

Selection of IS Audit Firms/Organizations for Information Systems Audit

ADDITIONAL TERMS AND CONDITION (ATC)

All the clauses mentioned in this Additional Terms and Conditions (ATC) document will be integral part of the bid document. In case of any contradiction or conflict of interest the terms and conditions, eligibility criteria and technical compliance as mentioned in ATC document will prevail.

ABBREVIATION

The long form of some abbreviations commonly used in the bid is given below:

Abbreviations	Description
AMC	Annual Maintenance Contract
ATS	Annual Technical Services
BG	Bank Guarantee
BOM	Bill of Material
DD	Demand Draft
DIT	Department of Information Technology
EMD	Earnest Money Deposit
EOD	End of Day
EOL	End of Life
EOS	End of Support/Sell
FMS	Facility Management Services
GST	Goods and Service Tax
HO	Head Office
IT	Information Technology
KYC	Know Your Customer
LD	Liquidated Damage
MSE	Micro & Small Enterprise
MSME	Micro Small & Medium Enterprises
NBFC	Non-Banking Financial Company
NDA	Non-Disclosure Agreement
NEFT	National Electronic Funds Transfer
NI Act	Negotiable Instruments Act
OEM	Original Equipment Manufacturer
OSD	Original Solution Developer
PBG	Performance Bank Guarantee
PO	Purchase Order

POBO	Payments-on-behalf-of
RBI	Reserve Bank of India
RTGS	Real Time Gross Settlement
RTO	Recovery Time Objective
SB	Successful Bidder
SLA	Service Level Agreement
SP	Service Provider
TAT	Turn Around Time
TCO	Total Cost of Ownership
UDIN	Unique Document Identification Number
UMRN	Unique Mandate Reference Number
UPI	Unified Payments Interface
UTR	Unique Transaction Reference



PART-I

1. Introduction

UCO Bank, a body Corporate, established under The Banking Companies (Acquisition and Transfer of Undertakings) Act 1970, having its Head Office at 10, B.T.M. Sarani, Kolkata- 700001, India, hereinafter called "The Bank", is one of the leading public sector Banks in India having more than 3300+ Domestic Branches, two Overseas Branches one each at Singapore & Hong Kong Centres. All the branches of the Bank are CBS enabled through Finacle 10. x as a Core Banking Solution.

2. Overview And Objective

UCO Bank intend to on-board two Cert-in empaneled Auditor for conducting different IS Audit work during 2 years (2025 to 2027). In this regard, Bank invites tenders comprising of eligibility, technical bid and Commercial bid from prospective bidders having proven capabilities of IS/IT Audit functionalities. Bank intends to select a bidder who has expertise in IT and Business understanding related to financial sector. The prospective bidders are required to adhere to the terms of this RFP document and any deviations to the same shall not to be acceptable to UCO Bank.

The bidder (also called the vendor or bidder through this document) appointed under the RFP document shall own the single point responsibility for fulfilling all obligations and providing all deliverables and services required for successful implementation of the project. Unless agreed to specifically by the Bank in writing for any changes in the document issued, the bidders responses should comply with the scope of work.

3. Eligibility Criteria

Sl. No.	Criteria	(Proof of documents required / must be submitted)
1.	Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on bid submission date. or Registered as a partnership firm (registered under section-59 of the Partnership Act, 1932) or	1. Copy of Certificate of Incorporation issued by Registrar of Companies, Shareholding pattern, Copies of MOA and AOA (For Companies). 2. Copy of LLP Incorporation certificate. In case of partnership firms, Deed of Partnership should be submitted. 3. Shareholding pattern (For Companies and LLPs) 4. PAN, TAN, GSTIN Certificate and any other tax related document

	A limited liability partnership (under the Limited Liability Partnership Act, 2008) in India	if applicable is required to be submitted along with the eligibility bid.
2.	The bidder should have a minimum annual turnover of Rs. 2.5 Crore per year during the last three financial years i.e. 2021-22, 2022-23 & 2023-24. This must be the individual company turnover and not of any group of companies.	Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing profit, net worth and turnover of the company for the consecutive last three financial years i.e., 2021-22, 2022-23 & 2023-24 should be submitted.
3.	Bidder should have maintained a Positive Net-Worth during the last three financial years i.e. 2021-22, 2022-23 & 2023-24	Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing profit, net worth and turnover of the company for the consecutive last three financial years i.e. 2021-22, 2022-23 & 2023-24 should be submitted.
4.	The bidder should be an empaneled Security Audit Firm with CERT-IN as on bid submission date.	Copy of valid CERT-IN certificate.
5.	The bidder must be having core audit team of minimum 20 members having permanent employees who hold Industry Standard Certifications CISA/ DISA/ CISSP/ CEH/ CISM/ CA (valid as on date) and requisite experience (minimum 3 years) to handle the work as per the scope.	The profile of the Core Audit team must be submitted as per format given in Annexure – XIV and Annexure XV. Respective professional certificates to be submitted.
6.	<p>Bidder should have industry-wide presence and expertise in conducting Information Systems (IS) Audit including VA-PT, Business understanding related to Banking sector, good track record and must have prior experience of conducting such audit/ special audit, mentioned below, of any Bank in India (SCBs, SFBs, Payment Banks) in last 5 years.</p> <p>The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last two</p>	<p>Documentary proof must be provided along with copies of Work Order clearly mentioning the areas of IS Audit, IT Audit completed/covered in the audit work.</p> <p>Apart from above, relevant copy of any one of the following is to be submitted:</p> <ol style="list-style-type: none"> 1. Completion Certificates 2. Project Sign-Offs 3. Satisfactory client certificate <p>The firm must submit a self-declaration that the members of core team has</p>

	<p>financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India.</p> <p>The bidder should have conducted Audit in following at least 10 areas out of 16 areas: -</p> <ol style="list-style-type: none"> 1. Process Audit of Banking operations 2. VA/PT Capabilities 3. Source Code Audit 4. Application Audit 5. Network Audit 6. Audit of Security devices available at SOC 7. Database Management System Audit 8. IT/Digital/Information Security Governance and Management 9. Data Centre, Disaster Recovery Centre Audit 10. Business Continuity Audit 11. Data Security Audit 12. Reconciliation of Banking Payment Systems 13. Assessment of Banking applications mapped to their corresponding business logic & relevant regulatory guidelines. 14. Cloud Audit 15. SWIFT Audit 16. Migration Audit <p>The experience in aforesaid areas should be from either one or multiple Public / Private Sector Banks/Payment Banks in India.</p>	<p>participated in the audits as mentioned in scope in last 3 years.</p>
7.	<p>Bidder should not have conflict of interest in carrying out the Audit. i.e. The firm should not have been engaged with the Bank in any form either direct or indirect assignment except concurrent audits in the past two years as on date of bid submission.</p>	<p>Undertaking on company letterhead mentioning the same should be submitted.</p>
8.	<p>Bidder should have proven methodologies & tools for conduct of audit. Tools should be as Industry Standard and free from bugs and vulnerabilities.</p>	<p>Self-Declaration in format attached – mentioning tool that are free from bugs</p>

9.	The Bidder should not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity as on the date of bid submission	Self-declaration to this effect on the company's letterhead should be submitted
10.	Bidder should submit an Undertaking regarding compliance of all Laws, Rules, Regulations, by-Laws, Guidelines, Notifications etc.	Documentary evidence to be submitted by the bidder as per Annexure – XVI.
11.	Bidder should not have been debarred / black-listed by any Bank or RBI or ICAI or any other regulatory authority or Financial Institutions in India as on date of RFP submission.	Annexure-VI should be submitted
12.	The bidder should ensure that there are no legal proceedings / inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	Self-declaration to this effect on the company's letterhead should be submitted.
13.	Bidders who are party to any ongoing/pending/contemplated litigation with UCO Bank, shall not be allowed to participate in this tender.	A self-declaration to this effect must be submitted along with the technical bid.

Note:

The service provider must comply with all above-mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily. Documentary Evidence for compliance to each of the eligibility criteria must be enclosed along with the bid together with references. Undertaking for subsequent submission of any of the required document will not be entertained under any circumstances. However, UCO BANK reserves the right to seek clarifications on the already submitted documents. Non-compliance of any of the criteria will entail rejection of the offer summarily. Any decision of UCO BANK in this regard shall be final, conclusive and binding upon the service provider.

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



PART-II

Broad Scope of Work

The Bank intends to select CERT-IN empanelled Information Systems (IS) Audit Firms/Organizations to conduct IS Audit and VA-PT at Bank's DC and DR at mentioned locations. The bidder has to complete the audit onsite using proven methodologies & tools for conduct of audit. The bidder has to supply all essential tools for audit and bank will only provide support for its utilization/use. The bidder has to suggest the tool to be utilised in the audit which should be whitelisted and in CertIN site and get it approved by the Bank for its utilization. The tool should be capable to work in VM environment also. The bidder has to ensure that they remain CERT-IN Empanelled IS Audit firm/Organisation throughout the contract period.

During the execution of Audit work, the bidder must station auditor onsite until completion of Audit work and for checking compliance without additional charges to Bank. Remote access will not be given to the vendor. The Bank will only arrange space plan to the auditors.

The bidders selected by the RFP should possess deep understanding of both IT Systems and Banking procedures, allowing them to assess interconnectedness between Bank's Technology and its Financial operations.

Bidder shall be responsible to complete the allocated job and fulfilling all obligations and providing all deliverables and services required for successful completion of the project. Unless agreed to specifically by the Bank in writing for any changes in the document issued, the bidder responses should comply with the scope of work.

The bidder should adhere to the guidelines of RBI, Govt. of India, NPCI, UIDAI, SWIFT, NCIIPC etc. and Bank's internal guidelines during conducting the IS Audit covering the various key areas:

- Preparation of IS Audit Plan in Consultation with concerned Bank officials.
- Defining Checklist for different applications/area of audit in Consultation with the Bank.
- Planning execution of the Audit.
- Conducting the IS Audit.
- Documenting the audit process.
- Report submission to the Bank.
- Conducting the compliance audit.
- Imparting training to Bank's internal audit team on audit areas

Offices/Units covered:

- Data Centers at Bengaluru (Primary site for CBS and non-CBS applications) NOC, SOC at Kolkata.
- Disaster Recovery Sites for CBS applications and non-CBS applications at Kolkata, NDR-Bengaluru.
- Treasury Division, SWIFT Center at Bengaluru/Kolkata/Mumbai.

- Digital Banking Facilities at Bengaluru/Kolkata.
- Bank's CTS Centers at Delhi, Chennai & Mumbai.
- Bank's Contact Centers/ Call Centres at Kolkata/New Delhi/Bengaluru.
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements at Bengaluru/Mumbai/Kolkata /Chennai or any other Bank's office/ Vendors location.
- Other HO divisions/ Service Providers at Bengaluru / Mumbai/ Kolkata/ Chennai or any other Bank's office at any place, where critical application/ IT infrastructure is installed or may be installed in future.
- Locations of Service Providers to whom specific services are outsourced.

Broad Areas of Audit

I. Regular IS Audits:

1. **VULNERABILITY ASSESSMENT (VA)** - Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.
2. **PENETRATION TESTING (PT) (EXTERNAL/INTERNAL)** - Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.)
3. **APPLICATION AUDIT**- Application audit shall be conducted for all applications within the bank.
4. **PROCESS AUDIT** - Process audit must be conducted for Data Centre (DC), Disaster Recovery (DR) Centre and any critical location where our critical IT infrastructure is hosted and Critical IT applications and any new applications before go-live or on major changes.
5. **NETWORK ARCHITECTURE REVIEW** - Network design of critical network architecture and infrastructure performance controls shall be reviewed.
6. **FIREWALL RULE BASED REVIEW** - All the configuration output of the firewall rules shall be captured and studied, policy/rule-wise, manually or using the tools so that any mis-configuration residing may be mitigated.
7. **SOURCE CODE AUDIT/REVIEW** - Source Code Audit or Secure Code Review, as applicable, of inhouse- developed packages or outsourced applications.
8. **DATABASE AUDIT**

9. KRIs and KPIs Prepared by CISO OFFICE

10. **VA/PT OF INTERNET CONNECTED PCs** - VA/PT (Vulnerability Assessment and Penetration Testing) of Internet connected Desktops/ PCs of Corporate Departments.

11. SECURITY AUDIT OF CLOUD SERVICES

12. **PERFORMANCE TESTING** - Load Testing, Stress Testing, Capacity Testing and Spike Testing of Mobile Banking Applications.

13. **AUDIT OF CHANGE LOGS** - Audit of Change Logs refers to the process of reviewing and examining the records that documents changes made to a system, software application, database, or any other type of information system.

14. **VENDOR AUDIT & SITE AUDIT** - Vendor Audit is a process of evaluating and assessing the IT-related practices and controls of a third-party vendor or supplier.

15. **SECURE CONFIGURATION REVIEW/AUDIT** - Secure Configuration Review of Operating System (OS) and Database (DB). Configuration Audit of Servers, Network and Security Devices covering critical Applications, like CBS (domestic and overseas), Mobile Banking, Internet Banking, UPI, GBM, RTGS, NEFT, SWIFT, etc.

16. **GOVERNANCE AUDIT**- A governance audit is an independent review of governance framework, policies, and processes of various departments / verticals across the Bank.

17. **AUDIT OF STORAGE OF PAYMENT SYSTEM DATA** - Bank shall conduct audit to ensure that the entire data relating to payment systems operated by them are stored in a system only in India.

18. SYSTEM AUDIT REPORT (SAR) NSDL

19. IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)

20. **AUDIT OF DIGITAL LENDING** - Periodic validation tests of the algorithm/model used in Business Rule Engine (BRE) – once in six months during the first two years and suggest any remedial measures basis operational audit observations.

21. **CYBER SECURITY FRAMEWORK REVIEW** - As part of IS Audit Program, the adequacy and adherence to the controls of RBI's Cyber Security Framework and other applicable regulatory guidelines.

22. **SWIFT Customer Security Program (CSP) Assessment** - SWIFT Customer Security Controls Framework (CSCF) (latest version – Current version is CSCF - V2025).

23. AUDIT OF VIRTUAL MACHINES (VMs)

24. Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS

25. Audit/Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)

26. Information Security Management System (ISMS) for ISO 27001:2022 Certification

27. Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong

28. MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore

29. Migration Audit

30. Forensic Audit/ Forensic Analysis/Investigations:

31. Security cum functional audit of new applications

II. Security cum Functional Audit:

Security cum Functional Audit will be done before GO-Live for New developed application/ After Major Changes in existing applications (both in-house and developed by external vendors).

Deliverables

Time Lines

- a) Selected IS Auditor will provide schedule of audit like Annual/Quarterly/Special Audit, at least 7 working days prior to start of audit along with full credentials of Audit team (with qualification & experience as defined in RFP) who will be conducting the audit.
- b) Completion of quarterly Process Review Audit, Device Level Audit, VA & PT audit as mentioned above within 18 working days.
- c) Minutes of daily meeting will be prepared by next day where observations are based on discussion and will be signed by all participants.
- d) Giving draft report for discussions with owners within 3 working days after completion of audit.
- e) Discussion of the issues with Divisional Head/owner after 2 working days from date of submission of draft report.
- f) The Security Cum Functional Audits have to be initiated within three days of allotment of audit and completed within 21 working days.

Training

Training to be provided to Bank's officials on half yearly basis.

1. Training is to be given to internal IS Audit team on uses of Tools used for Audit purpose, understanding scripts to be run on server, conducting VAPT, preparation of the Reports based on the identified vulnerabilities (i.e. identifying Risk Impact and Recommendation to mitigate the identified risks).
2. The IS Auditor should explain, to the bank's team all the processes, procedures involved in arriving at audit findings including interpretation of outputs generated by various audit tools.

Reports:

Report should be provided with snap shot / evidence/ documents details from which observation made wherever is easily understood by Bank.

Reporting formats should at the minimum include

- Compliance status of previous quarter report will include observations with status as following- Found complied/ found partially complied/ Found Non-complied/ Exception taken as a separate report.
- Audit report of current quarter with status Repeat/ Exception / New.
- The IS Auditor shall provide different types of reports which would address all issues/observations regarding compliances.
- If repeated – (i) Since when on same server. (ii) Since when on Similar asset.
- If exception– expiry date & authorized by whom.
- Vulnerability ID (Unique identification number (alpha numeric) for each vulnerability and the Identifier should be such that it is Unique for any previous Vulnerability process also.
- Vulnerability Identified (specific to equipment / resources - indicating name and IP address of equipment, Application name where Vulnerability exists and office / department name and should not be generalized).
- Broad domain categorization of activity (Port/SQL Injection/ Services/Physical Access Control/ Logical Access Control/ Environment etc.).
- Risk category & Exploitable status as against –Critical, High, Medium, Low level observations.
- Servers/ Resources affected with IP address.
- Department (in office) to whom the Vulnerability relates.
- Risk / Implication.
- Recommendation for risk mitigation/ removal – step wise. If not resolved, alternate solutions will be provided over phone/ email or personal visits to department if required. Response over phone/ email should come within 4 hours of receipt of request.
- Provision for updating owner's compliance comments.
- Reports should be department wise with brief about Identification of auditee (Address & contact information), Date, location &, time span of audit.
- Explicit reference to key policy and procedure documents of the Bank/RBI against identified risk/observation.
- The reports shall be customized as per the requirements of the Bank.

- Additional mandatory or voluntary standards or regulations applicable to the banking industry as best practices should be reported under "Improvement /suggestions".
- Standards followed
- Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment)
 - a. Tools used b. List of vulnerabilities identified. c. Description of vulnerability d. Test cases used for assessing the vulnerabilities. e. Analysis of vulnerabilities and issues of concern.
- Personnel involved in the audit, including identification of any trainees.
- The various audit reports/ templates should be got integrated with the Bank's ITGRC Application.
- All the reports should contain the URL, IP Address, Application and Server Name, Host Name etc. in respect of the assets which are subjected to Audit.

The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.

MIS:

Successful bidders will use some tools preferably Web Based (cost if any, should be included in audit fee), which shall be capable of providing audit report, and which should support dashboard format (Major gaps with subsequent details through links). It should be capable of presenting reports sorted on following major domains and presentable in pie chart/ graphs/excel sheet. Bank will have the right to use that tool.

Should be able to view/ print report sorted on following:

- Compliance status of previous quarter report –Found Complied/ Found partially complied/ Found Non complied/ Exception taken wise
- Audit report of current quarter with status Repeat/ Exception or New Vulnerability wise.
- Repeated.
- Exceptions.
- Broad domain activity wise.
- Risk category & Exploitable status as against – Critical, High, Medium, Low level observations
- Servers/ Resources affected wise.
- Each server/ resources vulnerability history (activity wise) should be maintained so that trend analysis can be done at any point of time.
- Department wise Vulnerability reports.
- Report showing the major vulnerabilities for a given period of 3, 6 or 12 months for broad domain, server, resources, office, department wise etc.
- Report will be given in editable (Excel) and non-editable softcopy so that editable can be used in updating compliances by User Department
- Report will be given in signed hard copy also.
- Presentation on findings of audit will be given to Management by the Auditor within a week's time of final report submission and should be accompanied by senior consultant for each quarterly audit.

- Any other ADHOC report as per requirement by the Bank.
- Dashboards should be available in respect of the movement of posture of audits during given period based on various parameters.

RISK MOVEMENT:

- Overall risk of each Office – Critical, High, Medium, Low
- Overall risk for Domain and department wise
- Risk movement as compared to previous audits – broad category wise.
- Will maintain history of all previous audit risks scores conducted by successful bidder.

Successful bidder and Auditee will decide Major domains, departments, activities before start of 1st audit based on which report will be prepared. The same can be reviewed whenever there is a change.

Audit Units/Areas:

The Applications/Infrastructure and Site Audit under the IT Universe of the Bank shall include but not limited to the following Audit Units.

1. Governance Audit

A governance audit is an independent review of governance framework, policies, and processes of various departments / verticals across the Bank. It assesses whether the concerned departments / verticals systems are effective in Supporting the organization's mission, mitigating risks, promoting transparency and defining accountability, adhering to laws, regulations, and internal policies (IT Policy, Digital Policy, Cyber Security Policy etc) of the Bank, meeting the regulatory guidelines etc.

