviewed periodically and in the event of non-satisfactory performance the Bank reserves the right to terminate the contract at its sole discretion by giving **One month notice** (30 Days) notice without assigning any reasons and without any cost or compensation therefor.

4.3.5.8 Bidders who are issued work orders shall execute a Non Disclosure Agreement (NDA) with the Bank assuring confidentiality of Bank's data.

4.4 PAYMENT TERMS:

Payment Terms per Audit Round is given below:

4.4.1 No advance payment will be made.

4.4.2 50% of the charges/fees of a particular Type of Audit (**Annexure 10**) will be payable after submission of the following

- Audit Plan
- Risk Rating of different Audit Units as per Scope of Work
- Check-List for different Audit Units as per Scope of Work
- Audit report as per Scope of Work

4.4.3 25% of the charges/fees will be payable after Bank receiving Compliance Review Report complete in all respect.

4.4.4 Balance 25% will be payable after one month of submission of Review Report complete in all respect, provided bank is satisfied that Review has been conducted complete in all respect as per Scope.

4.4.5 TDS would be deducted for any payment made by the BANK as per the prevailing Rules of Government of India.

4.4.6 GST will be paid as per the prevailing rate.

4.5 PAYING AUTHORITY:

The payments as per the Payment Schedule covered herein above shall be paid by Audit & Inspection Department of UCO Bank, Head Office, 10 B. T. M. Sarani.

4.6 TAXES AND DUTIES:

The bidder will be entirely responsible to pay all taxes whatsoever in connection with delivery of the services at the sites including incidental services and commissioning except applicable Taxes.

Wherever the laws and regulations require deduction of such taxes at the source of payment, Bank shall effect such deductions from the payment due to the vendor. The remittance of amount so deducted and issue of certificate for such deductions shall be made by Bank as per the laws and regulations in force. Nothing in the contract shall relieve the vendor from his responsibility to pay any tax that may be levied in India/abroad on income and profits made by the vendor in respect of this contract.

4.7 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 tender notice and shall be entitled to reject any or all tenders without assigning any reason whatsoever.

4.8 LIQUIDATED DAMAGES/PENALTY CLAUSE:

Subject to Force majeure, if the Bidder fails to deliver or perform the services within the time period(s) specified in the agreement, Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value, as liquidated damages, a sum equivalent to 0.5% of the services for each week or part thereof of delay until actual delivery or performance upto a maximum deduction of 10% of the order value. **Once the maximum is reached Bank may consider cancellation of the order and the Performance Security submitted may be invoked.**

4.9 FORFEITING OF BID SECURITY:

The Bid security may be forfeited: -

4.9.1 If a Bidder withdraws its Bid during the period of Bid validity specified by the Bidder on the Bid Form; or

4.9.2 If it was found that the successful Bidder had made any statement or had enclosed any documentary evidence which turns out to be false / incorrect at any time till the bank's final settlement of the bills submitted by the bidder, for the audit assignment undertaken by the bidder.

4.9.3 The bid security amount will be forfeited if the vendor refuses to accept purchase order or having accepted the purchase order fails to carry out his obligations mentioned therein.

++

SECTION-V: ANNEXURES

ANNEXURE-1: ELIGIBILITY CRITERIA

(Ref: RFP _____dated_____for IS Audit)

Srl. No	Eligibility Criteria	Proof of documents to be submitted
1	The IS Audit firm/company should be in the business of Information System auditing (IS Auditing) in India at least for last three years as on 31.03.2017 (in case of mergers/ acquisition/ restructuring or name change, the date of establishment of the earlier/original Partnership Firm/ Limited Company can be taken in to account).	Copy of the Certificate of Incorporation and Certificate of Commencement of Business (whichever applicable) to be submitted.
2	The Bidder must be a profit making firm/company in any two of the last three years (supporting documents for the year **2014-15, 2015-16, 2016-17** to be submitted).	Copy of the audited balance sheet of the company showing turnover of the company should be submitted.
3	The Bidder must have a turnover of at least **Rs. 2 crore** in the last three financial years (**2014-15, 2015-16, 2016-17**).	Copy of the audited balance sheet
4	The Bidder must be having on their rolls, on permanent employment basis**, a minimum of 10 (ten nos.)** professionals who hold professional certifications like CISA/ DISA/ CISSP/ CISM/ISO 27001 with requisite experience to handle the work as per the Scope (valid as on date).	Self Declaration to this effect with the organizational structure details and necessary professional certificates to be submitted in company letter head. The Profile of the Audit team to be submitted in **Annexure 7** format.
5	The bidder should have Banks/ Financial Institutions as their clients for IS Audit. The bidder must have completed comprehensive System Audit, in last two financial years, for at least One (01) Public Sector Bank in India. (Documentary proofs must be provided as per format given in Annexure-3 along with copies of Work Order etc.).	Copy of Purchase Order & Letter of Confirmation/ Client Certification from the Bank to be enclosed.
	Bidder complies with all Laws, Rules, Regulations, Bye-Laws, Guidelines, Notifications etc.	An undertaking in **Annexure-4** Format should be submitted in a Letter Head
	Bidder shall also submit an undertaking for undertaking IS Audit Assignment.	An undertaking in **Annexure-5** Format should be submitted in the company letter head
	Bidder must be generally complying with Pre-Contract Integrity Pact**.**	An undertaking in **Annexure-6** Format should be submitted in the company letter head.
6	To ensure audit independence, the bidder should not have been a vendor/Consultant of IT equipment/ peripherals/ software/Services to UCO Bank in the past 3 years.	A Self Declaration to this effect on the company letter head to be submitted
7	The bidder should not have been blacklisted by any Public Sector Bank/ICAI. A declaration to this effect must be submitted by the bidder.	A Self Declaration to this effect in the company letter head to be submitted
11	The Bidder should be an empanelled Security Auditing Firm with CERT-In as on RFP publication date and also during the course of Audit.	Relevant Certificate in this regard to be submitted.
12	The Bidder must be an Indian firms **or Company** to be eligible to participate in the tendering process	**---**

ANNEXURE-2: GENERAL DETAILS OF THE BIDDER

(Ref: RFP _____dated_____for IS Audit)

A. Profile of Bidder

1. Name of bidder:
2. Location
   Regd. Office:
   Controlling Office:
3. Constitution
4. Date of incorporation & Date of Commencement of business:
5. PAN No :
6. Major change in Management in last three years
7. Names of Banker/s

B. Financial Position of Bidder for the Last three Financial years

	2014-15	2015-16	2016-17
Turn over			
Net Profit			

N.B. Enclose copies of Audited Balance Sheets along with enclosures

C. Proposed Service details in brief

- Description of service:
- Details of similar service provided to banks in India specifying the number of Banks and branches
  - In PSU banks
  - In non-PSU banks

Details of Experience in implementation of similar orders

(i)

PSU		
Name of Bank	Period	
	From	To

(ii)

Non-PSU		
Name of Bank	Period	
	From	To

N.B. Enclosed copies of Purchase Orders as references.

Signature of Bidder: _____
Name: _____
Business Address: _____

Place:
Date:

ANNEXURE-3: REFERENCES OF IS AUDITS COMPLETED FOR BANKS.

(Ref:- RFP _____dated_____for IS Audit)

(The details of each assignment should be furnished on a separate page. The details should relate to the assignments completed during the past two years. We expect four or five references in the minimum)

1	Name of the Bank	
2	Address	
3	Name of the Contact Person	
4	Designation	
5	Direct Phone number	
6	Mobile Phone	
7	E-mail id	
8	Month & Year in which IS Audit was conducted	
9	Names of professional personnel who carried out that assignment	
10	Brief particulars of the Systems for which IS audit was done.	

(Signature of Authorized Signatory with seal)

ANNEXURE-4: GENERAL DECLARATION-CUM-UNDERTAKING

(TO BE EXECUTED ON NON-JUDICIAL STAMP PAPER OF REQUISITE VALUE)

To

UCO Bank
Head Office
…… Department
Add:-……

Sub: Declaration-Cum-Undertaking <u>regarding compliance with all statutory requirements</u>

In consideration of UCO Bank, a body corporate, constituted under Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 as amended from time to time having its Head Office at 10, Biplabi Trailokya Maharaj Sarani, Kolkata-700001 (hereinafter referred to as "Bank" which expression shall include its successors and assigns), we, M/s……., having its Registered Office at……, do hereby, having examined the RFP including all Annexure, confirm and agree to comply with all Laws, Rules, Regulations, Bye-Laws, Guidelines, Notifications etc.