2. Process Audit

2.1.1 Process Audit shall cover but not limited to the following units: -

- i. Anti-Money Laundering (AML) – Domestic
- ii. Anti-Money Laundering (AML) - Overseas
- iii. Lending Automation Processing System (LAPS)/Lead Originating (Processing) System (LPS) including STP
- iv. E-KYC/C-KYC authentication infrastructure.
- v. RTGS/NEFT Infrastructure
- vi. Core Banking System (CBS) including Connect 24 Interface and Central Stand in Application Server (CSIS) - Domestic Application
- vii. Core Banking System (CBS) including Connect 24 Interface and Central Stand in Application Server (CSIS)- Overseas Application
- viii. Government Business Module (GBM) (DC & DR)
- ix. Integrated Treasury Management System (ITMS)
- x. LPS/EDPMS/IDPMS/TRACCS
- xi. Alternate Delivery Channels includes
 - **Internet Banking/E Banking (FEBA):**-Shall cover but not limited to the following aspects

- A. Detailed review of the Internet Banking security architecture vis-à-vis the RBI guidelines.
- B. Bank's internet Banking product line, transaction flow, Operational activities.
- C. Review on internal controls & security are in place to minimize errors & frauds.
- D. Interface with other organizations for utility bill payments/share Trading etc.
- E. Interface with CBS & other applications.
- F. Process of creation/Activation/Resetting/delivery of Internet Banking User IDs/ passwords.
- G. Password/PIN management.
- H. Authentication controls.
- I. Two Factor Authentication Solutions for E-Banking.
- J. Information Security Framework.
- K. Web Server
- L. Logs of activity
- M. De-militarized zone & Firewall.
- N. Security reviews of all servers used for Internet Banking.
- O. Database and System administration

➤ **Mobile Banking /UCO mBanking plus/Corporate mBanking Audit:**

Mobile Banking Audit shall cover but not limited to the following aspects

- A. Detailed review of the Mobile Banking Security architecture vis-à-vis the RBI guidelines.
 - B. Bank's Mobile Banking product line, transaction flow.
 - C. Review on internal controls in place to minimize errors & frauds.
 - D. Interface with other organizations for utility bill payments & other purposes etc.
 - E. Interface with CBS, Financial Transaction Switch & other applications.
 - F. Parameterization & customization of Mobile Banking.
 - G. Process of creation/Activation/Resetting/delivery of M- PINS.
 - H. Authentication controls.
- BHIM UCO UPI
 - UCO Secure (Digisafe)
 - mPassbook (Domestic)
 - mPassbook (Singapore)
 - mPassbook (Hongkong)
 - UCO Pay plus
 - Corporate mBanking
 - NPA tracker
 - UCO Cluster
 - UCO Sandeh Nivaran
 - Digilocker
 - Value Added Services (3rd Party) – Trade Market Place, E-Com Market Place, Wealth Management
 - UCO ARBD mobile app

- IMPS
- UPI
- Chatbot (UMA)
- BHIM Aadhaar Pay
- UCO Smart Pay
- Online Fee Collection (In-house & Outsourced) Module.
- Process Audit OTC (One Time Combination) vault opening in Bank's ATM and Cash Recycler.
- Smartpay Fee Collection System.
- Debit Card
- Prepaid Card (Retail)
- Prepaid Card (Corporate)
- Merchant Application for onboarding & Digital payment acceptance hosted at Cloud/ QR Kit/ Sound Box
- Whatsapp Banking hosted at Cloud
- UPI123 hosted at Cloud
- E-Commerce marketplace hosted Cloud
- POS Terminal, Portal/App, Switch, Reconciliation
- MSME Suite
- Micro ATM
- Any Other
- **Automated Teller Machine (ATM)/Cash Recycler & Digital Banking Unit:**
Installed at different locations in Metros, Urban and Rural areas (5 ATM/ Cash Recycler in each location). ATM Centre/Switch Audit shall cover but not limited to the following aspects: --
 - A.** ATM center management: PIN Management, Card Management, Time Management in delivering ATM Card/PIN to Customers and Hot listing of cards.
 - B.** ATM helpdesk and monitoring.
 - C.** Branch procedures.
 - D.** Reconciliation: -Visa, Rupay, POS, NFS, Us-on-Us Chargeback procedures etc. (at ATM Transaction Banking Division, Mumbai/Kolkata).
 - E.** Card Printing/Dispatch, Green PIN Generation through various channels.
 - F.** Instant Debit Card Printer
 - G.** ATM/Prepaid Card Switch setup, configuration, Security, control & Risk Management.
 - H.** ATM Switch operational controls, Consortium issues & Reconciliation/ Functional Managerial activities.
 - I.** Monitoring procedure of ATM's / Cash Recycler Status (Uptime/downtime).
 - J.** Processing of requests received through Debit Card Request (DCR) module in Finacle.
 - K.** Review of EWDIT Software of Euronet.
 - L.** Interface systems (Connect 24, Verified by Visa, Rupay etc.).
 - M.** Offsite Security Services.
 - N.** Status of required certifications as per International as well as regulatory stipulations.

- Bharat Bill Payment System (BBPS) / Bill Desk
- On-Line account opening System
- PFMS (Public Financial Management System)
- Digital Customer Onboarding
- CRM (Customer Relationship Management)
- Micro ATM
- MSME Suite
- Central Bank Digital Currency (CBDC), wallet
- Omni Channel Application
- Any other existing and upcoming applications related to Alternate Delivery Channel

xii. Privacy and Data Protection: Privacy and Data Protection Audit shall cover but not limited to the following aspects:

- A. Controls established for data conversion process.
- B. Information classification based on criticality and sensitivity to business Operations.
- C. Fraud prevention and Security standards.
- D. Isolation and confidentiality in maintaining of Bank's customer Information, documents, records and procedure by banks.
- E. Procedures for identification of owners.
- F. Procedures of erasing, shredding of documents and
- G. Media containing sensitive information after the period of usage.
- H. Media control within the premises.
- I. Compliance with Regulatory/Statutory Data Privacy/Protection/Localization guidelines.

xiii. IT Architecture: IT Architecture shall cover but not limited to 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
- **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

xiv. Security System for Online Card Transaction (SSOCT):

The SSOCT shall cover but not limited to the following aspects

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

xv. Review of IT Processes and IT Management Tools: The review of IT Processes

and Management tools shall cover but not limited to the following aspects:

- A. IT Asset Management
- B. Enterprise Management System
- C. Help Desk
- D. SDLC & Change Management
- E. Incident Management
- F. Network Management
- G. Backup & Media Management
- H. Anti-Virus Management
- I. IT Governance
- J. Implementation of Active Directory & Desktop management.
- K. Vendor & SLA Management
- L. ESCROW Management System
- M. Cyber Security Management Plan.

xvi. IT/Digital/Cyber Security Policies review: An assessment/review of all the important Policies/ Procedure Documents of the Bank such as

- A. Information Technology (IT) Policy
- B. Information Security Policy
- C. Cyber Security Policy
- D. Application Security Policy
- E. Active Directory Policy
- F. ATM Policy
- G. Internet Banking Policy
- H. Vendor and Outsourcing Policy
- I. Cyber Crisis Management Plan Policy
- J. Policy on Document Management System (DMS) Digitization of Critical Records AND Documents
- K. Fintech Policy
- L. Data Privacy and Security Policy
- M. IT Purchase Policy
- N. Hardware Acquisition Maintenance Upgradation Policy
- O. IT Skillset Development Policy
- P. Debit Card Policy
- Q. IT Asset Disposal Policy
- R. Mobile Banking Policy
- S. Network Policy
- T. Prepaid Card Policy
- U. Merchant On-boarding Policy
- V. Digital Banking Outlet Policy
- W. Social Media Policy
- X. Any other policies related to IT/Digital Banking/Cyber Security of the bank which are not listed above.

xvii. Asset Management: Asset Management shall cover but not limited to the following aspects:

- A. Records of assets mapped to owners
- B. For Payment Card Industry (PCI) covered data, the following should be implemented:
 - B.1 Proper usage policies for use of critical employee facing technologies

B.2 Maintenance of Inventory logs for media

B.3 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.

B.4 Review of duties of employees having access to asset on regular basis.

xviii. IT Financial Control Audit: IT Financial Control shall cover but not limited to the following aspects

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

xix. IT Operations Audit: IT Operations shall cover but not limited to the following aspects:

- A. Application Security covering access control
- B. Business Relationship Management
- C. Customer Education and awareness for adaptation of security measures.
- D. Mechanism for informing Banks for deceptive domains, suspicious emails
- E. Trade-marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
- F. Use of Secure Socket Layer (SSL) and updated certification in website
- G. Informing client of various attacks like phishing
- H. Capacity Management
- I. Service Continuity and availability management
- J. Consistency in handling and storing of information in accordance to its classification
- K. Securing of confidential data with proper storage
- L. Media disposal
- M. Infrastructure for backup and recovery
- N. Regular backups for essential business information and software
- O. Continuation of voice mail and telephone services as Part of business contingency and disaster recovery Plans
- P. Adequate insurance maintained to cover the cost of Replacement of IT resources in event of disaster
- Q. Avoidance of single point failure through contingency Planning

R. Service Level Management.

xx. Project Management: Project Management shall cover but not limited to the following aspects:

- A.** Information System Acquisition, Development and Maintenance
- B.** Sponsorship of senior management for development projects
- C.** New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
- D.** Scrambling of sensitive data prior to use for testing purpose
- E.** Release Management
- F.** Access to computer environment and data based on job roles and responsibilities
- G.** Proper segregation of duties to be maintained while granting access in the following environment – Live, Test, Development
- H.** Segregation of development, test and operating environments for software.

xxi. Record Management: Record processes and controls shall cover but not limited to the following aspects:

- A.** Policies for media handling, disposal and transit
- B.** Periodic review of Authorization levels and distribution lists
- C.** Procedures of handling, storage and disposal of information and media
- D.** Storage of media backups
- E.** Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement.

xxii. Technology Licensing: Technology Licensing shall cover but not limited to the following aspects:

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

xxiii. 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.

- A. Compliance:** Assess the third-party's ability/control framework in place to comply with laws/regulations.
- B. Information Security & Privacy:** Assess third party controls over the Availability, confidentiality, and integrity of third party data.
- C. Physical Security:** Assess facility access and security measures implemented by the third party.
- D. Country Risk:** Assess political, geographic, regulatory, legal, and economic risks of sourcing to a country or region.
- E. Business Continuity & Resiliency:** Assess the third parties ability to perform in the event of a process failure or catastrophic event.
- F. Financial:** Assess financial stability for the third party to continue provide the product/service.
- G. Technology:** Assess the adequacy and appropriateness of the third parties systems and applications to provide the

product/service

- H. Subcontractor:** Assess the risk management processes surrounding the use of subcontractors by third parties.
- I. Operational Competency:** Assesses the ability of the third party to deliver the contracted products/services.

xxiv. Business Continuity Management & Cyber Crisis Management:

Business Continuity Management Audit shall cover but not limited to the following aspects:

- A.** Top Management guidance and support on BCP & DRP
- B.** Addressing of HR issues and training aspects
- C.** Providing for the safety and wellbeing of people at branch or location at the time of disaster
- D.** Assurance from Service providers of critical operations for having BCP & DRP in place with testing performed on periodic basis.
- E.** Independent Audit and review of the BCP/DRP and test result
- F.** Participation in drills conducted by RBI for Banks using RTGS/NDS/CFMS Services
- G.** Maintaining of robust framework for documenting, maintaining and Testing business continuity and recovery plans by Banks and Service Providers.
- H.** The BCP methodology covering the following:
 - B.1 Identification of critical business
 - B.2 Owned and shared resources with supporting function
 - B.3 Risk assessment on the basis of Business Impact Analysis ('BIA')
 - B.4 Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO')
 - B.5 Minimizing immediate damage and losses
 - B.6 Restoring of critical business functions, including customer-facing systems and payment settlement systems
 - B.7 Establishing management succession and emergency powers.

xxv. Call Centre Audit: Call Centre Audit shall cover but not limited to the following aspects

- A.** Review of the call center architecture.
- B.** Vulnerability/ Threat Assessment.
- C.** Review on internal controls in place to minimize errors & frauds.
- D.** Manageability of the solution implemented by means of administrative control such as administrative password.
- E.** Adequacy of security features of the application implemented.
- F.** Solution should not breach the security of any other installations of Bank in any way.
- G.** Review of interfaces if any
- H.** Authentication controls.

xxvi. Operating System Audit: The Operating System audit shall cover but not limited to the following aspects for Servers, Databases, Network equipments, Security Systems, Storage Area Networks.

- A.** Set up and maintenance of system parameters.
- B.** Configuration Management

- C. Patch Management
- D. Change Management Procedures
- E. Logical Access Controls
- F. User Management & Security
- G. OS Hardening
- H. Performance, Scalability and Availability

xxvii. Email/Mail Messaging System Audit: The Mail Messaging audit shall cover but not limited to the following aspects:

- A. Overall Mail Messaging System management.
- B. Architecture & design review of Mail Messaging System.
- C. Performance of Mail Messaging Servers.
- D. Archival & Backup process.
- E. Configuration Audit/Hardening review for all servers, network devices (Routers, Firewall, Switches) used in Mail Messaging System.
- F. Impact Analysis of Mail Servers.

xxviii. Risk Based Internal Audit (RBIA) Audit: Risk Based Internal Audit shall cover but not limited to the following aspects:

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

xxix. Maintenance Audit: The IS Asset maintenance shall cover but not limited to 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

xxx. MIS & Automated Data Flow (ADF) Audit:

Audit of Automated Data Flow (MIS-ADF) to RBI shall cover but not limited to the following aspects:

- A. Vulnerability/ Threat Assessment of the Servers and associated Peripherals.
- B. Review of MIS ADF Architecture.
- C. Review of DC-DR Replication.
- D. IS Audit with respect to Data Integrity & Consistency.
- E. Manageability of the solution implemented by means of administrative control such as administrative password.
- F. 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.).
- G. Review of interfaces, particularly with Finacle & others, if any. Authentication controls (OS, Database, Storage and Application Security & Authentication).
- H. Controls for managing change, patch, Source Code and Sensitive DB password.
- I. Controls for performing/changing parameter setup of functionality across applications (also controls for impact analysis of changes made).

xxxi. Cheque Truncation System (CTS) Audit:

CTS at Chennai, Mumbai & Delhi audit shall cover but not limited to the following aspects (Southern, Western & Northern Grids)-

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

xxxii. Security Operating Centre (SOC) – (includes modules viz. WAF, PIMS, DAM, APT, NBA, SIEM, DECOY, ITGRC, NAC, DLP, NPM, VAS, Patch Management Solution, etc.) with ARC Sight as a single Window incident management, ticketing and reporting System. The audit should include Review of rules of SOC Devices/Tools including Arc Sight, DAM etc.

xxxiii. SWIFT Infrastructure, XMM Middleware.

SWIFT Centre Review cover the following aspects

- A. Data Center controls related to SWIFT systems (DC and DR).
- B. Access controls, Authentication framework.
- C. Application Registration Controls

- D. IT Architecture Audit - related to SWIFT Transaction processing
- E. Incident and Change Management
- F. Audit for OS Security baselines and Application Security Controls
- G. Review of Firewall rules and Network security/ Management controls of all other interfacing systems including CBS
- H. Network Security controls of SWIFT infrastructure
- I. Disaster Recovery and Business Continuity Process
- J. Compliance in line with Bank's RTO and RPO
- K. Version Control and Change Management Process
- L. Scalability and Availability
- M. IT Operations for SWIFT related Applications
- N. Log monitoring process pertaining to SWIFT Infrastructure, assurance on log manipulation, Ensure logs cannot be manipulated /deleted by third party including administrator of the system.
- O. Application Security Review of SWIFT Infrastructure
- P. Arrangements for source code review
- Q. Review of Risk Assessment and suggest mitigation measures for the identified service
- R. VAPT of OS, Database and Network devices
- S. Review of SWIFT architecture including VPNs hosting SWIFT Alliance access, Payment validation (AML and suspicious transactions) engine.
- T. Perform malware analysis of memory of important systems
- U. Control assessment at the key entry points for malware
- V. Review of malware Incident Management and Response
- W. Active scanning of the target hosts to identify any malware infections
- X. SWIFT certificate / SSL review
- Y. Encryption of data in static / transmit mode
- Z. Review of outsourcing arrangement (SLA) vis-a-vis industry standards
- AA. Review of Firewall internal/ external rules w.r.t. SWIFT
- BB. Antivirus scanning on servers and user PCs
- CC. Review of security controls / Management controls of all other interfacing systems including CBS
- DD. Arrangements for Anti-phishing/ takedown of rogue applications
- EE. Review of Standard Operating Procedures
- FF. Review of Middleware between systems
- GG. Review of Fraud Risk Management System related to SWIFT activities/ functions
- HH. IT General controls review
- II. Creation, approval of SWIFT transaction process in Core Banking
- JJ. Control at pre-transmission stage (i.e. before sending payment messages to Bank with which Nostro Account is maintained)
- KK. Controls post transmission of payment messages
- LL. Review of Nostro Reconciliation Process

- MM. Review of operations carried out by Trade Finance Team
- NN. Review of various SWIFT related activities/ functions carried out by domestic branches
- OO. To comply with SWIFT Customer Security Program - Guidance given by SWIFT covering 16 mandatory and 11 advisory controls of SWIFT customer security controls framework
- PP. Compliance audit post ATR submitted by the Bank on remediation of the identified gaps.
- QQ. Functionality review of SWIFT systems
- RR. Validation of financial parameters, etc.
- SS. Assessment of gaps in implementation of policies
- TT. Compliance to the legal/regulatory guidelines.

Controls and implementation of advisory/circular issued by RBI/SWIFT system to strengthen the SWIFT infrastructure.

xxxiv. Registration Authority (RA) Office Audit: RA office set-up under IDRBT Set-up audit shall cover but not limited to the following aspects:

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

xxxv. MPLS Network Architecture, Management & Audit

xxxvi. Document Management System (DMS)

xxxvii. Active Directory

xxxviii. Proxy Application Server

xxxix. Payment Gateway Audit: -Review of interface with approx. 10 Payment Gateways used by the Bank viz. ATM, Cash Recycler Mobile Banking, Internet Banking, Bill Desk, Citrus etc. Verification of controls for RTGS, NEFT, SFMS, SWIFT, NFS etc. at Payment Gateway as per the regulator's policies and guidelines.

xl. Biometric Infrastructure for Finacle Login, Attendance System, e-KYC.

xli. Centralized Anti-Virus Solution

xlii. UCO Bank Rewardz Program

xliii. Audit for IT Act Compliance

xliv. Audit of Disaster Recovery Plans

xliv. Audit of privileged users (Database, OS)

xlvi. Capacity Planning of IT Infrastructure of Critical Applications

xlvi. Audit of Service Level Management

xlvi. Audit of License Management

xlix. Cyber Security Framework Audit

I. Application Audit-ADC applications (Mobile Banking, E-Banking, UPI etc.) on various platforms

ii. **ANTI VIRUS:**

- Proactive virus prevention and detection procedures are in place and implemented. Virus definitions are updated regularly.
- Monitoring of antivirus servers located at different locations and other locations for having updated latest versions and definitions (t+1) basis.
- Monitoring procedures effectiveness for branch level client's updations.
- Antivirus rules/policy review as per Global standard practices /RBI Guidelines.
- Assurance on release of patches by various osd vis-à-vis implementation status on desktops/pcs/servers/systems and submit a gap analysis report.
- Ensuring Organization units are created as per the business requirement and users are authenticated through active directory system.
- BCP on ad (Active Directory) system, back up and its resilience.

lii. **Others:**

- A. Privileges available to Systems Integrator and Outsourced Vendors.
- B. Evaluate role, responsibility and accountability of IT Process owners.
- C. 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.
- D. 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
- E. Alignment of IT strategy with Business strategy.
- F. IT Governance related processes.
- G. Long Term IT strategy and Short Term IT plans.
- H. Information security governance, effectiveness of implementation of Security policies and processes.
- I. Review of RBI, IT examination report (GAP assessment of Cyber Security Control).

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

3. Source Code Audit

The in-house developed Applications/ Outsourced application approx. 250(+/-20%) application/API / Customization and any outsourced applications if required.

Source Code Audit or Secure Code Review, as applicable, of inhouse- developed applications or outsourced applications (In case of respective vendors are unable to

provide the Third-party Independent IS Audit Certificate). Version control aspect of in-house software must be covered under Source Code Audit.

4. Vulnerability Assessment

The Vulnerability Assessment (**VA**): VA of IT assets (applications, systems and infrastructure) deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc. through their life cycle (pre-implementation, post implementation, major changes etc.) shall cover a minimum of 1200-1500 (+/-10%) **devices on half-yearly basis** and VA of IT infrastructure related to PCI DSS compliance will be done on **Quarterly basis**. A list of Servers/devices in different locations will be given to the selected vendor.

Threat Vulnerability and Risk Assessment (TVRA) for Data Centre as per scope of Monetary Authority of Singapore (MAS) and Hong Kong Monetary Authority (HKMA) shall also be covered. Credential based Vulnerability Assessment (VA) shall be conducted.

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

- Vulnerability assessment of all servers along with their operating system, Switch, network equipment, security equipment installed, ATM etc.
- 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. Appropriate updated tools should be used for each phase of test.