We do also hereby irrevocably and unconditionally agree and undertake to save and keep the Bank, including its respective directors, officers, and employees and keep them harmless from and against any claim, demand, losses, liabilities or expenses of any nature and kind whatsoever and any damage caused from and against all suits and other actions that may be instituted taken or preferred against the Bank by whomsoever and all losses, damages, costs, charges and expenses arising out of non-compliance with or non-adherence to any statutory/regulatory requirements and/or any other law for the time being in force.

Dated this _____ day of _____,20 _____ .

Place:

For M/s. ……
……

[Seal and Signature(s) of the Authorized Signatory (ies)]

ANNEXURE-5: UNDERTAKING BY THE BIDDER FOR TAKING UP IS AUDIT ASSIGNMENT

To,

The Asst. General Manager
UCO Bank,
Head Office,
Audit & Inspection Department (1st Floor)
10, B. T. M. Sarani
Kolkata- 700 001

Dear Sir,

Re: Our Request For Proposal (RFP) for Information Systems Security audit of UCO Bank

(Ref:- RFP _____dated_____)

a) We hereby confirm that we have read and understood the eligibility criteria and we fulfill the same.

b) We further confirm that all the information as per requirement of the Bank have been included in our RFP.

c) Further, we hereby undertake and agree to abide by all the terms and conditions and guidelines stipulated by the Bank. We understand that any deviation may result in disqualification of our RFP.

d) We have not been blacklisted by any Public Sector Bank/ RBI/IBA or any other Government agency/ICAI. No legal action is pending against us for any cause in any legal jurisdiction.

e) We undertake that adequate number of qualified auditors will be deployed for audit process to complete the audit within stipulated time.

f) We undertake that we will have legal right to use any third party software if required for audit and under such licenses, in terms set out under any relevant license or sublicense agreement. We will indemnify the Bank for any and all costs that may arise out of the use of software, in which it is alleged that any rights of the owners of such software have been infringed.

(Signature and the capacity of the person duly authorized to sign Bid for and on behalf of)

ANNEXURE-6: PRE-CONTRACT INTEGRITY PACT

(to be stamped as per the Stamp Law of the respective State)

General

This pre-contract Agreement (hereinafter called the Integrity *Pact)* is made on……..day of the month of……, 20___between, on one hand UCO BANK, a body corporate constituted under The Banking companies (Acquisition & Transfer Act of 1970), as amended by The Banking Laws (Amendment) Act, 1985, having its Head Office at 10, Biplabi Trailokya Maharaj Sarani , Kolkata-700001 {hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s……..represented by Shri……..,…… (hereinafter called the "BIDDER/Seller" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to **avail**/procure (Name of the Stores/Equipment/item/ **Services**) and the BIDDER/Seller is willing to offer/has offered the the Stores/Equipment/item/ **Services** and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a ……Department performing its functions on behalf of UCO BANK.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to :-

Enabling the BUYER to obtain the desired said stores/equipment/Services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling BIDDERS to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:
Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will, during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

Commitments of BIDDERS

3. The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Government.

3.3 BIDDERS shall disclose the name and address of agents and representatives and Indian BIDDERS shall disclose their foreign principals or associates.

3.4 BIDDERS shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has

any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the

BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender. The term relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

3.13 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER'S exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5. Earnest Money (Security Deposit)

5.1 While submitting the bid documents, the BIDDER shall deposit an amount (to be specified in RFP) as Earnest Money/Security Deposit, with the BUYER through any of the following instruments:

i. Bank Guarantee in favour of UCO Bank, 10 B.T.M Sarani, Kokata;
ii. A confirmed guarantee by an Indian Nationalised Bank (other than UCO Bank), promising payment of the guaranteed sum to the BUYER on demand of UCO Bank within the time mentioned by UCO Bank without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.
iii. Any other mode or through any other instrument (to be specified in the RFP).

5.2 The Earnest Money/Security Deposit shall be valid upto a period of **180 days** together with a **claim period of 30 days**.

5.3 In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact

5.4 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required:-

i. To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.
ii. The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.
iii. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.
iv. To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Base Rate of UCO Bank, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.
v. To en-cash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.

vi. To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

vii. To debar the BIDDER from participating in future bidding processes of the UCO Bank for a minimum period of five years, which may be further extended at the discretion of the BUYER.

viii. To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

ix. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.

x. Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be-entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fall Clause

The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission.

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

8.6 The BIDDER (s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER 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 shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

8.7 The BUYER 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 parties/The parties will offer to the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of BUYER/'Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic Situations.

9. Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 3 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, whichever is later. In case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

12.2 Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The parties hereby sign this Integrity Pact at —----------on----------.

BUYER	**BIDDER**
Name of the Officer Authorized Signatory Designation Deptt	Name of the Officer Authorized Signatory Designation Deptt
Witness	**Witness**
1.	1.
2.	2.

ANNEXURE-7: PROFILE OF THE PROPOSED CORE AUDIT TEAM FOR THIS ASSIGNMENT

(Ref: - RFP _____dated_____for IS Audit)

Sl. No.	Name of Proposed Auditor	Professional Qualifications/ Certifications	Role in IS Audit (Task/ Module)	Banking Solutions expertise	IS Audit Expertise in terms of years and areas of expertise	Number of similar assignments involved in Banks in India (Provide details)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

(Signature and the capacity of the person duly authorized to sign Bid for and on behalf of)

ANNEXURE-8: CV OF CORE AUDIT TEAM MEMBER

(Ref: - RFP _____dated_____for IS Audit)

(To be furnished on a separate sheet for each Team member)

Name of Staff			
Date of Birth			
Professional Qualifications/ Certifications			
Services in the firm from			
Previous employment record	Organization	From	To
Activities carried out			
Details of key assignments handled in the past three years			
Organization	Month and year	Details of assignment carried out	

ANNEXURE-9: TECHNICAL BID

(Ref: - RFP _____dated _____for IS Audit)

Sl. No.	Particulars	Compli-ance Yes/No
1	The bidder has at least 10 resources on its payroll having requisite experience of conducting any areas of the Audit as per the scope of RFP. The auditing team should be a mix of (CISA or DISA) and (CISSP or CISM) and CEH certified (Certificate to be valid as on date) required to conduct IS audit as per the Scope. ➢ The list of the Audit Team members to be enclosed in **Annexure 7.** ➢ CV of Core Audit team members for UCO Bank to be enclosed in **Annexure 8.**	
2	The Core Team/Resources earmarked for conducting audit for UCO Bank must have experience in relevant fields covering the Scope of Work for at least 2 years.	
3	At least one auditor who is earmarked for Conducting audit for UCO Bank, for any area of the Scope of audit of the RFP must be a **permanent employee of the bidder**. (documentary proof must be attached)	
4	The resources earmarked for Penetration testing/Vulnerability & Threat Assessment are highly skilled & experienced ethical hackers certified in CEH certification.	
5	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Source Code Audit as per the Scope of this RFP	
6	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Application Audit as per the Scope of this RFP	
7	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting VA/PT & Threat Assessment as per the Scope of this RFP	
8	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Process, Site & Infrastructure Audit as per the Scope of this RFP	
9	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Operating System (OS) Audit as per the Scope of this RFP	
10	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Database Audit as per the Scope of this RFP	
11	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Network Architecture and Firewall Rule Audit as per the Scope of this RFP	
12	The bidder/auditor to be deployed for UCO Bank must have at least two years experience in conducting Cyber Security Audit as per the Scope of this RFP. The auditing team should be CISSP or CISM certified.	
13	All the audit activities, methodology, approach & tools to used by the bidder complies with RBI guidelines, IT act 2000, 2008 & other applicable regulations.	

Note: Documentary proof for all the above mentioned points is mandatory.

We have noted all the terms & conditions mentioned in the RFP document, evaluation of Technical Bid for the purpose of offering this Technical Bid. We agree to the terms contained in the RFP document and submit our Technical Bid contained hereinabove.