5. Penetration Testing

Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.) throughout their lifecycle (pre-implementation, post-implementation and/or after major changes). Penetration Testing (External) shall be conducted mandatorily on all public facing applications/URLs/Website/APIs/Cloud Applications exposed to the internet.

The final list of IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.) for Penetration Testing will be provided to the selected bidders. The Approximate Number of public facing websites/URLs/applications/APIs for Penetration Testing is about 250 (+-20%).

In addition, the same shall be conducted as and when any new IT Infrastructure or Application is introduced or when any major change is performed on Application or Infrastructure.

Black Box Penetration Testing (BB PT) will be done of IT infrastructure. However, for PCI DSS compliance related IT Infrastructure, Grey Box Testing (GBT)/ White Box Testing (WBT) shall be done.

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.

6. Vendor & Site Audit:



6.1.1 Vendor Audit

Vendor Audit is a process of evaluating and assessing the IT-related practices and controls of a third-party vendor or supplier. **Vendor Audit** shall cover specific aspects of the vendor's operations, such as data security, compliance with contractual agreements, service level agreements (SLAs) and adherence to industry standards, regulations. This shall be done as per scope given in RBI Master Direction on Outsourcing of Information Technology Services 2023, other regulatory guidelines and Bank's outsourcing policy. In the case of infrastructure hosted at Vendor site, Auditor will conduct On-Site visits to the vendor's facilities to access physical security measures and observe their operational practices. The Audit typically begins with a risk assessment to identify potential vulnerabilities or weaknesses in vendor's systems or processes that could pose a risk to the organization.

6.1.2 Site Audit for Various IT Infrastructure/Facilities like Data Centre, Treasury, CTS Centers, ATM vendor site etc.

As part of the audit the following are to be covered

- Bangalore Datacenter,
- Kolkata Datacenter/DR,
- Treasury Mumbai,
- CTS-(New Delhi, Chennai, Mumbai or any other new location)

- Near DR Site-Bangalore,
- ATM Switch Audit at Mumbai
- Prepaid Card Facility Chennai
- POS Infrastructure Facility
- SMS system,
- Card printing facility (Chennai & Pune),
- SWIFT centers
- Vendor's Sites wherever applicable

Site Audit shall cover but not limited to the following aspects

- Changes in System/process related to RBI and other Statutory Bodies Circular /Guidelines
- Review of PCI DSS Report Compliance (ROC) and Attestation of Compliance (AOC) during site Audit.
- Data Security steps taken by Vendor
- Review of VA and PT report of Vendor during Site Audit
- Financial Strength of the Vendor

The Data Centre facilities Audit at the above-mentioned sites shall cover but not limited to the following aspects:

- Building Management Systems
- Power Supply, UPS & DG
- Logical Access Control
- Physical Access Controls
- Environment Control
- Datacenter 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
- High availability

Note: Any new addition/up-gradation in sites, hardware, software, new deliverables and 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.

7. Application Audit

Application audit shall be conducted for all applications within the bank based

on the checklist approved from the Vertical Head of Audit and Inspection Department. Entire checklist based on the applicability shall be covered for each audit.

Some critical applications are CBS (Domestic & Overseas), Internet Banking (Domestic & Overseas), ADC channels, GBM, LAPS, MMS, NEFT, RTGS, SWIFT, UPI, BBPS, IMPS, DMS, Mobile Banking, CTS, Biometric Authentication System (BAS), AEPS etc.

The Application audit shall cover but not limited to the following aspects:-

- Controls for performing/changing parameter setup of functionality across applications.
- Segregation of duties.
- Application parameterization process.
- 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.
- Regular updation of job cards , SOPs with new version releases.
- If outsourced, escrow arrangement with application vendors.
- Interfacing between Finacle/ADC & other ancillary Applications.
- Controls for opening/modifications of Office Accounts /GL heads.

8. Database Audit (CBS, ADC, LAPS, RTGS, NEFT, ITMS, RBIA, GBM, MISADF, M-Banking, E-Banking, UPI, IMPS, PFMS, SWIFT, Smart Fee Collection System, GST, BBPS etc. (approximately 80 databases)).

The Database audit shall cover but not limited to the following aspects:--

- Role of DBA
- 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.
- Review of Users having access to the Database Server

- Synchronization between DC & DR Databases for CBS/Alternate Delivery Channels (ADC), between Treasury Primary Database at Mumbai & Treasury DR Database at Kolkata and between MISADF Database at Kolkata & Treasury DR Database at Mumbai 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

9. Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications:

- UCO mBanking plus
- BHIM UCO UPI
- UCO Secure (Digisafe)
- mPassbook (Domestic)
- mPassbook (Singapore)
- mPassbook (Hongkong)
- UCO Pay+
- Corporate mBanking
- NPA tracker
- UCO Cluster
- UCO Sandeh Nivaran (Cloud environment)
- UCO ARBD mobile app
- UCO Merchant etc.

10. Network Audit

The Network audit shall cover but not limited to the following aspects:--

- Overall Network architecture
- 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/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.

11. Firewall Rule Based Review

All the configuration output of the firewall rules shall be captured and studied, policy/rule-wise, manually or using the tools so that any mis-configuration residing may be mitigated.

12. Assessment of KPI & KRI

As per RBI Circular Ref.No.DBS(CO).CSITE/9094/31.01.015/2016-17 dated 23.05.2017, “CISO shall develop Cyber Security KRIs and KPIs and get an independent assessment of the same including its coverage at least on a quarterly basis”. Assessment of KRIs and KPIs prepared by CISO.

13. Audit for Sustenance of ISO-27001 Certification for DC-DR Operations:

Auditor for Internal Audit shall provide onsite handholding support to Bank prior to the Surveillance Audit(s) and liaise with the External Auditor, each year, for sustenance of ISO-27001 Certification. During the course of Certification, broadly following documents have been provided / created and shall be made available for the on boarded Auditor:

1. ISMS Scope, Framework and Policy.
2. Risk Treatment Plan / Risk Management Register.
3. Statement of Applicability
4. Measurement of Effectiveness.
5. Internal Audit Report.
6. Corrective and Preventive Actions (CAPA) Report.

Department envisages the following scope for the Auditor to be on boarded for Internal Audit in regard to the sustenance of ISO-27001 Certification:

1. Guidance for compliance of non-Complied items mentioned in Risk Management Register.
2. Ensure sustenance of the complied items mentioned in the Risk Management Register.
3. Conducting Internal Audit before commencement of Final Audit each year for ascertaining the readiness of Bank for the Final Audit and recommending for the same.

4. Liaising with External Auditor for smooth conduct of ISO-27001 Compliance Audit (the details of the Audit Firm shall be shared with the selected bidder for liaising). Any other items relevant to ISO-27001 Certification as per standard may be part of the scope.

14. AUDIT OF CHANGE LOGS

Audit of Change Logs refers to the process of reviewing and examining the records that documents changes made to a system, software application, database, or any other type of information system. Change logs are typically used to track and record modifications, updates, or alterations made to these systems over time.

15. SECURITY AUDIT OF CLOUD SERVICES

IS Audit of Cloud Services shall be conducted for assurance on deployment of cloud security on systems hosted in clouds.

It shall also be conducted as and when any new IT Infrastructure or application is introduced or migrated to cloud.

16. SECURE CONFIGURATION REVIEW/AUDIT

Secure Configuration Review of Operating System (OS) and Database (DB) shall be done on yearly basis. Configuration Audit of Servers, Network and Security Devices covering critical Applications, like CBS (domestic and overseas), Mobile Banking, Internet Banking, UPI, GBM, RTGS, NEFT, SWIFT, etc.

The configuration review shall be done based on the Secure Configuration Documents.

17. AUDIT OF STORAGE OF PAYMENT SYSTEM DATA

Audit to ensure that the entire data relating to payment systems operated by them are stored in a system only in India as per RBI and other regulatory guidelines. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

18. SYSTEM AUDIT REPORT (SAR) NSDL

The audit will be conducted as per the checklist provided by NSDL and all the points of the checklist are required to be addressed.

19. IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)

As per Regulation 14(1)(h) of Aadhaar (Authentication and Offline Verification) Regulations, 2021, operations and systems are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance

with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;

"Compliance checklist for certifying compliance with controls that the AUA/KYC User Agency (KUA) is required to have in place."

Compliance checklist for certifying compliance with controls that the AUA/KUA is required to have in place Version 1.0 [issued in March 2024] and latest version also.

20. AUDIT OF DIGITAL LENDING

Periodic validation tests of the algorithm/model used in Business Rule Engine (BRE) – once in six months during the first two years and suggest any remedial measures basis operational audit observations.

IS Audit of digital lending IT Infrastructure and Process Audit of new product before moving into live

Regular audit of Digital Lending Process and compliance thereon (at least annually).

21. CYBER SECURITY FRAMEWORK REVIEW

As part of IS Audit Program, the adequacy and adherence to the controls of RBI's Cyber Security Framework and other applicable regulatory guidelines will be reviewed and measured, to assess the level of risk /preparedness arising due to newer threats in products or processes.

22. SWIFT Customer Security Program (CSP) Assessment

SWIFT Customer Security Controls Framework (CSCF) (latest version – Current version is CSCF - V2025)

The SWIFT Customer Security Controls Framework (CSCF) consists of mandatory and advisory security controls for SWIFT users. The controls evolve over time to combat new and arising threats and to implement new developments in Cybersecurity.

23. AUDIT OF VIRTUAL MACHINES (VMs)

An audit of Virtual Machines (VMs) includes:

- (a) **Access Controls** – Review user access, authentication, and privilege management.
- (b) **Configuration Management** – Check VM settings, hardening, and compliance with security baselines.
- (c) **Patch Management** – Verify OS and application updates.
- (d) **Logging & Monitoring** – Ensure logging is enabled and logs are reviewed.
- (e) **Backup & Recovery** – Assess backup frequency, integrity, and restoration process.
- (f) **Network Security** – Review firewall rules, segmentation, and traffic monitoring.
- (g) **Resource Utilization** – Analyze CPU, memory, and storage usage.
- (h) **Incident Response** – Check for security event handling procedures.
- (i) **Encryption & Data Protection** – Validate encryption for data at rest and in transit.

Compliance & Policy Adherence – Ensure alignment with regulatory and internal policies.

24. Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS

Comprehensive audit should cover the entire application, including the following:

- (a) web application (both thick client and thin client);
- (b) mobile apps;
- (c) APIs (Including API whitelisting);
- (d) databases;
- (e) hosting Infrastructure and obsolescence;
- (f) cloud hosting platform and network infrastructure; and
- (g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant Information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is—

- (a) modification in application functionality; or
- (b) addition/modification of APIs; or
- (c) migration to new infrastructure platform or cloud service; or
- (d) change in configuration of application hosting, servers, network components and security devices; or
- (e) change in access control policy.

25. Audit/Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)

Regular audits and assessments of SBOM and CBOM processes should be conducted to ensure accuracy and completeness. An SBOM is a list of all the components, libraries and modules that make up software providing transparency into its composition.

26. Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong

Cyber Security Audit/Assessment/Risk Assessment of Hongkong centre of Bank having one branch as per Cyber Resilient Assessment Framework of Hong Kong Monetary Authority (HKMA).

27. MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore

Cyber Security Audit/IT Risk Assessment of Singapore centre of Bank having one branch as per Technology.

28.MIGRATION AUDIT

Data Migration Audit will verify the migration of the legacy system to the new system with minimal disruption or downtime, with data integrity and no loss of data.

29.VA/PT OF INTERNET CONNECTED PCs

VA/PT (Vulnerability Assessment and Penetration Testing) of Internet connected Desktops/ PCs of Corporate Departments shall be done.

30. SECURITY CUM FUNCTIONAL AUDIT OF NEW APPLICATIONS:

Security cum Functional Audit of approximately 100 applications per year will be done before GO-Live for New in-house developed application/ After Major Changes in existing applications (both in-house and developed by external vendors). Scope of Security cum Functional Audit include:-

- Functionality implemented vis-à-vis the Bank's requirements.
- Input, processing and output controls across various schemes across the bank.
- Coverage and adequacy of UAT test cases.
- IS Audits i.e. Vulnerability Assessment, Penetration Testing, External Assessment, Configuration Audit, Data Migration Audit, Application security Audit etc.
- Controls for performing/changing parameter setup of functionality across applications.
- Through-put validation.
- Automated batch processing, scheduled tasks, critical calculations etc.
- IT General Control Review.
- In case of web based application, the validation against top 10 OWASP, CWE/SANS Top 25 vulnerabilities, etc.
- Regular updation of job cards with new version releases.
- Checks against network attacks.
- Code Review, wherever possible.
- Code obfuscation.
- Application Security & Controls Review.
- Database Security & Integrity Review.
- Review of Interface Controls with other applications (both Internal and External).
- Review of Network & Communication Controls with relation to the application package.

- Test of robustness of the system by running a specific number of transactions on it.
- Evaluation of Efficiency & Effectiveness of the package vis-à-vis business processes and requirements. Whether the objectives of the application are likely to be fulfilled by implementation.
- Assessment of the risk component in the package.
- Compliance testing of the changes in software made for mitigation of the discrepancies pointed out in the audit report.

31. Forensic Audit/ Forensic Analysis/Investigations:

- Bank may assign Forensic Analysis/Investigations as per the requirement, same to be conducted as by adhering following minimum guidelines:
- The bidder should have well established procedure for conducting Forensic Analysis/Investigation and the same shall be provided to Bank.
- The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence and examination of the evidences should be done in the copy of the original evidences.
- Persons conducting an examination of digital evidence should have been suitably trained and should have sufficient experiences.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
- The process or lifecycle of doing forensics should be followed as per the Industry best practice and regulatory guidelines.
- The bidder shall provide their findings with recommendations in report format as per the incidence investigation process.
- Bidder should arrange to deployment of forensic team within 1 hour of reported incidences.

TYPES OF AUDIT & FREQUENCY OF AUDIT

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

Sl. No.	Type of IS Audit	Frequency
1.	PENETRATION TESTING (PT) (EXTERNAL/INTERNAL)	Half Yearly
2.	VULNERABILITY ASSESSMENT (VA)	Half Yearly/Quarterly, as applicable
3.	APPLICATION AUDIT	Yearly
4.	MIGRATION AUDIT	As and when required.
5.	PROCESS AUDIT	Yearly
6.	NETWORK ARCHITECTURE REVIEW	Yearly

7.	FIREWALL RULE BASED REVIEW	Half Yearly
8.	SOURCE CODE AUDIT/REVIEW	Yearly
9.	DATABASE AUDIT	Yearly
10.	KRIs and KPIs Prepared by CISO OFFICE	Quarterly
11.	VA/PT OF INTERNET CONNECTED PCs	Half Yearly
12.	SECURITY AUDIT OF CLOUD SERVICES	Yearly
13.	PERFORMANCE TESTING	Yearly
14.	AUDIT OF CHANGE LOGS	Quarterly
15.	VENDOR & SITE AUDIT	Yearly
16.	SECURE CONFIGURATION REVIEW/ CONFIGURATION AUDIT	Yearly
17.	GOVERNANCE AUDIT	Yearly
18.	AUDIT OF STORAGE OF PAYMENT SYSTEM DATA	Yearly
19.	SYSTEM AUDIT REPORT (SAR) NSDL	Yearly
20.	IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)	Yearly
21.	PRE-IMPLEMENTATION AUDIT OF NEW APPLICATION (SECURITY & FUNCTIONAL)	As and when required.
22.	AUDIT OF DIGITAL LENDING	Yearly
23.	RBI CYBER SECURITY FRAMEWORK REVIEW	Yearly
24.	SWIFT CSP Assessment	Yearly
25.	AUDIT OF VIRTUAL MACHINES (VMs)	Yearly
26.	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Yearly (One Time)
	Limited audit shall be performed six months after the comprehensive audit	Half Yearly
27.	Audit/ Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)	Yearly or as and when required.
28.	Information Security Management System (ISMS) for ISO 27001:2022 Certification Sustenance	Yearly
29.	Forensic Audit/ Forensic Analysis/Investigations:	As and when required
30.	Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong	Yearly
31.	MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore	Yearly

Note: No deletion or omission or modification in the scope will be entertained either during the bidding period or after selection of auditor.

PART-III

1. Earnest Money Deposit

The Bidder(s) must submit Earnest Money Deposit in the form of **Bank Guarantee (BG)** only, valid for a period of 90 days together with a claim period of 45 days in favour of UCO Bank payable at Kolkata for an amount mentioned hereunder:

Particulars of Job to be undertaken	Earnest Money Deposit
Selection of IS Audit Firms/Organisations for Information System Audit	Rs. 10,00,000/- (Rupees Ten Lakh Only)

Bank details are as below:

Bank details for BG
IFSC- UCBA0001870

In case the bid validity is extended, the validity of EMD should also be extended accordingly. Non-submission of Earnest Money Deposit will lead to outright rejection of the offer. Sending EMD other than BG form will not be entertained. 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) either at the time of or before the execution of Service Level Agreement (SLA).

Following categories of Bidder(s) however, be exempted from furnishing bid security:

- Micro and Small Enterprises (MSEs) who are holding valid Udyam Registration and are manufacturer of the offered Product or Service (Primary Product / Service - in case of bunch bid with total value wise evaluation) and give specific confirmation to this effect at the time of bid submission and claim EMD exemption.
- Start-ups as recognized by Department for Promotion of Industry and Internal Trade (DPIIT), holding valid Startup Recognition Certificate which is to be uploaded while bidding and claiming EMD exemption.
- Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s).
- Central / State PSUs.

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

- a. If the bidder withdraws its bid during the period of bid validity (90 days from the date of opening of bid).
- b. 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
- c. The selected bidder withdraws his tender before furnishing on unconditional and irrevocable Performance Bank Guarantee.
 - d. The bidder violates any of the provisions of the terms and conditions of this tender specification.
 - e. In case of the successful bidder, if the bidder fails:
 - To sign the contract in the form and manner to the satisfaction of UCO BANK.
 - To furnish Performance Bank Guarantee in the form and manner to the satisfaction of UCO BANK either at the time of or before the execution of Service Level Agreement (SLA).
 - If the Vendor, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal, fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP.

2. Delivery, Installation & Implementation

The proposed audit should be started within 15 days of receiving the purchase order and to be completed as per IS Audit plan and calendar which is mutually agreed between Bank and Vendor. After receiving initial reports, Bank will complete the compliance. Post compliance auditor will review the compliance and submit a compliance certificate to the Bank within one month.

3. Contract Period:

The tenure of the Contract will be for a period of 2 (two) years effective from the date of execution of the Service Level Agreement (SLA) unless terminated earlier by the Bank by serving 90 days' prior notice in writing to the selected bidder at its own convenience without assigning any reason and without any cost or compensation therefore.

However, after the completion of the contract period of 2 (two) years, the contract may be extended/renewed for further period on mutually agreed terms and conditions. An SSLA will be executed to amend the contract period.

The performance of the selected bidder shall be reviewed every quarter and the Bank reserves the right to terminate the contract at its sole discretion by giving 90 days' notice without assigning any reasons and without any cost or compensation therefor. Any offer falling short of the contract validity period is liable for rejection.

The selected bidder is required to enter into a Service Level Agreement (SLA), the format whereof is to be supplied by the Bank.

4. Performance Bank Guarantee

The selected Bidder shall, within a period of fifteen (15) days from the date of Letter of Intent (LOI)/Purchase Order (PO) have to furnish a Performance Bank Guarantee, format as per Annexure – III issued by any scheduled commercial bank (other than UCO Bank) equivalent to 10% of the project cost/Total Cost of Ownership (TCO) valid for a period of 27 months (24 months + claim period of three (3) months) from the date of SLA/Purchase Order (PO) for indemnifying any loss to the Bank.

The Performance Bank Guarantee shall act as a security deposit either in case the selected Bidder is unable to commence the project within the stipulated time or the commencement of the project is delayed inordinately beyond the acceptable levels, the Bank reserves the right to forfeit the same.

Further, the Bank reserves the right to invoke the Performance Bank Guarantee in case the selected Bidder is not able to fulfill any and/or all conditions specified in the document or is unable to complete the project within the stipulated time and such breach remains uncured within such period as mentioned in the Clauses of Termination/Order Cancellation. This is independent of the Liquidated Damages (LD) on delivery and installation.

The selected Bidder shall be responsible for extending the validity date and claim period of the Performance Bank Guarantee as and when it is due on the account of non-completion of the project and/or extension/renewal of contract period.

In case the Service Level Agreement/Contract is extended, the selected Bidder shall have to submit the Bank Guarantee equivalent to 10% of the project cost/Total Cost of Ownership (TOC) for the extended period along with a claim period of three (3) months.

5. Payment Terms

Payment Terms per Audit Round is given below:

- i. No advance payment will be made.
- ii. 50% of the charges/fees of a particular Type of Audit 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
- iii. 25% of the charges/fees will be payable after Bank receiving Compliance Review Report complete in all respect.

- iv. Balance 25% will be payable after one month of submission of Review Report complete in all respect (re-audit confirmation), provided bank is satisfied that Review has been conducted complete in all respect as per Scope.
- v. TDS would be deducted for any payment made by the BANK as per the prevailing Rules of Government of India.
- vi. GST will be paid as per the prevailing rate.

Penalty

The selected bidder shall perform its obligations under the work order and the agreement entered into with the Bank, in a professional manner.

If the Selected bidder fails to complete the due performance of the contract in accordance with the specification and conditions of the offer document, the Bank reserves the right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty for non-performance.

i) Penalty for not initiation of project on time:

Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value, as penalty, a sum equivalent to 0.5% of the services for each week or part thereof of delay in starting of actual audit works as specified in the agreement up to 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.

ii) Penalty for not closing the project on time:

Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value, as penalty, a sum equivalent to 0.5% of the services for each week or part thereof of delay until actual delivery or performance up to 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.

Any delay reason attributed to the Bank will not be considered for penalty. But it will be bidders responsibility to prove the same.

iii) Limitation Of Penalty

Overall penalty calculated above, shall be restricted to total value of Performance Bank guarantee submitted by the Successful Bidder. However, any penalty imposed by RBI/ Ombudsman / Other Bank / Any other Government Authority / Office on Customer complaints due to Proposed Solutions operation

will be recovered from the Successful Bidder over and above the penalty imposed by the Bank.

Penalties, if any shall be calculated for every quarter and recovered from any payments to be made by the Bank to the Bidder. Wherever applicable as stated above while effecting any payment, deduction towards LD payment will be made. Hence the bidder should raise the invoice deducting the penalty amount.

6. Paying Authority

The payments as per the Payment Schedule covered hereinabove shall be paid by **Head Office, Audit and Inspection Department**. However, Payment of the Bills would be released, on receipt of advice / confirmation for satisfactory delivery and commissioning, live running and service report etc. Also, the bidder has to submit the certificate of insurance covering all the risks during transit, storage, installation, commissioning, testing and handling including third party liabilities

Following Documents are to be submitted for Payment:

- Invoice in Triplicate
- Duly receipted Delivery Challans
- Original Octroi Receipts, if any
- Installation Report, counter signed by an authorized official from the delivery site

7. Price Validity

The selected bidder will be required to keep the price valid for whole contract period. from the date of issuance of Purchase Order. There shall be no increase in price for any reason whatsoever during the price validity period and Bank may place the additional Purchase Orders to the selected bidder for any or all of the services at the agreed unit rate for line items as mentioned in the commercial format i.e. Annexure – XIII during the price validity period. Bank may procure additional hardware/software/licenses as mentioned in the RFP document, after the price validity period, on mutually agreed terms during the contract period

8. STAGES OF EVALUATION

There would be Three (3) stages for evaluation process.

The Stages are:

- Eligibility Criteria Evaluation

- Technical Evaluation
- Commercial Evaluation

The Eligibility Criteria would be evaluated first for the participating bidders. The bidder, who qualify all Eligibility Criteria will be shortlisted for the Techno-commercial bid evaluation.

A. Eligibility Evaluation

The Eligibility would be evaluated first for the participating bidders. The bidders, who would qualify all Eligibility Criteria will be shortlisted for the technical bid evaluation.

B. Technical Evaluation

The proposals will be evaluated in two stages. In the first stage, i.e. Technical Evaluation, the bidders will be shortlisted, based on bidder's responses. In the second stage, the commercial bids would be evaluated.

During the period of evaluation, bidders may be asked to provide more details and explanations about information provided in the proposals. Bidders should respond to such requests within the time frame indicated in the letter/e-mail seeking explanation.

The resources offered should meet all the technical requirements mentioned in scope of work and Bills Of Material, Annexure – XII. Non-compliance to any of the technical specification may attract rejection of the proposal

C. Commercial Evaluation

The commercial bids of only technically qualified bidders will be opened and evaluated by the Bank and the evaluation will take into account the following factors:

- i. The Bill of Material must be attached in Technical Bid as well as Commercial Bid. The format will be identical for both Technical Bid and Commercial Bid, except that the technical bid should not contain any price information (with Prices masked). Technical bid without masked Bill of Materials will be liable for rejection. Any deviations from the Bill of Material / non-submission of prices as per the format shall make the bid liable for rejection.
- ii. The L1 bidder will be selected on the basis of the amount quoted for the proposed audit/testing as per commercial bid.
- iii. The optimized TCO (Total Cost of Ownership) identified in the commercial bid would be the basis of the maximum outflow of the Bank for undertaking the scope of work.
- iv. In case there is a variation between figure and words, the value mentioned in

words will be considered.

- v. In the event the vendor has not quoted / not mentioned / left blank item(s) in the commercial bid, it would be considered as free of cost. However, for the purposes of payment and finalization of the contract, the value of zero cost in the not quoted / not mentioned / left blank item(s) would be used.
- vi. Bank may waive off any minor infirmity or non-conformity or irregularity in a bid, which does not constitute a material deviation.
- vii. If there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price shall be corrected accordingly. In any case unit price cannot be increased & offered quantity cannot be decreased to correct the TCO.
- viii. If there is discrepancy between percentage and amount, the amount calculated on percentage basis will prevail.
- ix. If the bidder does not accept the correction of errors, the bid will be summarily rejected.
- x. **In all the above cases the TCO quoted as a 'Total Cost' in GeM would be the final price for evaluation purpose. However, TCO may be reduced to be in-line with unit price for order placement.**
- xi. Discrepancies if any, would be corrected as per the TCO without increasing any of the unit price and payment would be made on unit price only.

9. AWARD OF CONTRACT

The bidder who quotes the **lowest price** will be treated as **L1 Bidder**.

Bank will **shortlist maximum of 2 bidders**, one who has quoted the lowest (L1) and other who has matched L1 price and emerged as 2nd lowest (L2) based on GeM evaluation. Order will be placed in proportions of 60:40 based on cost between L1 & L2 bidder respectively.

L1 price (TCO) matching option will be extended to all bidders whose commercial are responsive on GeM portal. Among the bidders matching the L1 price, priority may be given to L2 bidder in GeM listing. If L2 bidder is not agreeing to match L1 TCO, the next lowest (L3) will be given a chance and so on. This will be continued till Bank gets a maximum of two bidders. In the event, no other bidder matches the L1 price, entire order will be awarded to L1 bidder.

Among the selected two bidders, whosoever has quoted the lowest price for a particular line item will be considered as the lowest price for that line item. Accordingly, the bidders will be given a chance to match the line-item wise price.

Master order will be placed for 60% of TCO to L1 and 40% of TCO to L2. Subsequent detailed bifurcation of work order will be placed by Bank as and when required. Bank will maintain the 60:40 ration throughout the contract.

However, the Bank shall be under no obligation to accept any bid or any other offer received in response to this Tender notice and shall be entitled to reject any or all offers including those incomplete offers without assigning any reason whatsoever. The Bank reserves the right to make any changes in the terms and conditions of purchase. The Bank will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations unless there is change in the terms and conditions of purchase.



PART-IV

1. Due Diligence

The Bidder is expected to examine all instructions, forms, terms and specifications in this ATC and study the ATC document carefully. Bid shall be deemed to have been submitted after careful study and examination of this ATC with full understanding of its implications. The Bid should be precise, complete and in the prescribed format as per the requirement of this bid. Failure to furnish all information required by this ATC or submission of a Bid not responsive to this ATC in each and every respect will be at the Bidder's own risk and may result in rejection of the Bid and for which UCO Bank shall not be held responsible.

2. Rejection of the Bid

The Bid is liable to be rejected if:

- i. The document doesn't bear signature of authorized person on each page signed and duly stamp.
- ii. It is received through E-mail.
- iii. It is received after expiry of the due date and time stipulated for bid submission.
- iv. Incomplete Bids, including non-submission or non-furnishing of requisite documents / Conditional Bids/ deviation of terms & conditions or scope of work/ incorrect information in bid / Bids not conforming to the terms and conditions stipulated in this Request for proposal (RFP) are liable for rejection by the Bank.
- v. Bidder should comply with all the points mentioned in the RFP. Non-compliance of any point will lead to rejection of the bid.
- vi. Any form of canvassing/lobbying/influence/query regarding short listing, status etc. will be a disqualification.
- vii. 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).
- viii. Non-submission of Pre-Contract Integrity Pact as per format given in Annexure - IV.
- ix. If the masked commercial bid submitted without masking the prices OR commercial bid submitted in open condition along with the technical bid

3. PRE-BID MEETING

The queries for the **Pre-bid** Meeting should reach us in writing by email to hodit.proc@ucobank.co.in as per 'Annexure-X' on or before 28-07-2025. Pre-Bid meeting will be held on 29-07-2025 (Tuesday) at 13:00 hrs. through WebEx meetings. The link will be shared to the bidders submitting pre-bid queries and/or request to

attend pre-bid meeting through e-mail only. It may be noted that no query from any bidder shall be entertained if received after the above-mentioned date. Queries raised by the prospective bidder and the Bank's response will be hosted at Bank's website, GeM Portal & CPP Portal. No individual correspondence will be accepted in this regard.

4. 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 successful bidders, the EMD will be forfeited by the bidder.

5. 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.

6. Clarification of offer

To assist in the scrutiny, evaluation and comparison of offers/bids, UCO 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 and no change in the price or substance of the bid shall be sought, offered or permitted. Any decision of UCO Bank in this regard shall be final, conclusive and binding on the bidder.

7. Late Bids

Any bid received by the Bank after the deadline (Date and Time mentioned in Bid Details table / Pre-Bid / subsequent addendum / corrigendum) for submission of bids, will be rejected and / or returned unopened to the bidder.

8. Issue of Corrigendum

At any time prior to the last date of receipt of bids, Bank may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the RFP document by a Corrigendum. Any such corrigendum shall be deemed to be incorporated into this RFP.

9. 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.

10. Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information, including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of Bank or any of its officers, employees, contractors, agents, or advisers.

11. Purchase preference to Micro and Small Enterprises (MSEs)

Purchase preference will be given to MSEs as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail the Purchase preference, the bidder must be the manufacturer of the offered product in case of bid for supply of goods. Traders are excluded from the purview of Public Procurement Policy for Micro and Small Enterprises. In respect of bid for Services, the bidder must be the Service provider of the offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service.

If L1 is not an MSE and MSE Seller (s) has/have quoted price within L1+ 15% (Selected by Buyer) of margin of purchase preference /price band defined in relevant policy, such Seller shall be given opportunity to match L1 price and contract will be awarded for 25% (selected by Buyer) percentage of total quantity.

12. 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.

13. No Legal Relationship

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

14. Cancellation of Tender Process

- a. UCO BANK reserves the right to accept or reject in part or full any or all offers at its sole discretion at any stage without assigning any reason thereof and without any cost or compensation therefor. Any decision of UCO Bank in this regard shall be final, conclusive and binding upon the bidders.
- b. The Bank reserves the right to accept or reject any Bid in part or in full, and to cancel the Bidding process and reject all Bids at any time prior to contract award, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for Bank's action.

15. Corrupt and Fraudulent Practices

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

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

AND

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

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

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

16. Non-Transferrable Offer

This Request for Proposal (RFP) is not transferable. Only the bidder who has purchased this document in its name or submitted the necessary RFP price (for downloaded RFP) will be eligible for participation in the evaluation process.

17. Period of Bid Validity

Bids shall remain valid for **90 (Ninety)** days after the date of bid opening prescribed by UCO BANK. UCO BANK holds the rights to reject a bid valid for a period shorter than 90 days as non-responsive, without any correspondence. In exceptional circumstances, UCO BANK may solicit the Bidder's consent to an extension of the validity period. The request and the response thereto shall be made in writing. Extension of validity period by the Bidder should be unconditional and irrevocable. The EMD provided shall also be suitably extended. A bidder acceding to the request will neither be required nor be permitted to modify its bid. A bidder may refuse the request without forfeiting its EMD. In any case the EMD of the bidders will be returned after completion of the process.

18. No Commitment to accept Lowest or any Bid

UCO Bank shall be under no obligation to accept the lowest or any other offer received in response to this RFP and shall be entitled to reject any or all offers including those received late or incomplete offers without assigning any reason whatsoever. UCO Bank will not be obliged to meet and have discussions with any vendor, and or to listen to any representations, and Bank's decision would be final, conclusive and binding upon the bidder.

19. Errors and Omissions

Each Recipient should notify Bank of any error, omission, or discrepancy found in this RFP document in the form of pre-bid queries within the time as given in control sheet, otherwise Bank's decision would be final conclusive and binding upon the bidder.

20. Acceptance of Terms

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

21. RFP Response

If the response to this RFP does not include the information required or submission is through Fax mode or through e-mail, the response to the RFP is liable to be rejected. In this regard, Bank may seek clarification & Bank's decision would be final and binding upon the bidder.

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.

22. Notification

Bank will notify the Respondents in writing as soon as possible 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.

23. Erasures or Alterations

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.

24. Clarifications on and Amendments to RFP document

Prospective bidders may seek clarification on the RFP document by letter/fax/e-mail till the date mentioned in the bid control sheet. Further, at least 7 days' time prior to the last date for bid-submission, the Bank may, for any reason, whether at its own initiative or in response to clarification(s) sought from prospective bidders, modify the RFP contents by amendment. Clarification /Amendment, if any, will be notified on Bank's website.

25. Language of Bids

The bid as well as all correspondence and documents relating to the bid exchanged by the bidder and the Bank shall be in English language only.

26. Authorized Signatory

The bid shall be signed by a person or persons duly authorized by the Bidder with signature duly attested. In the case of a body corporate, the bid shall be signed by person who is duly authorized by the Board of Directors / Competent Authority of the bidder or having Power of Attorney.

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 certified by Company Secretary along with Power of Attorney duly stamped, 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.

27. Adoption of Integrity Pact

UCO Bank has adopted practice of Integrity Pact (IP) as per CVC guidelines. The Integrity Pact essentially envisages an agreement between the prospective vendors / bidders / sellers, who commit themselves to Integrity Pact (IP) with the Bank, would be considered competent to participate in the bidding process. In other words, entering into this pact would be the preliminary qualification. In case of bids for the purchase of Goods, Services, and Consultancy etc. not accompanied with signed IP by the bidders along with the technical bid, the offers shall be summarily rejected. The essential ingredients of the Pact include:

- i. Promise on the part of the principal not to seek or accept any benefit, which is not legally available.
- ii. Principal to treat all bidders with equity and reason
- iii. Promise on the part of bidders not to offer any benefit to the employees of the principal not available legally
- iv. Bidders not to enter into any undisclosed agreement or understanding with other bidders with respect to prices, specifications, certifications, subsidiary contract etc.
- v. Bidders not to pass any information provided by the principal as part of business relationship to others and not to commit any offence under PC/IPC Act.
- vi. Foreign bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principals or associates.
- vii. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.
- viii. For Joint Ventures (JV) entities, Integrity Pact should be signed by all partners.
- ix. In case of foreign contractor, details of their Indian counterpart should be submitted to Bank by the vendor

Integrity Pact, in respect of a particular contract, shall be operative from the date IP is signed by both the parties till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings. IP shall cover all phases of contract i.e. from the stage of Notice Inviting Tenders (NIT)/Request for Proposals (RFP) till the conclusion of the contract i.e. final

payment or the duration of warrantee/guarantee. Format of IP is attached as **Annexure – IV** for strict compliance.

The following Independent External Monitors (IEMs) have been appointed by UCO Bank, who will review independently and objectively, whether and to what extent parties have complied with their obligation under the pact.

1. Dr. Manoj Kumar Chhabra

C-182 (3rd Floor), Sarvodya Enclave.
Malviya Nagar, New Delhi-110017.
email: mkchhabra10@gmail.com

2. Shri Rajvir Singh

H.No. B-71A, Ashok Enclave part-II,
Sector -37, Faridabad, Haryana
email: rsgodara1963@gmail.com

All pages of Integrity Pact (IP) must be signed and stamped Integrity Pact (IP) should be deposited with IT Department undertaken procurement at the address mentioned along with RFP document.

28. Preference to Make in India



The policy of the Govt. of India to encourage “Make in India” and promote manufacturing and production of goods and services in India, “Public Procurement (Preference to Make in India), Order 2017 and the revised order issued vide GOI, Ministry of Commerce and Industry, Department for Promotion of Industry and Internal trade, vide Order No. P-45021/2/2017-PP (BE-II) dated 19th July 2024 subsequent amendments will be applicable for this tender.

The local supplier at the time of submission of bid shall be required to provide a certificate as per **Annexure-XVI** from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement.

29. Restriction On Procurement Due to National Security

Any bidder from a country sharing a land border with India will be eligible to bid in this tender only if the bidder is registered with the Department for Promotion of Industry and Internal Trade (DPIIT). A copy of the valid Certificate to be attached with the Bid.

Certificate as per the Annexure XI to be attached along with the Bid. Vide Ministry of Finance OM No. 6/18/2019-PPD dated 23rd July 2020.

Reference is made to Government of India order F. No. 7/86/2020/BOA-I dated 07.08.2020 on restrictions on procurements from bidders from a country or countries, on grounds of Defence in India, or matters directly or indirectly, related thereto, including national security.

- i. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority.
- ii. "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such person, participating in a procurement process.
- iii. "Bidder from a country which shares a land border with India" for the purpose of this Order means: -
 - a. An entity incorporated, established or registered in such a country; or
 - b. A subsidiary of an entity incorporated, established or registered in such a country; or
 - c. An entity substantially controlled through entities incorporated, established or registered in such a country; or
 - d. An entity whose beneficial owner is situated in such a country; or
 - e. An Indian (or other) agent of such an entity; or
 - f. A natural person who is a citizen of such a country; or
 - g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

- iv. The beneficial owner for the purpose of (iii) above will be as under:

In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation:

- a. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five per cent. of shares or capital or profits of the company;

b. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

1. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership or entitlement to more than fifteen percent of capital or profits of the partnership;
2. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;
3. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
4. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. An Agent is a person employed to do any act for another, or to represent another in dealings with third person.

The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority.

30. OTHER TERMS AND CONDITIONS

- i. Cost of preparation and submission of bid document: The bidder shall bear all costs for the preparation and submission of the bid. UCO Bank shall not be responsible or liable for reimbursing/compensating these costs, regardless of the conduct or outcome of the bidding process. Documents (viz. Integrity pact, Bank Guarantee, Undertakings etc.) which are to be executed on non-judicial stamp paper, have to be submitted in original / hard-copy at the communication address mentioned below, within three days from the date of bid opening:

**UCO Bank, Head Office-II
Department of Information Technology,**

Procurement Cell,
7th Floor, 3 & 4 DD Block, Sector – 1
Salt Lake, Kolkata – 700064

- ii. The Bank reserves the right to modify any terms, conditions and specifications of this request for submission of offer and to obtain revised bids from the bidders with regard to such changes. The Bank reserves its right to negotiate with any or all bidders. The Bank reserves the right to accept any bid in whole or in part.
- iii. The Bank reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar features of a bidder. When the Bank makes any such rejection, the Bank will not be bound to give any reason and/or justification in this regard to the bidder. The Bank further reserves the right to reject any or all offers or cancel the whole tendering process due to change in its business requirement.
- iv. Response of the Bid: The Bidder should comply all the terms and conditions of RFP.
- v. The bidder is solely responsible for any legal obligation related to licenses during contract period for the solution proposed and Bidder shall give indemnity to that effect.
- vi. 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.

31. Normalization of bids:

The Bank has discretion to go through a process of Eligibility evaluation followed by the technical evaluation and normalization of the bids to the extent possible to ensure that eligible bidders are more or less on the same technical ground.

The Bank can repeat this normalization process at every stage of bid submission or till the Bank is satisfied. The eligible bidder/s have to agree that they have no reservation or objection to the normalization process and all the technically short listed bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The shortlisted bidder/s, by

submitting the response to this RFP, agrees to the process and conditions of the normalization process.

32. Single Point Of Contact

The selected bidder shall appoint a single point of contact, with whom Bank will deal, for any activity pertaining to the requirements of this RFP.

33. Right To Alter Quantities

The Bank reserves the right to alter the number of services/ hardware/ software/ licenses specified in the tender in the event of changes in plans of the Bank. Any decision of UCO BANK in this regard shall be final, conclusive and binding on the bidder. The bank reserves the right to place order for additional services/hardware/software/licenses at the agreed price during the contract period with the same terms and conditions. Banks is not obligate to purchase all the quantity of the services/hardware/software/licenses as mentioned above. Bank reserves the right to alter the quantities at any time not exceeding 25% of the total contract value without prior notice to the selected bidder(s).