Date: / / (Signature of Authorized Official)

ANNEXURE-10: COMMERCIAL BID

(Ref: - RFP _____dated _____for IS Audit) **Amount in Rs**

Srl No	Particulars	Amount including all expenses excluding GST (A)	GST as per the current rate applicable (B)	Amount (C)= (A)+(B)	Frequency per Year (D)	Total amount (E)= ((C) x (D) x 3) for Three years
1.	Fees for Process & Site audit defined under **Scope of Work** in the RFP (Inclusive of all fees & expenses)				**Once in a year** (Conduct of Audit & Compliance Review)	
2.	Fees for Application Controls Audit defined under **Scope of Work** in the RFP (Inclusive of all fees & expenses)				**Once in a year** (Conduct of Audit & Compliance Review)	
3.	Fees for Network architecture Review/Audit defined under **Scope of Work** in the RFP (Inclusive of all fees & expenses)				**Once in a year** (Conduct of Audit & Compliance Review)	
4	Fees for Firewall Rule base Review/Audit defined under **Scope of Work** in the RFP (Inclusive of all fees & expenses)				**Quarterly** (Conduct of Audit & Compliance Review)	
5	Fees for Penetration Testing defined under **Scope of Work** in the RFP (Inclusive of all fees & expenses) (20 to 25 IPs/URLs)				**Quarterly** (Conduct of Audit & Compliance Review)	
6	Fees for Vulnerability Assessment defined under **Scope of Work** in the RFP (Inclusive of all fees & expenses) (350 to 375 Servers/Devices)				**Quarterly** (Conduct of Audit & Compliance Review) (However, VA for Critical Public facing Routers/Servers/Devices to be done on monthly basis e.g. e-Banking, m-Banking). **Approx:** 20-25 Devices	
7	Source Code Audit (20 to 25 In-house Developed packages)				**Once in a year** (Conduct of Audit & Compliance Review)	
8	Operating System Audit (350 to 375 Servers/Devices)				**Once in a year** (Conduct of Audit & Compliance Review)	
9	Database Audit (All Major Applications listed in the Scope of Work) (approx 25 to 30)				**Once in a year** (Conduct of Audit & Compliance Review)	
10	A detailed Gap Analysis Report on Security maturity Level against international standards like ISO etc. of the bank.				**Once in a year** (Conduct of Audit & Compliance Review)	
11	**TOTAL COST OF AUDIT** (1+2+3+4+5+6+7+8+9)					

(TOTAL AMOUNT IN WORDS: - Rupees)

Note: Any new addition/up-gradation in sites, hardware, software, new deliverables, and change in architecture or due to regulatory requirement as per the Scope of Work, during the period of Audit must also be covered in the scope of this audit without any additional cost to the bank.

We have noted all the terms & conditions mentioned in the RFP document for the purpose of offering this Bid. We agree to the terms contained in the RFP document and submit our Commercial Bid contained hereinabove.

Date: / / (Signature of Authorized Official with Seal)

Note:--

- The Commercial Bid should contain the Total Project cost, on a fixed cost Basis. UCO Bank will neither provide nor reimburse any expenditure towards any type of Accommodation, Travel Ticket, Airfares, Train fares, Halting expenses, Transport, Lodging, Boarding etc.
- The prices quoted above should be inclusive of all taxes as applicable except GST.
- L1 Bidder will be decided on the Total Professional Fee mentioned under Sl. No. 10 hereinabove.
- Providing commercial proposal in other than this format may lead to rejection of the bid.
- The fees amount submitted against each line-item will be frozen for three years (period of empanelment)
- Bank may decide not to conduct a particular type of audit in a particular year. The decision in this matter will be entirely with the bank.

ANNEXURE-11: COMMERCIAL OFFER UNDERTAKING

To,

The Asst. General Manager
UCO Bank,
Head Office,
Audit & Inspection Department (1st Floor)
10, B. T. M. Sarani
Kolkata- 700 001

Dear Sir,

Sub: **Commercial Offer in response to your RFP _____dated_____for IS Audit**

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

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

We also confirm that the **prices offered shall remain fixed for a period of 180 days from the date of submission of the offer**.

We also understand that the **Bank is not bound to accept the offer either in part or in full**. If the Bank rejects the offer in full or in part the Bank may do so without assigning any reasons therefore.

Yours faithfully,
Authorized Signatories

(Name, Designation and Seal of the Company)
Date:

ANNEXURE-12: TECHNO COMMERCIAL BID UNDERTAKING

Ref. No: **Date:**

To

The Asst. General Manager
UCO Bank,
Head Office,
Audit & Inspection Department (1st Floor)
10, B. T. M. Sarani
Kolkata- 700 001

Having examined the RFP ref no _____date _____including all Annexure, the receipt of which is hereby duly acknowledged, we the undersigned, offer to deliver the services in conformity with the said RFP in accordance with the Schedule of Prices indicated in the Commercial Offer and made part of the Bid.