34. Human Resource Requirement

The selected bidder by executing the agreement shall be deemed to have unconditionally agreed as under:

- a) The selected bidder shall provide a contingent of well-trained personnel and extend necessary mentoring and operational support to the intermediary network of agents, etc. as part of the solution/service.
- b) The selected bidder shall confirm that every person deployed by them on the project has been vetted through a third-party background check prior to their engagement. The selected bidder shall manage the activities of its personnel or others engaged in the project, etc., and shall be accountable for all the personnel deployed/engaged in the project.
- c) In case the performance of the selected bidder/their CSP/agent/employees engaged in the project is not satisfactory or is detrimental to the interests of the Bank, the selected bidder shall have to replace the said person within the time limits stipulated by the Bank. Where the selected bidder fails to comply with the Bank's request, the Bank may replace the said person or their agents/employees on its own.
- d) No right to employment in the Bank shall accrue or arise to the employees or agents of the selected bidder, by virtue of engagement of employees, agents, etc. of the selected bidder for any assignment under this project. It is further clarified that the arrangement herein with the selected bidder is a contract for service.

e) The selected bidder shall exercise due diligence and only engage persons having established identity, integrity, requisite qualifications, skills and deployment experience for all critical activities.

f) The Bidder has to submit following KYC documents for onsite/Offsite engineer

- I. Resume latest (Candidate Photograph should be part of Resume only) and Print should be in color only.
- II. Address Proof (Local and Permanent)- Duly attested photocopy by candidate and Bidder HR
- III. Aadhar Card - Duly attested photocopy by candidate and Bidder HR
- IV. Relieving Certificate of Previous employer - Duly attested photocopy by candidate and Bidder HR
- V. Passport - Duly attested photocopy by candidate and Bidder HR
- VI. Background Police Verification report - Duly attested photocopy by candidate and Bidder HR

g) The selected bidder shall extend all of the outsourced banking and financial services by deploying such personal that have high integrity and meet the qualifications and other criteria stipulated by the Reserve Bank of India, Government or the Bank from time to time and agrees and undertake that during the subsistence of this agreement they will not employ any personnel/individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time, as per the provisions of Minimum Wages Act 1948.

35. Preliminary Scrutiny

UCO Bank will scrutinize the offers to determine whether they are complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether all the necessary information supported by documentary evidences are submitted as per prescribed method. Offers not meeting the prescribed guidelines and or with incorrect information or not supported by documentary evidence, wherever called for, would summarily be rejected. However, UCO Bank, at its sole discretion, may waive any minor non-conformity or any minor irregularity in an offer. UCO Bank reserves the right for such waivers and this shall be binding on all vendors.

36. Sub-Contracting

As per the scope of this Agreement sub-contracting is not permitted, unless otherwise permitted by the Bank.

37. Taxes

- a. Bidder shall be solely liable for the payment of all taxes, duties, fines, penalties, etc., by whatever name called as may become due and payable under the local, state and/or central laws, rules and/or regulations as may be prevalent and as amended from time to time in relation to the services rendered pursuant to this agreement. The Bank may in its discretion, but without being bound to do so, make payment of Taxes, duties as aforesaid and in the event of such payment, Bank shall be entitled to deduct the payment so made from the payment due to Bidder in respect of Bills.
- b. The Bank shall not be liable nor responsible for collection and / or payment of any such taxes, duties, fines, penalties etc., by whatever name called, that are due and payable by bidder, under the local, state and/ or central laws, rules and /or regulations as may be prevalent and as amended from time to time.
- c. Nothing contained herein shall prevent the Bank from deducting taxes deductible at source as required by any law/s or regulation/s. Bidder shall be responsible to report any non-receipt of certificate of taxes deducted at source within ninety (90) days of deduction of such taxes at source by the Bank to bidder. The Bank will not issue any duplicate certificate for deduction of taxes at source unless such request is made within ninety (90) days of the closure of the financial year.
- d. Bidder shall co-operate fully in the defence of any claim/s by any local, state or union authorities against The Bank with respect to any taxes and/or duties due and payable by bidder and /or individuals assigned by bidder under this agreement. Without limiting the generality of the foregoing bidder shall upon request by The Bank, give to The Bank all documents, evidences in a form satisfactory to The Bank to defend such claim/s. Any claims filed against The Bank, the cost to be borne by the selected bidder.
- e. The payments which is/are **inclusive of GST and other taxes, fees etc.** as per the Payment Schedule covered herein above shall be paid by **Head Office, DC Infra Cell**. However, Payment of the Bills would be released, on receipt of advice / confirmation for satisfactory delivery and commissioning, live running and service report etc. after deducting all penalties.

38. Confidentiality And Secrecy

The RFP document is confidential and is not to be reproduced, transmitted, or made available by the Recipient to any other party. The RFP document is provided to the Recipient on the basis of the undertaking of confidentiality given by the Recipient to Bank. Bank may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same terms and conditions as this original and subject to the same confidentiality undertaking.

The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Bank or any of its customers, suppliers, or agents without the prior written consent of Bank.

The bidder/selected bidder must undertake that they shall hold in trust any Information received by them under the Contract/Service Level 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.
- The selected service provider acknowledges and agrees that all tangible and intangible information obtained, developed or disclosed including all documents, data, papers, statements, any business/customer information, trade secrets and process of the UCO Bank relating to its business practices in connection with the performance of services under this Agreement or otherwise, is deemed by the UCO Bank and shall be considered to be confidential and proprietary information ("Confidential Information"), solely of the UCO Bank and shall not be used/disclosed to anybody in any manner except with the written consent of The UCO Bank.
- The selected service provider shall ensure that the same is not used or permitted to be used in any manner incompatible or inconsistent with that authorized by the UCO Bank. The Confidential Information will be safeguarded and the selected service provider will take all necessary action to protect it against misuse, loss, destruction, alterations or deletions thereof.
- **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 execute a Non-Disclosure Agreement to the bank as per bank's format before or at the time of execution of the Service Level Agreement.**

39. Compliance With Laws

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

All the employees/operator deployed by the Vendor for the digitization activity must comply with government's rules and regulations like Minimum Wages Act, Provident Fund, Labour Law, ESIC facility standard, CVC / RBI guidelines.

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

The Vendor confirms to Bank that it complies with all Central, State, Municipal laws and local laws and rules and regulations and shall undertake to observe, adhere to, abide by, comply with and notify Bank about compliance with all laws in force including Information Technology Act 2000 as amended from time to time or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligation's towards them and for all purposes of this Contract, and shall indemnify, keep indemnified, hold harmless, defend and protect Bank and its officers/staff/ personnel/ representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligation's arising therefrom.

The Vendor shall promptly and timely obtain all such consents, permissions,

approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate Bank and its employees/officers/staff/personnel/representatives(agents from and against all claims or demands of liability and all consequences that may Occurs or arise for any default or failure on its part to conform or comply with the above and all other statutory obligation's arising there from and Bank will give notice of any such claim or demand of liability within reasonable time to the Vendor. The Vendor shall also provide a certificate from Statutory Auditor or Cost Auditor of the Company or from practicing Cost Accountant giving the percentage local contents as defined in PPP order issued by GOI from time to time and applicable for the said procurement/project.

40. 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 maybe which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance, such as:



- Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics,
- Situations, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes,
- Terrorist attacks, 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 delay in performing his / her obligations resulting from any Force Majeure cause as referred to and / or defined above.

41. Completeness Of The Project

The project will be deemed as incomplete if the desired objectives of the project as mentioned in Section "Scope of Work" of this document are not achieved.

42. Order Cancellation

The Bank reserves its right to cancel/terminate the Order/Agreement in the event of occurrence of one or more of the following circumstances, that are not occasioned due to reasons solely and directly attributable to the Bank alone:

- a) The **selected Bidder/Vendor** commits a breach of any of the terms and conditions of the Letter of Intent/Purchase Order/Agreement;
- b) The selected Bidder/Vendor violates the Laws, Rules, Regulations, Bye-Laws, Guidelines, and Notifications etc.;
- c) Serious discrepancy in the quality of service of selected Bidder/Vendor expected during the implementation, rollout and subsequent maintenance process;
- d) The selected Bidder/Vendor goes into liquidation voluntarily or otherwise;
- e) An attachment is levied or continues to be levied upon the selected Bidder/Vendor for a continuous period of 7 days upon the effects of the order;
- f) The progress regarding execution of the order by the selected Bidder/Vendor is found to be unsatisfactory;
- g) Non-compliance by the selected Bidder/Vendor of the scope of the job;
- h) Repetitive failure of the deployed personnel of the **selected** Bidder/Vendor to perform the job to the satisfaction of the Bank;
- i) The selected Bidder/Vendor fails to complete the assignment as per the timelines prescribed in the Work Order/ said Agreement/Contract and the extension, if any allowed.
- j) On the events of data piracy/privacy/system failures/security failures by the selected Bidder/Vendor;
- k) If deductions on account of liquidated damages exceed more than 10% of the total order price.

In case of cancellation/termination of Order/Agreement due to the above stated situations, the following consequences will entail:

- i. **In case the selected Bidder/Vendor fails to deliver the ordered hardware, software, services and FM resources as stipulated in the delivery schedule, UCO BANK reserves the right to procure these deliverables from alternate sources at the risk, cost and responsibility of the selected Bidder/Vendor with the capping of 125% of the original quoted cost for such deliverable.**
- ii. **If the selected Bidder/Vendor does not perform satisfactorily or delays in execution of contract, UCO Bank reserves the right to get the balance order executed by**

another party of its choice, in this event the selected Bidder/Vendor is bound to make good with the capping of 125% of the original quoted cost for such deliverable, which UCO Bank may have to incur in executing the balance order. This clause is applicable, if for any reason, the order is cancelled.

- iii. UCO Bank reserves the right to recover any dues payable by the selected Bidder/Vendor under the contract from any amount outstanding to the credit of the selected Bidder/Vendor, including the bills and /or invoking the Performance Bank Guarantee under this Agreement.
- iv. In case of cancellation of order, any advance payments (except payment against ATS) made by the Bank to the selected Bidder/Vendor for implementation of project, would necessarily have to be returned to the Bank. If the selected Bidder/Vendor fails to return such payment within thirty (30) days, then the selected Bidder/Vendor have to return the amount to the Bank with interest @ 15% per annum, further the selected Bidder/Vendor would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be incurred by the Bank to appoint any other Vendor. This is after repaying the original amount paid.
- v. The selected Bidder/Vendor shall be liable under this section if the contract/purchase order has been cancelled in case the sum total of penalties and deliverables exceeds 10% of the TCO.

In case of order cancellation/termination, Bank will notify the selected Bidder/Vendor within Ninety (90) days' notice period inclusive of Thirty (30) days cure period before cancellation/termination of the Order/Agreement. However, it is clarified that the notice should specifically contain that the Ninety (90) days period for cancellation is inclusive of cure period of Thirty (30) days, if the selected Bidder/Vendor fails to cure within Thirty (30) days' time the notice for cancellation will become absolute. For the sake of clarity, the period of 90 (Ninety) days will begin from the date of receipt of termination/cancellation notice in accordance with Clause no. 76 (in part-V) of this Agreement. Any other mode of communicating the termination/cancellation of the Agreement will be deemed to be invalid.

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.

43. Indemnity

In consideration of the Bank having agreed to accept our offer in terms of this bid, we the Bidder herein doth hereby agree and undertake that we shall indemnify and keep indemnified the Bank including its respective Directors, Officers and Employees, from

and against any claims, demands, actions, proceedings, damages, recoveries, judgments, costs, charges liabilities, losses arising out of all kinds of accidents, destruction, deliberate or otherwise, violation of applicable laws, regulations, guidelines and/or environmental damages, if any, during the contract period or expenses of any nature and kind whatsoever and by whomsoever made in respect of the said RFP and any damage caused from and against all suits and other actions that maybe instituted or preferred against the Bank or which the Bank may have to bear, pay or suffer directly or indirectly due to omission or commission of any act on our part and/or on the part of our employees, representatives, agents and/or associates, sub-contractors in performance of the obligations enumerated under the said Request for Proposal.

We the Bidder further irrevocably and unconditionally agree and undertake to hold the Bank harmless, indemnify and keep the Bank indemnified from any of its following acts and deeds, irrespective of the value, genuineness or enforceability of the aforesaid Contract/Agreement or insolvency, bankruptcy, reorganization, dissolution, liquidation or change in ownership of UCO Bank or us or any other circumstance whatsoever which might otherwise constitute a discharge of the Bidder:

a. material breach of any of the terms of the RFP/ SLA or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty or breach of confidentiality etc., of the service provider under these presents and/or Request for Proposal and Service Level Agreement/Contract/Master Service Level Agreement;

b. infringement of any intellectual property right, patents, trademarks, copyrights etc., including any claims of infringement of any third-party copyright, patents or other intellectual property and/or any third party claims on the Bank for malfunctioning of the equipment, software or deliverables or usage of any license, or such other statutory infringement in respect of all components provided to fulfill the scope of work under these presents and/or Request for Proposal and Service Level Agreement/Contract/Master Service Level Agreement;

PROVIDED HOWEVER (i) Bank notifies BIDDER in writing within 15 days of the claim and/or Bidder is having knowledge of the same and/or reasonably it should be in notice of the bidder (ii) BIDDER will have control of the defense and all related settlement negotiations, however, if Bank, deem fit and proper may take control of the defense (iii) Bank provides BIDDER with the assistance, information, and authority reasonably necessary to perform the above, and (iv) the Bank will not make any statements, admissions or public remarks which may prejudice to the interest of the bidder.

Exclusion:

Bidder shall not be obligated or liable under any provision of this Agreement for any performance problem, claim of infringement or other matter to the extent same is resulting, in whole or in part, from: (i) any modification of any Solution (other than a modification made solely by Bidder); (ii) any use of a Solution in breach of the Agreement; (iii) any combination of the Solution with any other software, hardware, product, technology, data or services; (iv) any use of any version of a Solution other than the Supported Release;

Bank's failure to implement corrections or changes to a Solution provided by Bidder/ Bidder; (vi) Bank's failure to subscribe to support and maintenance if then offered for the Solution; (vii) any Embedded Software; (viii) any transaction processed on behalf of Bank or its affiliates, users, or customers, including any credit, fraud or counterfeit losses; or (ix) any negligence, wrongful act, or breach of the Agreement by Bank or its Authorized Recipients, users or Customers.

"Embedded Software" shall mean embedded or bundled third-party software, including open-source software. A 'Release' means the periodic provision of updates or modifications which Bidder, in its discretion, may incorporate into the Solution. A 'Supported Release' shall mean the immediately preceding Release, or other Releases made available in the previous twelve (12) months)

यूको बैंक UCO BANK

If any infringement claim is raised by any third party or any person, the Bidder will have the following remedial measures at their expenses:

- modify or replace all or part (s) of the Solution to make it non-infringing;
- procure for the Bank the right/license to continue using the Solution; or
- remove all or part (s) of the Solution. If the Vendor so removes all or a part (s) of a Solution, then the Vendor shall refund the same to the Bank in proportion, if Bank has paid a one-time upfront initial license fee for the Software.

However, it is clarified that this remedy will not curtail any of Bank's rights under this Agreement.

c. for any loss or damages caused to the Bank's premises or property, loss of reputation & loss of life etc., solely attributable due to the acts of the Bidder/Bidder's employees, representatives, agents and/or associates;

d. non-compliance of the Bidder with the applicable laws and/or statutory obligations, if any, in performing its duties as a service provider under the said Request for Proposal and Service Level Agreement/Contract/Master Service Level Agreement;

e. Gross Negligence or wilful misconduct attributable to the Bidder, its employees, representatives, agents and/or associates or any liabilities which pose significant risk;

We shall not enter into any settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the rights, interest and reputation of the Bank (and/or its customers, users and service providers).

Service Provider will not be liable for any loss of profits, revenue, contracts or anticipated savings or and consequential or indirect loss or damages however caused.

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

Any notice, request or other communication to be given or made under this indemnity shall be in writing addressed to either Party at the address stated in the previously mentioned Agreement/Contract.

We hereby declare that this Indemnity is in addition to the Liquidated Damages as provided in these presents.

44. Publicity



Any publicity by the selected bidder in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank. The Bidder shall not make or allow making a public announcement or media release about any aspect of the Contract unless The Bank first gives the Bidder its prior written consent.

45. Privacy And Security Safeguards

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

46. Guarantees

Selected bidder should guarantee that all the material as deemed suitable for the delivery and management for this RFP. All software must be supplied with their original and complete printed documentation.

47. Exit Option And Contract Re-Negotiation

The Bank reserves the right to cancel the said Agreement/Contract in the event of happening one or more of the following conditions:

- a) Failure of the selected bidder/Vendor to accept the Letter of Intent/Purchase Order and/or failure to furnish the Performance Bank Guarantee within a period of fifteen (15) days of receipt of Letter of Intent/Purchase Order;
- b) Delay in commissioning the Project beyond the specified period;
- c) Delay in completion of the commissioning/implementation and acceptance tests/checks beyond the specified periods;

Bank will notify the selected bidder/Vendor with Ninety (90) days notice inclusive of a cure period of thirty (30) days before cancellation/termination. However, it is clarified that the notice should specifically contain that the Ninety (90) days period for cancellation is inclusive of a cure period of thirty (30) days, if the Vendor fails to cure within thirty (30) days' time, then the notice for cancellation will become absolute. For the sake of clarity, the period of Ninety (90) days will begin from the date of receipt of termination/cancellation notice in accordance with Clause no. 76 (in Part-IV) of this Agreement. Any other mode of communicating termination/cancellation of the Agreement will be deemed to be invalid.

In addition to the cancellation of Purchase Order/said Agreement/Contract, the Bank reserves the right to appropriate the damages through invocation of Performance Bank Guarantee furnished by the selected bidder/Vendor.

Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Vendor will be expected to continue the services. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of six (6) to twelve (12) months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.

The Bank and the Vendor shall together prepare the Reverse Transition Plan. However, the Bank shall have the sole decision to ascertain whether such Plan has been complied with.

Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Vendor to the Bank or its designate to ensure smooth handover and transitioning of Bank's deliverables, maintenance and facility management.

The reverse transition period may or may not be within the contract period. In case the reverse transition period falls within the contract period, all the terms & conditions, scope of work mentioned in the contract will hold good along with smooth handover and transitioning of Bank's deliverables to the Bank or its designates/nominees and no extra payment shall be paid by the Bank for such reverse transition.

However, if the reverse transition mechanism to be adopted after the expiry of the contract period, the Bank and the Vendor shall together prepare the Reverse Transition Plan for smooth handover and transitioning of Bank's deliverables to the Bank or its designates/nominees including maintenance and facility management. Though in such case the Bank shall have the sole authority to ascertain whether such Plan has been complied with, but the payment for such reverse transition would be determined on pro rata basis or on mutual consent of the Parties.

48. Termination For Convenience

The Bank, by a written notice for a period of ninety (90) days (both in words and figures) sent to the selected Bidder/Vendor, may terminate the said Agreement/Contract, in whole or in part, at any time at its convenience. The notice of termination shall specify that the termination is for Bank's convenience, the extent to which the performance of work under the said Agreement/Contract is terminated and the date upon which such termination becomes effective.

49. Termination For Insolvency

The Bank may at any time terminate the Contract by giving written notice **(90 days' notice period)** to the Bidder, if the Bidder becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

50. Termination For Default

The Bank, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the bidder, may terminate this Contract in whole or in part, if the bidder fails to perform any obligation(s) under the Contract.

In case of Termination for Default Bank will provide notice period of 90 days inclusion cure period of 30 days. However, it is clarified that the notice should specifically contain that the 90 days period for cancellation is inclusive of cure period of 30 days, if the Vendor fails to cure within 30 days' time the notice for cancellation will become absolute.

51. Consequences Of Termination

In the event of termination of the Contract due to any cause whatsoever, (whether consequent to the 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 available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution / continued execution of the scope of the Contract.

In the event that the termination of the Contract is due to the expiry of the term of the Contract, a decision not to grant any (further) extension by UCO Bank, the bidder 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 Deed 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.

52. Signing Of Contract

The selected bidder(s) shall be required to enter into a service level agreement (SLA) with UCO Bank, within 15 days of the award of the Bid through a Letter of Empanelment or within such extended period as may be specified.

The SLA shall be based on the requirements of this RFP, the terms and conditions of purchase order, the letter of acceptance and such other terms and conditions as may be determined by the Bank to be necessary for the proper performance of the work in accordance with the Bid and the acceptance thereof, with terms and conditions contained in a Memorandum of Understanding to be signed at the time of execution of the Form of Contract.

The selected bidder will also sign a Non-Disclosure Agreement and Deed of Indemnity with the Bank on a format prescribed by the Bank.