We undertake, if our bid is accepted, to deliver the services/goods in accordance with the delivery schedule specified in schedule of requirement.

We agree to abide by this bid for the period of 180 days after the date fixed for Technical bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "**Prevention of Corruption Act 1988**".

We understand that the Bank is not bound to accept the lowest of any bid the Bank may receive.

We further understand that the **finalized prices will be frozen for a period of three years** from the date of entrustment of assignment/empanelment and that the Bank, at its discretion may entrust the assignment again in full or parts at the same price and terms as per its requirements.

Dated this _____ day of _____ 2018.

(Signature) (In the Capacity of)

Duly authorized to sign bid for and on behalf of

(Name & Address of Bidder) _____

ANNEXURE-13: EARNEST MONEY FORM (BG)

(FORMAT OF BANK GUARANTEE (BG) FOR EARNEST MONEY)
(ON A NON-JUDICIAL STAMP PAPER OF RS. 100.00)

To,

BG No: BG Date: BG Amount: Expiry Date:

The Asst. General Manager
UCO Bank,
Head Office,
Audit & Inspection Department (1st Floor)
10, B. T. M. Sarani
Kolkata- 700 001

Dear Sir,

In response to your invitation to respond to your RFP under Ref. No. _____dated _____ for Selection of Information System Security Auditor, 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 Selection of Information System Security Auditor and to provide related services as listed in the RFP document.

Whereas the 'Bidder' has submitted the proposal in response to RFP, we, the _____ (name of Guarantor Bank) hereby irrevocably guarantee an amount of `_____ (Rupees _____) as bid security as required to be submitted by the 'Bidder' 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 UCO Bank, during the period of 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 if any;

We undertake to pay immediately on demand to UCO Bank the said amount of `_____ (Rupees _____) 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 UCO Bank 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`_____ (Rupees_____).
2. This Bank Guarantee will be valid up to _____ (**last date of bid submission plus six calendar months**) and
3. We are liable to pay the guarantee amount or any part thereof under this Bank Guarantee only upon service of a written claim or demand by you on or before _____.
4. Our liability under this agreement shall not be affected by any infirmity or irregularity on the part of the 'Bidder' in bidding for the said work or their obligations there under or by dissolution or change in the constitution of the 'Bidder'.

In witness whereof The Bank, through the authorized officer has sets its hand and stamp on this day of _____ at _____.

For and behalf of _____
(Authorized Signatory with seal)

ANNEXURE-14: PERFORMANCE BANK GUARANTEE FORMAT

(PERFORMANCE GUARANTEE FORMAT)
(ON NON-JUDICIAL STAMP PAPER OF RS 100.00)

Bank Guarantee No. Date:

To,

UCO Bank

Kolkata, India

WHEREAS _____ (name of the Vendor) hereinafter called "the Bidder" or "the Vendor" has undertaken, in pursuance of Purchase Order No. dated 20____ to conduct Information Systems Security Audit in UCO Bank, hereinafter called "the order".

AND WHEREAS it has been stipulated in Conditions of Bidding in the Request for Proposal (RFP), the BIDDER/VENDOR is required to furnish, a Bank Guarantee by way of Performance Guarantee issued by a Scheduled Commercial Bank in India, in your favour, as per 3.4, Section III of the RFP, to secure due and satisfactory compliance of the, obligations by the BIDDER/VENDOR on their part, in accordance with the AGREEMENT,(which guarantee is hereinafter called as "the PEMORMANCE GUARANTEE,')

AND WHEREAS VENDOR has approached us (Name & address of the Bank issuing Performance guarantee) (hereinafter referred to as "_____Bank, _____Branch" which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns), for PERFORMANCE GUARANTEE

AND WHEREAS in consideration ---------- and the fact that the VENDOR has entered into the Agreement with you, WE _____Bank _____Branch, have agreed to issue the PEMORMANCE GUARANTEE in your favor.

THEREFORE WE _____Bank _____Branch, furnish you the PERORMANCE GUARANTEE in manner hereinafter contained and agree with you as follows:

We _____Bank _____Branch, undertake to indemnify you and keep you indemnified form the time to time to the extent of Rs._____ (Rupees _____ only) an amount equivalent to 10 % of the order/contract Value against any loss or damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of the VENDOR of any of the terms and conditions contained in the agreement and in the event of the VENDOR default or defaults in carrying out any of the work or discharging any of their obligations under the AGREEMENT or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof, we shall forthwith on demand pay to you such sum or sums not exceeding the sum of Rs. _____(Rupees _____ only) as may be claimed by you on account of breach on the part of VENDOR of their obligations in terms of the Agreement.

Notwithstanding anything to the contrary we agree that your decision as to whether the VENDOR has made any such default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you

the reason of or to establish your claim or claims under Performance Guarantee but will pay the same forthwith on your demand without any protest or demur.
This performance Guarantee shall continue and hold good until it is released by you on the application by the VENDOR after the expiry of the relative guarantee period of the contract and after the VENDOR had discharged all his obligations under the agreement and produced a certificate of due completion of the work under the Contract and submitted a "No Demand Certificate" provided always that the guarantee shall in no event remain in force after the date hereinafter mentioned without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the **expiry of three months from the said date** which will be enforceable against us notwithstanding that the same is or are enforced after the date of expiry of the guarantee or the extended period of guarantee hereinafter mentioned.

Should it be necessary to extend Performance Guarantee on account of any reason whatsoever, we undertake to extend the period of Performance Guarantee on your request under intimation to the VENDOR till such time mutually agreed by you with the VENDOR.

You will have the fullest liberty without affecting Performance Guarantee from time to time to vary any of the terms and conditions of the Agreement or extend the time of performance of the Contract or to postpone any time or from time to time any of your rights or powers against the VENDOR and either to enforce or forbear to enforce any of the terms and conditions of the Agreement and we shall not be released from our liability under Performance Guarantee by the exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the VENDOR or any other forbearance, act, or omission on your part of or any indulgence by you to the VENDOR or by any variation or modification of the Agreement or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will extend our liability hereunder beyond the limit of Rs, _____ (Rupees_____ only) as aforesaid or extend the period of the guarantee beyond the date hereinafter mentioned.

The Performance Guarantee shall not in any way be affected by your taking or giving up any securities from the VENDOR or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the VENDOR.

In order to give full effect to the guarantee herein contained, you shall be entitled to act as if we were 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 any of the provisions of Performance Guarantee.

Subject to the maximum limit of our liability as aforesaid, Performance Guarantee will cover all your claim or claims against the VENDOR from time to time arising out of or in relation to the Contract and in respect of which your claim in writing is lodged on us before expiry of three months from the date of expiry of the Performance Guarantee or the extended period of the Performance Guarantee hereinafter mentioned.

Any notice by way of demand or otherwise hereunder may be sent by special courier, fax or registered post to our local address as aforesaid and if sent by post it shall be deemed to have been given when the same has been posted.

The Performance Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees heretofore given to you by us (whether jointly with others or alone) and now existing uncancelled and that Performance Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.

The Performance Guarantee shall not be affected by any change in the constitution of the VENDOR or us nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will endure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.

The Performance Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during the currency including the extended period of the Performance Guarantee without your previous consent in writing.

We further agree and undertake to pay you the amount demanded by you in writing irrespective of any dispute or controversy between you and the VENDOR and we shall not raise any issue on such dispute or controversy for any reason whatsoever.
Notwithstanding anything contained herein

i. Our liability under this guarantees hall not exceed Rs._____(Rupees_____ only)

ii. This guarantees shall be valid up to _____

iii. We are liable to pay the guaranteed amount or any part thereof under this guarantee only and only if you serve upon us a written claim or demand at _____ within the validity period of the Performance Guarantee or the extended period of the Performance Guarantee.

Dated this _____ day of _____ 20__.