53. Technical Inspection And Performance Evaluation

- (i) UCO Bank reserves its right to carry out a technical inspection and performance evaluation (bench-marking) of the offered service/ solution/item(s).
- (ii) Eligible bidders will be required to demonstrate their services/ solution and / or to make technical presentation at Bank's Head Office, Kolkata for the proposed solution / service. Bidders will have to make such presentation / demonstration at their own cost.
- (iii) The bidders will be required to demonstrate the features of the proposed solution covering all the requirements mentioned in the "scope of work" as part of technical evaluation. Non-compliance of any point will lead to rejection of the bid. Commercial bids of only technically qualified bidders will be opened and evaluated by the Bank.

54. Verification

UCO Bank reserves the right to verify any or all statements made by the vendor in the Bid document and to inspect the vendor's facilities, if necessary, to establish to its satisfaction about the vendor's capacity to perform the job.

55. Dispute Resolution Mechanism

- a. The Bidder and The Bank shall endeavour their best to amicably settle all disputes arising out of or in connection with the Contract in the following manner:
 - i. 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.
 - ii. The matter will be referred for negotiation between Deputy General Manager of The Bank / Purchaser and the Authorised Official of the Bidder. The matter

shall then be resolved between them and the agreed course of action documented within a further period of 15 days.

- b. In case any dispute between the Parties, does not settle by negotiation in the manner as mentioned above, the same may be resolved exclusively by arbitration and such dispute may be submitted by either party for arbitration within 20 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.
- c. 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 45 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.
- d. 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 the Contract/Agreement 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.
- e. 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 and shall continue to render the Service/s in accordance with the provisions of the Contract/Agreement notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.

56. Arbitration

All dispute or differences whatsoever arising between the selected bidder and the Bank out of or in relation to the construction, meaning and operation, with the selected bidder, or breach thereof shall be settled amicably. If, however, the parties are not able to resolve any dispute or difference aforementioned amicably, the same shall be settled by arbitration in accordance with the Rules of Arbitration of the Indian Council of Arbitration and the award made in pursuance thereof shall be binding on the parties. The Arbitrator / Arbitrators shall give a reasoned award.

Work under the Contract shall be continued by the Selected bidder during the arbitration proceedings unless otherwise directed in writing by the Bank unless the

matter is such that the work cannot possibly be continued until the decision of the arbitrator or of the umpire, as the case may be, is obtained and save as those which are otherwise explicitly provided in the Contract, no payment due to payable by the Bank, to the Selected bidder shall be withheld on account of the on-going arbitration proceedings, if any unless it is the subject matter or one of the subject matters thereof. The venue of the arbitration shall be at KOLKATA, INDIA.

57. Applicable Law And Jurisdiction Of Court

The Contract with the Selected bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Kolkata (with the exclusion of all other Courts).

58. Limitation Of Liability

- i. For breach of any obligation mentioned in this document, subject to point no. (iii), in no event the Vendor shall be liable for damages to the Bank arising under or in connection with this Agreement for an amount exceeding the total project cost/contract value.
- ii. The **selected Bidder/Vendor** will ensure Bank's data confidentiality and shall be responsible for liability arising in case of breach of any kind of security and/or leakage of confidential customer/Bank's related information to the extent of **the loss caused to the Bank**.
- iii. The limitations set forth in point no. (i) shall not apply with respect to:
 - a) claims that are the subject of indemnification pursuant to violation **of** Intellectual Property Rights and Ownership.
 - b) **damages occasioned by the gross negligence or willful misconduct of selected Bidder/Vendor.**
 - c) damages occasioned by the **selected Bidder/Vendor** for breach of confidentiality obligations.
 - d) Regulatory or statutory **penalty** imposed by the Government or **any** Regulatory agency or non-compliance of statutory or regulatory guidelines applicable to the **Project**.
- iv) **The selected Bidder/Vendor will not be liable for any loss of profits, revenue, contracts or anticipated savings or and consequential or indirect loss or damages however caused.**

“Gross Negligence” means an indifference to, and/or a blatant violation of a legal duty with respect of the rights of others, being a conscious and voluntary disregard of the need to use reasonable care, which is likely to cause foreseeable grave injury or harm to persons, property, or both. Gross negligence involves conduct that is extreme, when compared with ordinary negligence. A mere failure to exercise reasonable care shall not be a gross negligence.

“Willful Misconduct” means any act or failure to act with an intentional disregard of any provision of this RFP/Contract, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

59. Amendment(S) In The Contract / Service Level Agreement

There shall be no variation(s) in or modification(s) in the terms of the Contract/ Service Level Agreement save and except by a written mutual consent signed by both the Parties i.e. the Bank and Vendor. Bank shall have the discretion/liberty to give effect to any amendment, modification etc. in the Contract/Service Level Agreement, if so required by Bank, sequel to any amendment(s)/ modification(s) etc. in the applicable Laws/Statutes including but not limited to amendment(s)/ modification(s) etc. in the existing Guidelines/ Instructions issued/to be issued by any Regulatory Authority.

60. Non- Solicitation

Both the Parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this Agreement/Contract during the period of the Agreement/Contract and one year thereafter, except as the Parties may agree on a case-by-case basis. The Parties agree that for the period of the Agreement/Contract and one year thereafter, neither Party will cause or permit any of its directors or employees who have knowledge of the said Agreement/Contract to directly or indirectly solicit for employment as the key personnel working on the project contemplated in this Agreement/Contract except with the written consent of the other Party. The above restriction would not apply to either Party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other Party (ii) respond to any public advertisement placed by either Party or its affiliates in a publication of general circulation or (iii) has been terminated by a Party prior to the commencement of employment discussions with the other Party.

61. Site Not Ready

Bank hereby agrees to make the site ready as per the agreed specifications, within the agreed timelines. Bank agrees that Bidder shall not be liable for any delay arising out of Bank's failure to make the site ready within the stipulated period, including but not limited to levy of liquidated damages for any delay in performance of Services under the terms of this Agreement.

62. Audit

The Vendor shall be subject to annual audit by internal/external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/such auditors in the areas of products (IT hardware/ Software/Source code/Manuals etc.) and services etc., provided to the Bank and the Vendor is required to submit such certification by such Auditors to the Bank.

The Vendor and or its /their outsourced agents/sub – contractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Vendor.

The Vendor shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Vendor. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 2 days (two days) to the Vendor before such audit and the same shall be conducted during the normal business hours.

Where any deficiency has been observed during the audit of the Vendor on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the Vendor shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the Auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the Vendor shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

The Vendor further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/Reserve Bank of India and/or any regulatory authority(ies). The Bank reserves the right to call for and/or retain any relevant information /audit reports on financial and security review with their findings undertaken by the Vendor. However, the Vendor shall not be obligated to provide records/data not related to the services provided under the said Agreement/Contract (e.g. internal cost breakup etc.).

63. Compliance With Is/Cyber Security Policy

The selected bidder shall have to comply with Bank's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the selected Bidders. Some of the key areas are as under:

- a) Responsibilities for data and application privacy and confidentiality.
- b) Responsibilities on system and software access control and administration.
- c) Custodial responsibilities for data, software, hardware and other assets of the Bank being managed by or assigned to the Vendor.
- d) Physical Security of the facilities.
- e) Physical and logical separation from other customers of the Vendor.
- f) Incident response and reporting procedures.
- g) Password Policy of the Bank.
- h) Data Encryption/Protection requirements of the Bank.
- i) In general, confidentiality, integrity and availability must be ensured.

64. Compliance With Reserve Bank Of India's Outsourcing Policy

During bid submission bidders should ensure compliance with the RBI's circular on "Master direction on outsourcing of Information Technology Services" vide circular number RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023. Selected bidder should comply with the directions of above referred RBI circular post award of contract.

The selected bidder must comply with Bank's outsourcing policy and must undergo due diligence process described in the policy. The necessary questioner and report formats shall be shared with the selected bidder.

65. Non-Assignment

The Vendor agrees that the Vendor shall not be entitled to assign any or all of its rights and or obligations under this Agreement to any entity including the Vendor's affiliate without the prior written consent of the Bank.

If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership, etc., this Agreement/Contract shall be considered to be assigned to the new entity and such an act shall not affect the rights of the Vendor under this Agreement/Contract.

66. Severability

If any provision of this Agreement is held to be illegal, invalid, or unenforceable under any Applicable Law, and if the rights or obligations of the Parties under this Contract/ Service Level Agreement will not be materially and adversely affected thereby (a) such provision will be fully severable; (b) this Contract/Service Level Agreement will be construed and enforced as if such illegal, invalid, or unenforceable provision had never been comprised a part hereof; and (c) the remaining provisions of this Contract/ Service Level Agreement will remain in full force and effect and will not be affected by the illegal, invalid, or unenforceable provision or by its severance here from.

67. Blacklisting

Grounds For Disqualification & Blacklisting

(A) Notwithstanding anything contained in this document, any Bidder/selected Vendor shall be disqualified when –

- a) any Bidder who has been black-listed or otherwise debarred by any Bank/Financial Institution/Central Government/State Government/any Central or State Undertaking or Corporation/Reserve Bank of India or any other Regulatory/ Statutory Authority as on as on date of the submission of this Tender/Procurement;
- b) any bidder whose Contract/Agreement with any Bank/Financial Institution/Central Government/State Government/any Central or State Undertaking or Corporation/Reserve Bank of India or any other Regulatory/ Statutory Authority has been terminated before the expiry of the Contract/Agreement for breach of any terms and conditions at any point of time during the last five years;
- c) any Bidder whose Earnest Money Deposit and/or Security Deposit have been forfeited by any Bank / Financial Institution/Central Government/ State Government/any Central or State Undertaking or Corporation/ Reserve Bank of India or any other Regulatory/Statutory Authority, during the last five years, for breach of any terms and conditions.

(B) Further disqualification can be imposed by the Bank in accordance with the procedures established, which may include but not limited to the following grounds, either at the stage of Competitive Bidding or at the stage of implementation of the Contract:

Commission of any act of:

- i) submission of a bid, proposal or any other document that is known or should be known by the Bidder to be false, misleading or non- meritorious or to contain false

information or concealment of information which will influence the outcome of the eligibility screening/selection process;

- ii) any documented unsolicited attempt by the Bidder to unduly influence the decision-making process of the Bank while determining the eligibility screening/selection process in favour of the Bidder;
- iii) unauthorized use of one's name or using the name of another for purpose of bidding;
- iv) breach of the terms of a public contract by a willful or material failure to perform in accordance with the terms thereof;
- v) withdrawal of a bid, or refusal to accept an award, or enter into contract with any Bank/Financial Institution/Central Government/State Government/ any Central or State Undertaking or Corporation/Reserve Bank of India or any other Regulatory Authority without any justifiable cause, after the Bidder had been adjudged as having submitted the lowest calculated Responsive Bid or highest rated Responsive Bid;
- vi) refusal or failure to furnish the required performance security within the prescribed time frame; यूको बैंक UCO BANK
- vii) refusal to clarify or validate the Bid submitted, in writing, within a period of seven (7) calendar days from receipt of the request for clarification if sought by the Bank;
- viii) that may tend to defeat the purpose of the competitive bidding, such as but not limited to; an eligible Bidder not purchasing the bid documents or not complying with the requirements during the evaluation of bid or habitually withdrawing from bidding or submitting letter of non-participation for at least three (3) times within a year, except for valid reasons;
- ix) lack of integrity or honesty or fraud, bribery, collusion or conspiracy;
- x) failure by the Bidder/Vendor, due to solely his fault or negligence, to mobilize and commence the work or perform within the specified time period, as specified in the Tender Document, including but not limited to the Request for Proposal/ Request for Quotation/ Agreement/Letter of Intention/Purchase Order etc.;
- xi) failure by the Bidder/Vendor to fully and faithfully comply with its contractual obligations without valid cause, or failure to comply with any written lawful instruction of the Bank or its representative(s) pursuant to the implementation of the Contract, which may include but not limited to the following:

- a. Employment of competent technical personal, competent engineers and/or work supervisors;
 - b. Provision of warning signs and barricades in accordance with approved plans and specifications and contract provisions;
 - c. Stockpiling in proper places of all materials and removal from the project site of waste and excess materials, including broken pavement and excavated debris in accordance with approved plans and specifications and contract provisions;
 - d. Deployment of committed equipment, facilities, support staff and manpower; and
 - e. Renewal of effectively date of the performance security after its expiry during the tenure of the Contract.
- xii)** assignment and subcontracting the Contract or any part thereof or substitution of key personnel named in the proposal without prior written approval by the Bank;
- xiii)** for the procurement of goods, unsatisfactory progress in the delivery of the goods by the manufacturer, supplier or distributor arising from his fault or negligence and/or unsatisfactory or inferior quality of goods, as may be provided in the contract;
- xiv)** for the procurement of consulting services, poor performance by the consultant of his services arising from his fault or negligence. The poor performance of the Consultant can include and may not be limited to defective design resulting in substantial corrective works in design and/or construction, failure to deliver critical outputs due to consultant's fault or negligence, specifying materials which are inappropriate, substandard, or way above acceptable standards, allowing defective workmanship or works by the contractor being supervised by the consultant etc.,
- xv)** for the procurement of infrastructure projects, poor performance by the contractor or unsatisfactory quality and/or progress of work arising from his fault or negligence as per the existing performance monitoring system of the Bank shall be applied, quality of materials and workmanship not complying with the approved specifications arising from the contractor's fault or negligence, willful or deliberate abandonment or non-performance of the project or contract by the contractor resulting to substantial breach thereof without lawful and/or just cause.
- (C)** Any parameters described, *supra*, attributable to any Partner/Director shall be construed as disqualification for the Firm/Company, as the case may be.

(D) The Bank will have the discretion to disqualify the Bidder/Vendor and/or initiate the process for blacklisting the Bidder/Vendor and may also entail forfeiture of performance security furnished by the Bidder/Vendor. “

68. Non-Disclosure

By virtue of Contract, as and when it is entered into between the Bank and the bidder, and its implementation thereof, the bidder may have access to the confidential information and data of the Bank and its customers. The bidder will enter into a Non-Disclosure Agreement to maintain the secrecy of Bank's data as per following: -

- a. That the bidder will treat the confidential information as confidential and shall not disclose to any third party. The bidder will also agree that its employees, agents, sub-contractors shall maintain confidentiality of the confidential information.
- b. That the bidder will agree that it shall neither use, nor reproduce for use in any way, any confidential information of the Bank without consent of the Bank. That the bidder will also agree to protect the confidential information of the Bank with at least the same standard of care and procedures used by them to protect its own confidential Information of similar importance. Without limitation of the foregoing, the bidder shall use reasonable efforts to advise the Bank immediately in the event that the successful bidder learns or has reason to believe that any person who has had access to confidential information has violated or intends to violate the terms of the Contract to be entered into between the Bank and the bidder, and will reasonably cooperate in seeking injunctive relieve against any such person.
- c. That if the bidder hires another person to assist it in the performance of its obligations under the Contract, or assigns any portion of its rights or delegates any portion of its responsibilities or obligations under the Contract to another person, it shall cause its assignee or delegate to be bound to retain the confidentiality of the confidential information in the same manner as the Bidder is bound to maintain the confidentiality. This clause will remain valid even after the termination or expiry of this agreement.
- d. That the bidder will strictly maintain the secrecy of Bank's data.

69. Intellectual Property Rights

- I. All copyrights, trademarks, patent, trade secret design and other intellectual property rights existing prior to the "Effective Date" will belong to the party that owned such rights immediately prior to the Effective Date". All modifications and enhancements to, and derivative works from, pre-existing intellectual property rights will belong to the party that owned such pre-existing intellectual property rights.

- II. Neither party will gain by virtue of this Contract any rights of ownership of copyrights, patents, trade secrets, trademarks or any other intellectual property rights owned by the parties prior to the date of signing of this Contract, other than customized software made by Vendor for Bank during the contract period.
- III. Bank owns all right, title and interest in and to the Bank's intellectual property rights existing prior to the "Effective Date" and all modifications and enhancements to, and derivative works from, such pre-existing intellectual property rights (collectively, "Bank Intellectual Property"). Nothing in this Contract transfers any ownership or title in or to any Bank Intellectual Property to Vendor or any third party. Subject to the limitations set forth in this Clause, Bank would grant access specifically and exclusively for the limited purpose of implementation of the proposed comprehensive and integrated technology solution to the Vendor to use of such of Bank Intellectual Property (excluding trade secrets, patents and trademarks) which may be reasonably necessary for the Vendor to perform its obligations under this Contract. Vendor hereby covenants with the Bank that the Vendor shall not use the same for any purpose other than the purpose for which the Bank will grant access to Vendor.
- IV. The "Software" directly acquired by the Bank from a software original equipment manufacturer, as part of the Implementation Services described in the Statement of Work, the software original equipment manufacturer will own all right, title and interest in and to such software existing prior to the "Effective Date" and all modifications and enhancements to, and derivative works from, such software (collectively, the "Third Party Intellectual Property"). Nothing in this Contract transfers any ownership in or any title to any Third-Party Intellectual Property to the Bank. Any issues arising out of third-party products or services shall be governed exclusively by the End User License Agreement and support agreement signed directly between the Bank and the original equipment manufacturer. Bank shall comply with the license terms, as may be specified by the respective licensors, applicable for the use of the Software provided under this Contract. Bank shall use such IP for its internal use only.
- V. All intellectual property developed during the term of this Contract that is neither Bank Intellectual Property nor Vendor Intellectual Property nor Third Party Intellectual Property ("New Intellectual Property"), shall be owned by Vendor, as between the Bank and Vendor, Vendor hereby grants the Bank an irrevocable, non-exclusive, world-wide perpetual license to use, execute, reproduce, display, perform and distribute New Intellectual Property without payment of any further amount for use within the Bank's Enterprise.

- VI.** For the purpose of this Contract, "Enterprise" shall mean and include any legal entity in which the Bank holds/ will hold shares at least to the extent of fifty percent (50%). Subject to Vendor having received the corresponding payment from the Bank, the Bank shall own all Intellectual Property Rights in all software and other materials (excluding any Vendor or third party products including any modifications, enhancements or customization made thereto) produced exclusively for the Bank by the Vendor pursuant to the project including any adaptations translations, derivative works and improvements that are developed by the Vendor, specifically and exclusively for the Bank whether protectable as a copyright, trademark, patent, trade secret and design or otherwise. The ownership of all Intellectual Property Rights in any information or materials provided to the Vendor by the Bank shall remain vested in the Bank. The ownership of all Intellectual Property Rights for any Bank customer information or materials provided to the Vendor by the Bank shall remain vested in the Bank.
- VII.** Nothing shall restrict either Party from the use of any ideas, concepts, knowhow, or techniques relating to data processing or network management, which either Party, individually or jointly, develops or discloses under this Contract, unless it is developed exclusively for the Bank use by the Vendor. The Vendor shall also at all point of time be under the obligations imposed under the terms of confidentiality while making use of such ideas, concepts, know-how or techniques. Also, such use shall not infringe either Party's patent rights or copyrights or a breach of confidentiality obligations. However, except for the licenses expressly granted by an agreement between the Bank and the Vendor, neither of the parties shall infringe on any patents or copyrights of the other Party.
- VIII.** IPR in "software and other materials" made exclusively for the Bank shall vest with the Bank alone. Material specifically developed by the Vendor for the Bank are defined as "Bank Materials" and same shall be passed on by the Vendor during the contract period.

70. Reverse Transition Mechanism

The Bidder understands the enormity of this Project and that it would require tremendous commitment of financial and technical resources for the same, for the tenure of Contract under this RFP. The Bidder therefore agrees and undertake that an exit resulting due to expiry or termination of Contract under this RFP or for any reason whatsoever would be a slow process over a period of six (6) months, after the completion of the notice period, and only after completion of the Bidders obligations under a reverse transition mechanism. During this period of Reverse Transition, the Bidder shall continue to provide the Deliverables and the Services in accordance with

the contract under this RFP and shall maintain the agreed Service levels. The Bank shall make payment for these services as per terms.

- a) All the warranties held by or in the name of the bidder shall be assigned or transferred as-is, in the name of the bank. The bidder shall execute any and all such documents as may be necessary in this regard.
- b) The parties shall return confidential information and will sign off and acknowledge the return of such confidential information.
- c) The bidder recognizes that considering the enormity of the assignment, the bidder agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the bidder under the scope, upon termination or expiration thereof, for any reason whatsoever.
- d) During which the existing bidder would transfer all knowledge, knowhow and other things necessary for the Bank or new bidder to take over and continue to manage the services.
- e) The bidder agrees that in the event of cancellation or exit or expiry of the contract it would extend all necessary support to the Bank or its selected bidders as would be required in the event of the shifting of the site.

71. Change Management



Changes to business applications, IT components and facilities should be managed by change management processes to ensure integrity of any changes.

All the IT components proposed under the RFP in the scope of RFP (such as application software, middleware etc.) should be periodically patched for all types of patches, such as - security patches, system patches etc. Emergency patches should also be applied immediately as per regulatory and other agencies directions etc.

If any software/module provided by bidder becomes End of support/ End of life during the warranty/ AMC/ ATS period, the same will be replaced by the next version of software without any cost to the Bank. Also, software replacements are done in a planned manner to ensure that no downtime is required on this account impacting customer services.

Bidder to ensure that the technology to be deployed needs to be latest, latest version of solution to be deployed and technology supplied should not be having residual life of less than 5 years from the date of effectiveness of contract.

72. Amalgamation

If the Bank undergoes an amalgamation, take-over, consolidation, reconstruction, merger, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the Bidder under this RFP.

73. Notices

Notice or other communications given or required to be given under the contract shall be in writing and shall be faxed/e-mailed followed by hand-delivery with acknowledgement thereof, or transmitted by pre-paid registered post or courier. Any notice or other communication shall be deemed to have been validly given on date of delivery if hand delivered & if sent by registered post than on expiry of seven days from the date of posting.

74. Waiver

Any terms or conditions of this Agreement may be waived at any time by the Party that is entitled to the benefit thereof. Such waiver must be in writing and must be executed by an authorized Officer of such Party. A waiver on one occasion will not be deemed to be a waiver of the same or either under breach or non-fulfillment on a future occasion. All remedies and benefits, either under this Agreement, or by law or otherwise afforded, will be cumulative and not alternative and without prejudice to the other remedy or benefit, as the case may be.

No failure or delay on the part of either Party in exercising any power, right or remedy under this Agreement shall be construed as a waiver thereof, nor shall any single or partial exercise of any such power, right or remedy preclude any other or further exercise thereof or the exercise of any other power, right or remedy.

75. NO RIGHT TO SET OFF

In case the Vendor has any other business relationship with the Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available to the Vendor under this arrangement with the Bank for any payment receivable under and in accordance with that business.

76. VIOLATION OF TERMS

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, suit for specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the Vendor from committing any violation or enforce the performance of the covenants, obligations and representations contained in this Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies the

Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

77. FIDELITY & SECRECY

The Vendor and its employees/personnel will strictly and individually undertake not to communicate or allow to be communicated to any person or divulge in any way any information relating to the process of implementation of solution (mention the name of the Project) and all information whatsoever concerning or relating to the Bank/concerned branch and its affairs to which the said employees/personnel will have access in the course of performance of the said Agreement.



Eligibility Criteria Compliance

Sl. No.	Criteria	(Proof of documents required / must be submitted)	List of documents submitted with details (if any)
1.	<p>Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on bid submission date</p> <p>or</p> <p>Registered as a partnership firm (registered under section-59 of the Partnership Act, 1932)</p> <p>or</p> <p>A limited liability partnership (under the Limited Liability Partnership Act, 2008) in India</p>	<p>1. Copy of Certificate of Incorporation issued by Registrar of Companies, Shareholding pattern, Copies of MOA and AOA(For Companies).</p> <p>2. Copy of LLP Incorporation certificate. In case of partnership firms, Deed of Partnership should be submitted.</p> <p>3. Shareholding pattern (For Companies and LLPs)</p> <p>4. PAN, TAN, GSTIN Certificate and any other tax related document if applicable is required to be submitted along with the eligibility bid.</p>	
2.	<p>The bidder should have a minimum annual turnover of Rs. 2.5 Crore per year during the last three financial years i.e. 2021-22, 2022-23 & 2023-24. This must be the individual company turnover and not of any group of companies.</p>	<p>Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing profit, net worth and turnover of the company for the consecutive last three financial years i.e., 2021-22, 2022-23 & 2023-24 should be submitted.</p>	
3.	<p>Bidder should have maintained a Positive Net-Worth during the last three financial years i.e. 2021-22, 2022-23 & 2023-24</p>	<p>Copy of the audited balance sheet & certificate from the Chartered Accountant</p>	

		of the company showing profit, net worth and turnover of the company for the consecutive last three financial years i.e. 2021-22, 2022-23 & 2023-24 should be submitted.	
4.	The bidder should be an empaneled Security Audit Firm with CERT-IN as on bid submission date.	Copy of valid CERT-IN certificate.	
5.	The bidder must be having core audit team of minimum 20 members having permanent employees who hold Industry Standard Certifications CISA/ DISA/ CISSP/ CEH/ CISM/ CA (valid as on date) and requisite experience (minimum 3 years) to handle the work as per the scope.	The profile of the Core Audit team must be submitted as per format given in Annexure – XIV and XV. Respective professional certificates to be submitted.	
6.	<p>Bidder should have industry-wide presence and expertise in conducting Information Systems (IS) Audit including VA-PT, Business understanding related to Banking sector, good track record and must have prior experience of conducting such audit/ special audit, mentioned below, of any Bank in India (SCBs, SFBs, Payment Banks) in last 5 years.</p> <p>The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last two financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India.</p>	<p>Documentary proof must be provided along with copies of Work Order clearly mentioning the areas of IS Audit, IT Audit completed/covered in the audit work.</p> <p>Apart from above, relevant copy of any one of the following is to be submitted:</p> <ol style="list-style-type: none"> 1. Completion Certificates 2. Project Sign-Offs 3. Satisfactory client certificate <p>The firm must submit a self-declaration that the members of core team has participated in the audits as mentioned in scope in last 3 years.</p>	
Page: 89 of 128			

	<p>The bidder should have conducted Audit in following at least 10 areas out of 16 areas: -</p> <ol style="list-style-type: none"> 1. Process Audit of Banking operations 2. VA/PT Capabilities 3. Source Code Audit 4. Application Audit 5. Network Audit 6. Audit of Security devices available at SOC 7. Database Management System Audit 8. IT/Digital/Information Security Governance and Management 9. Data Centre, Disaster Recovery Centre Audit 10. Business Continuity Audit 11. Data Security Audit 12. Reconciliation of Banking Payment Systems 13. Assessment of Banking applications mapped to their corresponding business logic & relevant regulatory guidelines. 14. Cloud Audit 15. SWIFT Audit 16. Migration Audit <p>The experience in aforesaid areas should be from either one or multiple Public / Private Sector Banks/Payment Banks in India.</p>		
7.	<p>Bidder should not have conflict of interest in carrying out the Audit. i.e. The firm should not have been engaged with the Bank in any form either direct or indirect assignment except concurrent audits in the past two years as on date of bid submission.</p>	<p>Undertaking on company letterhead mentioning the same should be submitted.</p>	
8.	<p>Bidder should have proven methodologies & tools for conduct of audit. Tools should be as Industry Standard and free from bugs and vulnerabilities.</p>	<p>Self-Declaration in format attached – mentioning tool that are free from bugs</p>	
<p>Page: 90 of 128</p>			

9.	The Bidder should not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity as on the date of bid submission	Self-declaration to this effect on the company's letterhead should be submitted	
10.	Bidder should submit an Undertaking regarding compliance of all Laws, Rules, Regulations, by-Laws, Guidelines, Notifications etc.	Documentary evidence to be submitted by the bidder as per Annexure – XVI.	
11.	Bidder should not have been debarred / black-listed by any Bank or RBI or ICAI or any other regulatory authority or Financial Institutions in India as on date of RFP submission.	Annexure-VI should be submitted	
12.	The bidder should ensure that there are no legal proceedings / inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	Self-declaration to this effect on the company's letterhead should be submitted.	
13.	Bidders who are party to any ongoing/pending/contemplated litigation with UCO Bank, shall not be allowed to participate in this tender.	A self-declaration to this effect must be submitted along with the technical bid.	

FORMAT OF EARNEST MONEY DEPOSIT (EMD)

To,
Deputy General Manager (DIT-Procurement & Infrastructure)
UCO Bank, Head Office-II,
3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir,

Ref: GeM bid no _____

In response to your invitation to respond to your bid for Selection of IS Audit Firm/Organization for Information Systems Audit. I, M/s _____ having their registered office at _____(hereinafter called the 'Vendor') wish to respond to the said bid for self and other associated vendors and submit the proposal to Selection of IS Audit Firm/Organization for Information Systems Audit, as listed in the bid document.

Whereas the 'Vendor' has submitted the proposal in response to bid, we, the _____Bank having our Head office _____hereby irrevocably guarantee an amount of ` _____/- (Rupees _____ only) as EMD as required to be submitted by the 'Vendor' as a condition for participation in the said process of bid.

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

If the Vendor withdraws his proposal during the period of the proposal validity;

Or

If the Vendor, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the bid or the terms and conditions mutually agreed subsequently.

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 bid 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 vendor.

Notwithstanding anything contained herein:

1. Our liability under this Bank guarantee shall not exceed ` _____ (Rupees _____ only).
2. This Bank guarantee will be valid up to ____; 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_____.

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

Yours faithfully,

For and on behalf of

_____ Bank

Authorised official

(NB: This guarantee will require stamp duty as applicable and shall be signed by the official whose signature and authority shall be verified. The signatory shall affix his signature, name and designation).



Performa for Performance Bank Guarantee
(To be stamped in accordance with the stamp act)

1. In consideration of UCO BANK, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertaking) Act, 1970, having its head office at 10 BIPLABI TRILOKYA MAHARAJ SARANI (BRABOURNE ROAD), Kolkata-700001 (hereinafter called "UCO BANK") having agreed to exempt **M/s** _____, a Company incorporated under the Companies Act, 1956 having its registered office at (Address of the selected bidder company) (hereinafter called "the said SELECTED BIDDER") from the demand, under the terms and conditions of UCO BANK's purchase order/ Letter of Intent bearing no.dated..... issued to the Selected bidder and an Agreement to be made between UCO Bank and the Selected bidder for a period of In pursuance of Request For Proposal no.....dated....., as modified, (hereinafter called "the said Agreement"), of security deposit for the due fulfillment by the said SELECTED BIDDER of the Terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs.....(Rupees.....Only).We,..... [indicate the name of the bank ISSUING THE BANK GUARANTEE] (hereinafter referred to as "the Bank") at the request of [SELECTED BIDDER] do hereby undertake to pay to UCO BANK an amount not exceeding Rs.....against any loss or damage caused to or suffered or would be caused to or suffered by UCO BANK by reason of any breach by the said SELECTED BIDDER of any of the terms or conditions contained in the said Agreement.
2. We [indicate the name of the bank ISSUING THE BANK GUARANTEE] do hereby undertake to pay the amounts due and payable under this guarantee without any demur, merely on a demand from UCO BANK stating that the amount claimed is due by way of loss or damage caused to or breach by the said SELECTED BIDDER of any of the terms or conditions contained in the said Agreement or by reason of the SELECTED BIDDER'S failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs.....
3. We undertake to pay to UCO BANK any money so demanded notwithstanding any dispute or disputes raised by the SELECTED BIDDER in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal. The payment as made by us under this bond shall be a valid discharge of our liability for payment there under and the SELECTED BIDDER for payment there under and the SELECTED BIDDER shall have no claim against us for making such payment.

4. We,[indicate the name of the Bank ISSUING THE GUARANTEE] further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of BANK under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till UCO BANK certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said SELECTED BIDDER and accordingly discharged this guarantee. Unless a demand or claim under this guarantee is made on us in writing on or before(Expiry of claim period), we shall be discharged from all liabilities under this guarantee thereafter.
5. We [indicate the name of Bank ISSUING THE GUARANTEE] further agree with UCO BANK that UCO BANK shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or to extend time of performance by the said SELECTED BIDDER from time to time or to postpone for any time, or from time to time any of the powers exercisable by UCO BANK against the said SELECTED BIDDER and to forebear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any variation, or extension being granted to the said SELECTED BIDDER or for any forbearance, act or omission on the part of UCO BANK of any indulgence by UCO BANK to the said SELECTED BIDDER or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.
6. This guarantee will not be discharged due to the change in the constitution of the Bank or the SELECTED BIDDER.
7. We, [indicate the name of Bank ISSUING THE GUARANTEE] lastly undertake not to revoke this guarantee during its currency except with the previous consent of UCO BANK in writing.

Notwithstanding anything contained herein:

- a. Our liability under this Bank Guarantee shall not exceed Rs..... (Rupees.....) Only.
- b. This Bank Guarantee shall be valid uptoand
- c. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before(date of expiry of Guarantee including claim period).
8. Dated the day of for [indicate the name of Bank]

Yours' faithfully,

For and on behalf of

_____ Bank

Authorised Official

NOTE:

1. Selected bidder should ensure that the seal and CODE No. of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bidder guarantee issued by banks located in India shall be on a Non-Judicial Stamp Paper of requisite value as applicable to the place of execution.



INTEGRITY PACT

(To be stamped as per the Stamp Law of the Respective State)

1. Whereas UCO Bank having its registered office at 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 acting through its Department of IT, represented by Authorised Signatory hereinafter referred to as the Buyer and the first party, proposes to provide Information Systems Audit services, hereinafter referred to as Stores and / or Services. And **M/s**_____ **having its registered office at**_____ **represented by**_____ **Authorised signatory**, (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignee), hereinafter referred to as the bidder/seller and the second party, is willing to offer/has offered the Stores and / or Services.

2. Whereas the Bidder/Seller is a private company/public company/ /partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Public Sector Undertaking and registered under Companies Act 1956. Buyer and Bidder/Seller shall hereinafter be individually referred to as —Party or collectively as the —parties, as the context may require.

3. Preamble

Buyer has called for tenders under laid down organizational procedures intending to enter into contract /s for Procurement of providing Information Systems Audit services and the Bidder /Seller is one amongst several bidders /Proprietary Vendor /Customer Nominated Source/Licenser who has indicated a desire to bid/supply in such tendering process. The Buyer values and takes primary responsibility for values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder (s) and / or Seller(s).

In order to achieve these goals, the Buyer will appoint Independent External Monitor(s) (IEMs) in consultation with Central Vigilance Commission, who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

4. Commitments of the Buyer

4.1 The Buyer commits itself to take all measures necessary to prevent corruption and fraudulent practices and to observe the following principles: -

- (i) No employee of the Buyer, personally or through family members, will in connection with the tender, or the execution of a contract demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
- (ii) The Buyer will during the tender process treat all Bidder(s) /Seller(s) with equity and reason. The Buyer will in particular, before and during the tender process, provide to all Bidder (s) /Seller(s) the same information and will not provide to any Bidders(s) /Seller(s) confidential /additional information through which the Bidder(s) / Seller(s) could obtain an advantage in relation to the process or the contract execution.
- (iii) The Buyer will exclude from the process all known prejudiced persons.

4.2 If the Buyer obtains information on the conduct of any of its employees which is a criminal offence under the Indian Legislation Prevention of Corruption Act 1988 as amended from time to time or if there be a substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer and in addition can initiate disciplinary action.

5 Commitments of the Bidder(s) /Seller(s):

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

- (i) The Bidder(s) /Seller(s) will not directly or through any other persons or firm, offer promise or give to any of the Buyer's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in exchange any advantage during the tendering or qualification process or during the execution of the contract.
- (ii) The Bidder(s) /Seller(s) will not enter with other Bidders / Sellers into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
- (iii) The bidder(s) /Seller(s) will not commit any offence under the Indian legislation, Prevention of Corruption Act, 1988 as amended from time to time. Further, the Bidder(s) /Seller(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Buyer as part of the business relationship, regarding plans, technical proposals and business details, including information constrained or transmitted electronically.

- (iv) The Bidder(s) /Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s) / sub-contractor(s), if any, Further, the Bidder /Seller shall be held responsible for any violation/breach of the provisions by its sub-supplier(s) /Sub-contractor(s).
- (v) Foreign bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principals or associates.
- (vi) Bidders not to pass any information provided by the Principal as part of business relationship to others and not to commit any offence under PC/IPC Act.
- (vii) Bidders to disclose the payments to be made by them to agents/brokers or any other intermediary.

5.2 The Bidder(s) /Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s) / sub-contractor(s), if any, Further, the Bidder /Seller shall be held responsible for any violation /breach of the provisions by its sub-supplier(s) /sub-contractor(s).

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

5.4 Agents / Agency Commission

The Bidder /Seller confirms and declares to the Buyer that the bidder/Seller is the original manufacturer/authorized distributor / stockiest of original manufacturer or Govt. Sponsored /Designated Export Agencies (applicable in case of countries where domestic laws do not permit direct export by OEMS of the stores and /or Services referred to in this tender / Offer / contract / Purchase Order and has not engaged any individual or firm, whether Indian or Foreign whatsoever, to intercede, facilitate or in any way to recommend to Buyer or any of its functionaries, whether officially or unofficially, to the award of the tender / contract / Purchase order to the Seller/Bidder; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller / Bidder agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in anyway incorrect or if at a later stage it is discovered by the Buyer that the Seller incorrect or if at a later stage it is discovered by the Buyer that the Seller/Bidder has engaged any such individual /firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this contract /Purchase order, the Seller /Bidder will be liable to refund that amount to the Buyer. The Seller will also be debarred from participating in any Tender for new projects / program with Buyer for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract / Purchase order either wholly or in part, without any entitlement of compensation to the Seller /Bidder who shall in such event be liable to refund agents

/ agency commission payments to the buyer made by the Seller /Bidder along with interest at the rate of 2% per annum above LIBOR (London Inter Bank Offer Rate) (for foreign vendors) and Base Rate of SBI (State Bank of India) plus 2% (for Indian vendors). The Buyer will also have the right to recover any such amount from any contracts / Purchase order concluded earlier or later with Buyer.

6. Previous Transgression

6.1 The Bidder /Seller declares that no previous transgressions have occurred in the last three years from the date of signing of this Integrity Pact with any other company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprise in India that could justify Bidder's /Seller's exclusion from the tender process.

6.2 If the Bidder /Seller makes incorrect statement on this subject, Bidder /Seller can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason without any liability whatsoever on the Buyer.

7. Company Code of Conduct

Bidders /Sellers are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behaviour) and a compliance program for the implementation of the code of conduct throughout the company.

8. Sanctions for Violation

8.1 If the Bidder(s) /Seller(s), before award or during execution has committed a transgression through a violation of Clause 5, above or in any other form such as to put his reliability or credibility in question, the Buyer is entitled to disqualify the Bidder(s) /Seller (s) from the tender process or take action as per the procedure mentioned herein below:

- (i) To disqualify the Bidder /Seller with the tender process and exclusion from future contracts.
- (ii) To debar the Bidder /Seller from entering into any bid from Buyer for a period of two years.
- (iii) To immediately cancel the contract, if already signed /awarded without any liability on the Buyer to compensate the Bidder /Seller for damages, if any. Subject to Clause 5, any lawful payment due to the Bidder/Seller for supplies effected till date of termination would be made in normal course.
- (iv) To encash Advance Bank Guarantees / Performance Bonds / Warranty Bonds, etc. which may have been furnished by the Bidder /Seller to the extent of the undelivered Stores and / or Services.

8.2 If the Buyer obtains Knowledge of conduct of Bidder /Seller or of an employee or representative or an associate of Bidder /Seller which constitutes corruption, or if the Buyer has substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer.

9. Compensation for Damages

9.1 If the Buyer has disqualified the Bidder(s) /Seller(s) from the tender process prior to the award according to Clause 8, the Buyer is entitled to demand and recover the damages equivalent to Earnest Money Deposit in case of open tendering.

9.2 If the Buyer has terminated the contract according to Clause 8, or if the Buyer is entitled to terminate the contract according to Clause 8, the Buyer shall be entitled to encash the advance Bank guarantee and performance bond / warranty bond, if furnished by the Bidder / Seller, in order to recover the payments, already made by the Buyer for undelivered Stores and / or Services.

10. Price Fall Clause

The Bidder undertakes that it has not supplied /is not supplying same or 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/PSBs during the currency of the contract and if it is found at any stage that same or similar product /Systems or Subsystems was supplied by the Bidder to any other Ministry /Department of the Government of India or a PSU or any Public Sector Bank at a lower price during the currency of the contract, then that very price 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.

11. Independent External Monitor(s)

11.1 The Buyer has appointed independent External Monitors for this Integrity Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors are given in ATC).

11.2 As soon as the integrity Pact is signed, the Buyer shall provide a copy thereof, along with a brief background of the case to the independent External Monitors.

11.3 The Bidder(s) / Seller(s) if they deem it necessary, May furnish any information as relevant to their bid to the Independent External Monitors.

11.4 If any complaint with regard to violation of the IP is received by the buyer in a procurement case, the buyer shall refer the complaint to the Independent External Monitors for their comments / enquiry.

11.5 If the Independent External Monitors need to peruse the records of the buyer in connection with the complaint sent to them by the buyer, the buyer shall make arrangement for such perusal of records by the independent External Monitors.