For and behalf of _____
(Authorized Signatory with seal)

(Signature of Authorized Signatory with seal)

ANNEXURE-15: PROPOSED METHODOLOGY & WORK PLAN
(Ref: - RFP _____dated_____for IS Audit)

Please mention the details of tasks you propose to do along with the estimates of time lines for each task, the key personnel you intend to engage for each of the tasks in the assignment and the deliverables for each task. In other words, this sheet should provide the entire Project Plan

Sl. No.	Details of tasks	Estimated Time lines	Methodology Used	Details of Key Personnel to be engaged	Deliverables

Note:

1. Additional Columns (on the right side of the table) may need to be provided for additional information as per the requirement of the bank.
2. The Methodology to be used for Conduct of IS Audit as per scope of work & as per the Board Approved Bank's Policy is to be submitted as a document by the bidder. The empanelment of the bidder, who is issued the work order, shall discuss the Methodology with bank before conduct of Audit.

(Signature of Authorized Signatory with seal)

ANNEXURE-16: PREVIOUS AUDIT COMPLIANCE REPORT

(ON BIDDER'S OFFICIAL LETTER HEAD)

(Ref: RFP _____dated_____for IS Audit)

CERTIFICATE

We certify that Mr./Ms._____CISA/CISSP/CCNA/CISM/ auditor from M/s. _____ (name of the Audit Firm) has verified the controls not implemented in the previous IS Audit of 2016-17 in various audit areas/Units. We further certify that except the following controls, all the controls are implemented by the Bank as on the date of present audit.

Place:
Date:

Signature of Authorized Signatory
Name:
Designation:
Organization Seal:

Controls which are still pending from the previous audit conducted during 2016-17

Audit Units/Areas	Controls not implemented as on the date of previous Audit (Mention date)	Controls implemented as on the date of present Audit (Mention Date)	Controls still pending as on Date (Mention Date) *

**** Details are to be given in Annexure- 17**

ANNEXURE-17: PREVIOUS AUDIT COMPLIANCE FORMAT

(Ref: RFP _____dated_____for IS Audit)

RISK ASSESSMENT OF CONTROLS WHICH ARE STILL PENDING (IF ANY) FROM THE PREVIOUS AUDIT

Sl. No.	Audit Unit/ Application/ Area	Description of Pending Control	Risk Category	Potential Impact	Comments by the Auditee dept. for non implementation	Risk Mitigation Strategy / Auditor's Recommendation

(Note: Number of Columns (on the right side of the table) may be increased to include additional Information**)**

Place: Signature of Authorized Signatory

Date:

Name:

Designation:

Organization Seal:

ANNEXURE-18: CHECKLIST FOR DOCUMENTS TO BE SUBMITTED

(Ref: RFP _____dated_____for IS Audit)

The Firms who are submitting the RFP are requested to fill this checklist and also to ensure that the details/ documents have been furnished as called for in this bidding document.

Please tick the Yes/No box for details furnished in the RFP and enclose the documents in the given order in your technical offer.

Sl. No.	Items	Remarks	Yes/No
1	Cost of Tender Document	Rs.5,000/- in the form of DD/PO	
2	EMD (Earnest Money Deposit)	Rs. 1,00,000/- in form of Bank Guarantee (Annexure-13)	
3	Table of Contents (List of documents enclosed)		
4	Eligibility Criteria & General Details of the bidder	As per Annexure-1 & 2	
5	Covering Letter in Bidder's Letter head duly signed by Authorized signatory	As per Annexure-3	
6	Letter of Authorization of Authorized signatory from the competent authority		
7	Technical Bid Techno Commercial Bid Undertaking	As per Annexure-9 As per Annexure-12	
8	Commercial Bid Commercial Offer Undertaking	As per Annexure–10 As per Annexure-11	
9	Certificate of Cert-in Empanelment		
10	Bidder's Undertaking for taking up Audit Assignment	As per Annexure–5	
11	Pre-Contract Integrity Pact	As per Annexure–6	
12	General-Declaration-Cum-Undertaking	As per Annexure–4	
13	References of IS Audits completed for Banks	As per Annexure-3	
14	Satisfactory proof of conducting similar comprehensive Information Systems Security Audit in at least two **Indian Public Sector Bank.**		
15	Details of the bidder's proposed Audit Plan, methodology/approach & Work Plan for providing services to the Bank with specific reference to the scope of work.	As per Annexure–15	
16	Proposed Core Audit Team Profile (Resume of the Core Audit Team with Name, Designation, qualification & experience details) CV of Core Audit Team Members	As per Annexure–7 As per Annexure–8	