11.6 The report of enquiry, if any, made by the Independent External Monitors shall be submitted to MD & CEO, UCO Bank, Head Office at 10, Biplabi Trailokya Maharaj Sarani, Kolkata-700001 within 2 weeks, for a final and appropriate decision in the matter keeping in view the provision of this Integrity Pact.

11.7 The word "Monitor" would include both singular and plural.

12. Law and Place of Jurisdiction

This Integrity Pact is subject to Indian Laws, and exclusive Jurisdiction of Courts at Kolkata, India.

13. 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 provision of the extant law in force relating to any civil or criminal proceedings.

14. Integrity Pact Duration.

14.1 This Integrity Pact begins when both parties have legally signed it. It expires of order / finalization of contract.

14.2 If any claim is made/ lodged during this time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by MD & CEO, UCO Bank.

14.3 Should one or several provisions of this Integrity Pact turn out to be invalid, the reminder of this Integrity Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

15 Other Provisions

15.1 Changes and supplements need to be made in writing. Side agreements have not been made.

15.2 The Bidders (s)/ Sellers (s) signing this IP shall not initiate any Legal action or approach any court of law during the examination of any allegations/complaint by IEM and until the IEM delivers its report.

15.3 In view of nature of this Integrity Pact, this Integrity Pact shall not be terminated by any party and will subsist throughout its stated period.

15.4 Nothing contained in this Integrity Pact shall be deemed to assure the bidder / Seller of any success or otherwise in the tendering process.

16. This Integrity Pact is signed with UCO Bank exclusively and hence shall not be treated as precedence for signing of IP with MoD or any other Organization.

17. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

18. The Parties here by sign this Integrity Pact.

BUYER

Signature:

Authorized Signatory

Department of IT

Place:

Date:

Witness:

(Name & Address)

BIDDER /SELLER

Signature:

Authorized Signatory (*)

Witness:

(Name & Address)



NON-DISCLOSURE AGREEMENT

(Confirmation of format should be enclosed with technical bid. Agreement to be executed on non-judicial stamp paper of requisite value by the selected bidder only,)

This Non-Disclosure Agreement is entered into on this Day of..... 2025

BETWEEN

UCO Bank, a body corporate, constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 as amended from time to time having its Head Office at No.10, BTM Sarani, Kolkata-700001 hereinafter referred to as **"the Bank"** (which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its assigns, administrators and successors) **of the FIRST PART/ DISCLOSING PARTY**

AND

.....(Which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its assigns, administrator and successors) of the **SECOND PART/ RECEIVING PARTY**
(Each of Bank and the vendor is sometimes referred to herein as a **"Party"** and together as the **"Parties"**).

WHEREAS the Vendor/Receiving Party is inter alia engaged to provide Information Systems Audit services as per the terms and conditions specified in the GeM bid Ref. No: _____. The Vendor/Receiving Party would be the single point of contact for this project.

WHEREAS Bank/Disclosing Party is inter alia engaged in the business of Banking; and

WHEREAS the Parties presently desire to discuss and/or consult with each other's business for the purposes of entering into Agreements to provide Information Systems Audit services.

WHEREAS the Parties recognize that each other's business involves specialized and proprietary knowledge, information, methods, processes, techniques and skills peculiar to their security and growth and that any disclosure of such methods, processes, skills, financial data, or other confidential and proprietary information would substantially injure a Party's business, impair a Party's investments and goodwill, and jeopardize a Party's relationship with a Party's clients and customers; and

WHEREAS in the course of consultation with respect to the potential business venture, the Parties anticipate disclosing to each other certain information of a novel,

proprietary, or confidential nature, and desire that such information be subject to all of the terms and conditions set forth herein below;

NOW THEREFORE the Parties hereto, in consideration of the promises and other good and valuable consideration, agree such information shall be treated as follows:

(2) **Confidential Information.** "**Confidential Information**" shall mean and include any information which relates to the financial and/or business operations of each Party, including but not limited to, specifications, drawings, sketches, models, samples, reports, forecasts, current or historical data, computer programs or documentation and all other technical, financial or business data, information related to each Party's customers, products, processes, financial condition, employees, intellectual property, manufacturing techniques, experimental work, trade secrets.

(3) **Use of Confidential Information.** The Vendor/Receiving Party agrees not to use the Bank/Disclosing Party's confidential Information for any purpose other than for the specific consultation regarding the potential business venture. Any other use of such Confidential Information by the Receiving Party shall be made only upon the prior written consent from an authorized representative of the Disclosing Party which wishes to disclose such information or pursuant to subsequent agreement between the Parties hereto.

3. Restrictions. Subject to the provisions of paragraph 4 below, the Party receiving Confidential Information (the "**Receiving Party**") shall, for contract period of Three (3) years from the date of the last disclosure of Confidential Information made under this Agreement (except for personal customer data which shall remain confidential forever), use the same care and discretion to limit disclosure of such Confidential Information as it uses with similar confidential information of its own and shall not disclose, lecture upon, publish, copy, modify, divulge either directly or indirectly, use (except as permitted above under clause (2) or otherwise transfer the Confidential Information to any other person or entity, including taking reasonable degree of care and steps to:

(a) Restrict disclosure of Confidential Information solely to its concerned employees, agents, advisors, consultants, contractors and /or subcontractors with a need to know and not disclose such proprietary information to any other parties; and

(b) Advise all receiving Party's employees with access to the Confidential Information of the obligation to protect Confidential Information provided hereunder and obtain from agents, advisors, contractors and/or consultants an agreement to be so bound.

I Use the Confidential Information provided hereunder only for purposes directly related to the potential business venture.

4. Exclusions. The obligations imposed upon Receiving Party herein shall not apply to information, technical data or know how, whether or not designated as confidential, that:

(a) is already known to the Receiving Party at the time of the disclosure without an obligation of confidentiality;

(b) is or becomes publicly known through no unauthorized act of the Receiving Party;

(c) is rightfully received from a third Party without restriction and without breach of this Agreement;

(d) is independently developed by the Receiving Party without use of the other Party's Confidential Information and is so documented;

(e) is disclosed without similar restrictions to a third party by the Party owning the Confidential Information;

(f) is approved for release by written authorization of the Disclosing Party; or

(g) is required to be disclosed pursuant to any applicable laws or regulations or any order of a court or a governmental body; provided, however, that the Receiving Party shall first have given notice to the Disclosing Party and made a reasonable effort to obtain a protective order requiring that the Confidential Information and/or documents so disclosed be used only for the purposes for which the order was issued.

(4) Return of Confidential Information. All Confidential Information and copies and extracts of it shall be promptly returned by the Receiving Party to the Disclosing Party at any time within thirty (30) days of receipt of a written request by the Disclosing Party for the return of such Confidential Information.

(5) Ownership of Information. The Receiving Party agrees that all Confidential Information shall remain the exclusive property of the Disclosing Party and its affiliates, successors and assigns.

(6) No License Granted. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in any Confidential Information disclosed to the Receiving Party or to any information, discovery or improvement made, conceived, or acquired before or after the date of this Agreement. No disclosure of any Confidential Information hereunder shall be construed by the Receiving Party to be a public disclosure of such Confidential Information for any purpose whatsoever.

(7) Breach. In the event the Receiving Party discloses, disseminates or releases any Confidential Information received from the Disclosing Party, except as provided above, such disclosure, dissemination or release will be deemed a material breach of this Agreement and the Disclosing Party shall have the right to demand prompt return of all Confidential Information previously provided to the Receiving Party and in such case, the Receiving party shall be bound to return all information within 30 days from the date of such demand. The provisions of this paragraph are in addition to any other legal right or remedies, the Disclosing Party may have under the Law for the time being in force.

(8) Arbitration and Equitable Relief.

(9) Arbitration. The Parties shall endeavor to settle any dispute/difference arising out of or relating to this Agreement through consultation and negotiation. In the event no settlement can be reached through such negotiation and consultation, the Parties agree that such disputes shall be referred to and finally resolved by arbitration under the provisions of the Arbitration and Conciliation Act, 1996 and the rules made thereunder from time to time. The arbitration shall be held at city of Head Office of member Bank. The language used in the arbitral proceedings shall be English. The arbitration proceeding shall be conducted by a panel of three arbitrators, each party shall appoint his own arbitrator and the two appointed arbitrators shall appoint the third arbitrator who shall act as presiding Arbitrator.

(b) Equitable Remedies. The Parties agree that in event of breach of any of the covenants contained in this Agreement due to negligence/fault/lack of the Receiving Party, the Disclosing party shall have, in addition to any other remedy, the right:

- i) To obtain an injunction from a court of competent jurisdiction restraining such breach or threatened breach; and
- ii) To specific performance of any such provisions of this Agreement. The Parties further agree that no bond or other shall be required in obtaining such equitable relief and the Parties hereby consent to the issuance of such injunction and to the ordering of specific performance.

I Legal Expenses: If any action and proceeding is brought for the enforcement of this Agreement, or because of an alleged or actual dispute, breach, default, or misrepresentation in connection with any of the provisions of this Agreement, each Party will bear its own expenses, including the attorney's fees and other costs incurred in such action.

(d) Indemnification: The Receiving Party shall indemnify the Bank and hold the Bank harmless against any loss caused to it as a result of the non-performance or improper performance of this Agreement by the Receiving Party, or its servants or agents to

perform any aspect of its obligations forming part of the subject matter of this Agreement.

10. Term. This Agreement may be terminated by either Party giving sixty (60) days' prior written notice to the other Party; provided, however, the obligations to protect the Confidential Information in accordance with this Agreement shall survive for a period of three (3) years from the date of the last disclosure of Confidential Information made under this Agreement (except for personal customer data which shall remain confidential forever).

11. No Formal Business Obligations. This Agreement shall not constitute create, give effect to or otherwise imply a joint venture, pooling arrangement, partnership, or formal business organization of any kind, nor shall it constitute, create, give effect to, or otherwise imply an obligation or commitment on the part of either Party to submit a proposal or to perform a contract with the other Party or to refrain from entering into an agreement or negotiation with any other Party. Nothing herein shall be construed as providing for the sharing of profits or loss arising out of the efforts of either or both Parties. Neither Party will be liable for any of the costs associated with the other's efforts in connection with this Agreement. If the Parties hereto decide to enter into any licensing arrangement regarding any Confidential Information or present or future patent claims disclosed hereunder, it shall only be done on the basis of a separate written agreement between them.

12. General Provisions.

(10) Governing Law. This Agreement shall be governed by and construed in accordance with the laws of India.

(b) Severability. If one or more of the provisions in this Agreement is deemed void by law, then the remaining provisions shall remain valid and continue in full force and effect.

I Successors and Assigns. This Agreement will be binding upon the successors and/or assigns of the Parties, provided however that neither Party shall assign its rights or duties under this Agreement without the prior written consent of the other Party.

(d) Headings. All headings used herein are intended for reference purposes only and shall not affect the interpretation or validity of this Agreement.

I Entire Agreement. This Agreement constitutes the entire agreement and understanding of the Parties with respect to the subject matter of this Agreement. Any amendments or modifications of this Agreement shall be in writing and executed by a duly authorized representative of the Parties.

(f) Jurisdiction of Court: All disputes under this Non-Disclosure Agreement are subject to the jurisdiction of Courts at City of Head office of Individual member Bank in India.

(g) Two original sets of Non-Disclosure Agreement are executed and retained by either parties, Bank and _____ (*the selected vendor*)

The Parties, by the signature of their authorized representatives appearing below, acknowledge that they have read and understood each and every term of this Agreement and agree to be bound by its terms and conditions.

For and on behalf of

.....

Signature: _____

Name: _____

Designation: _____

Date: _____

for and on behalf of

.....

(The selected bidder)

Signature: _____

Name: _____

Designation: _____

Date: _____



UNDERTAKING FOR NON-BLACKLISTING / NON-DEBARMENT OF THE BIDDER
(TO BE EXECUTED ON NON-JUDICIAL STAMP PAPER OF REQUISITE VALUE & DULY
ATTESTED BY A NOTARY)

Sub: Selection of IS Audit Firm/Organization for Information Systems Audit

- 1) I/We, Proprietor/Partner(s)/Director(s) of M/s..... hereby confirm that I/We have read and understood the eligibility criteria and fulfil the same.
- 2) I/We further confirm that all the information furnished by me/us, as per the requirement of the Bank, have been included in our bid.
- 3) I/We further hereby undertake and agree to abide by all terms and conditions and guidelines stipulated by the Bank. We understand that any deviation may result in disqualification of our bid.
- 4) *I/We further hereby declare that I/We have not been black-listed or otherwise debarred by any Bank/Financial Institution/Central Government/ State Government/any Central or State Undertaking or Corporation/ Reserve Bank of India or any other Regulatory Authority or any other Statutory Authority as on date of the submission of this Tender/Procurement.

(OR)

I/We further hereby declare that the Proprietorship Concern/Partnership Firm/Company/..... (if any other entity) namely M/s was blacklisted/debarred by.....(Name of the Authority who blacklisted/debarred) from taking part in their Tender/Procurement for a period ofyears w.e.f.to..... The period is subsisting/over on.....and now I/We is/are entitled to take part in Tender/Procurement.

- 5) I/We declare that no proceedings/inquiries/investigations have commenced/pending against me/us by any Statutory Authority/Regulatory Agency/Investigating Agency which may result in liquidation of company/ firm/proprietorship concern and/or may act as deterrent on the continuity of business and/or may hamper in providing the said services, as envisaged in this document.
- 6) I/We further hereby declare that no legal action is pending against me/us for any cause in any legal jurisdiction.

- 7) I/We undertake that adequate number of resources, if required by the Bank, will be deployed for the project to complete the assignment within the stipulated time.

***STRIKE OUT WHICH IS INAPPLICABLE**

(Deviation to the above if any, the Bidder must provide details of such action(s))

Signature (1) (2)

(duly authorized to sign)

Name:.....

Capacity in which as executed:.....

Name & registered address of the Bidder:.....

Seal of the Bidder to be affixed



General Details of the Bidder**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. Major change in Management in last three years:
6. Names of Banker /s:
7. Name & Contact Details of Authorized Signatory:

B. Financial Position of Bidder for the last three financial years

	2021-22	2022-23	2023-2024
Net Worth			
Turnover			
Net Profit (Profit After Tax)			

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:
 - In PSU banks
 - In non-PSU banks
 - In any other government organisation

D. Details of Experience in implementation of similar orders

Sl. No.	Name of Organisation	Description of application	Period during which installed	
			From	To

Place:

Date:

Authorised Signatory

Name:

Designation:

UNDERTAKING FOR PRICE VALIDITY & ACCEPTANCE OF ALL TERMS & CONDITIONS OF RFP

To,
Deputy General Manager (DIT-Procurement & Infrastructure)
UCO Bank, Head Office-II,
3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir,

Sub: Selection of IS Audit Firm/Organization for Information Systems Audit

We understand that Bank is not bound to accept the lowest or any bid received, and Bank may reject all or any bid. We shall keep the price valid for the entire contract period from the date of issuance of the first Work order.

If our bid is accepted, we are responsible for the due performance as per the scope of work and terms & conditions as per mentioned in RFP.

It is certified that the information furnished here in and as per the document submitted is true and accurate and nothing has been concealed or tampered with. We have gone through all the conditions of bid and are liable to any punitive action for furnishing false information / documents.

Yours faithfully,

For.....

(Signature and seal of authorized person) Place:

Date:

Undertaking for No Deviation

To

Deputy General Manager (DIT-Procurement & Infrastructure)

UCO Bank, Head Office-II,

3&4, DD Block, Sector-I

Salt Lake, Kolkata -700064

Dear Sir,

Sub: Selection of IS Audit Firm/Organization for Information Systems Audit

Further to our proposal dated, in response to the Request for Proposal (Bank's tender No. hereinafter referred to as "**RFP**") issued by Bank, we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original tender documents if any, issued by the Bank. The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

We undertake to execute Deed of Indemnity, Non-disclosure Agreement & provide Performance Bank Guarantee as per the annexure enclosed in the RFP, in case of emergence as a successful bidder.

Yours faithfully,

For.....

Designation:

(Signature and seal of authorized person) Bidder's corporate name:

Place:

Date:

**Format of Pre-Bid Queries to be submitted by the Bidder(s)
(If queries submitted through e-mail)**

Sub : Selection of IS Audit Firm/Organization for Information Systems Audit

To be e-mailed in '.docx' format strictly

Name of the Bidder:

Name of the Contact Person of the Bidder:

Contact Number of the Contact Person:

Email id of the Contact Person:

Bid PageNo.	Bid ClauseNo.	Original Clause	Query sought/ Suggestions of the Bidder

Restriction on Procurement due to National Security

This Certificate should be submitted on the letterhead of the bidder duly signed by an authorized signatory

**To,
Deputy General Manager (DIT-Procurement & Infrastructure)
UCO Bank, Head Office-II,
3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064**

Dear Sir,

Sub: Selection of IS Audit Firm/Organization for Information Systems Audit

1. "I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India; I hereby certify that this bidder is not from such a country and is eligible to be considered."
2. "I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India; / certify that this bidder is not from such a country or, if from such a country, have been registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. (Where applicable, evidence of valid registration by the Competent Authority shall be attached.)"

Yours Faithfully,

Authorised Signatory,

Name:

Designation:

Vendors Corporate Name:

Address:

Email:

Contact No.

Technical Compliance Sheet

The IS Auditor shall broadly have technical capability to cover but not limited to the following Audit Types at defined frequency per Audit Round.

Sl. No.	Type of IS Audit	Frequency	Mandatory (M)/ Non-Mandatory (NM)	Bidder's capability to execute the Audit Types (Y/N)
1.	PENETRATION TESTING (PT) (EXTERNAL/INTERNAL)	Half Yearly	M	
2.	VULNERABILITY ASSESSMENT (VA)	Half Yearly/Quarterly, as applicable	M	
3.	APPLICATION AUDIT	Yearly	M	
4.	MIGRATION AUDIT	As and when required.	M	
5.	PROCESS AUDIT	Yearly	M	
6.	NETWORK ARCHITECTURE REVIEW	Yearly	M	
7.	FIREWALL RULE BASED REVIEW	Half Yearly	M	
8.	SOURCE CODE AUDIT/REVIEW	Yearly	M	
9.	DATABASE AUDIT	Yearly	M	
10.	KRIs and KPIs Prepared by CISO OFFICE	Quarterly	M	
11.	VA/PT OF INTERNET CONNECTED PCs	Half Yearly	M	
12.	SECURITY AUDIT OF CLOUD SERVICES	Yearly	M	
13.	PERFORMANCE TESTING	Yearly	M	
14.	AUDIT OF CHANGE LOGS	Quarterly	M	
15.	VENDOR & SITE AUDIT	Yearly	M	
16.	SECURE CONFIGURATION REVIEW/ CONFUGURATION AUDIT	Yearly	M	
17.	GOVERNANCE AUDIT	Yearly	M	
18.	AUDIT OF STORAGE OF PAYMENT SYSTEM DATA	Yearly	M	
19.	SYSTEM AUDIT REPORT (SAR) NSDL	Yearly	M	
20.	IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)	Yearly	M	
21.	PRE-IMPLEMENTATION AUDIT OF NEW APPLICATION (SECURITY & FUNCTIONAL)	As and when required.	M	

22.	AUDIT OF DIGITAL LENDING	Yearly	M	
23.	RBI CYBER SECURITY FRAMEWORK REVIEW	Yearly	M	
24.	SWIFT CSP Assessment	Yearly	M	
25.	AUDIT OF VIRTUAL MACHINES (VMs)	Yearly	M	
26.	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Yearly (One Time)	M	
	Limited audit shall be performed six months after the comprehensive audit	Half Yearly		
27.	Audit/ Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)	Yearly or as and when required.	M	
28.	Information Security Management System (ISMS) for ISO 27001:2022 Certification Sustenance	Yearly	M	
29	Forensic Audit/ Forensic Analysis/Investigations:	As and when required	M	
30	Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong	Yearly	NM	
31	MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore	Yearly	NM	

Note : Bidder should have capability to complete all mandatory audit works mentioned in table above. Conditional acceptance will not be allowed and bidder may be disqualified.

Authorized Signatory

(Name:

Phone No.:

Fax:

E-mail:

COMMERCIAL TEMPLATE
(TO BE SUBMITTED WITH COMMERCIAL BID)

Bidder needs to submit mask commercial template along with technical bid masking the PRICE.

Table A: Items for which auditing is required regularly

All Amount in INR (₹)

Sl. No	Particulars	Frequency per Year (A)	Amount per Audit reference including all expenses (excl. GST) (B)	GST (C)	Total Amount (for 2 Years) (D) = 2A * (B+C)
1	Fees for VULNERABILITY ASSESSMENT (VA) approximately 200-300 IPs related to PCI-DSS	4			
2	Fees for VULNERABILITY ASSESSMENT (VA) other than PCI-DSS Certification approx. 1000-1200 Server/devices	2			
3	Fees PENETRATION TESTING (PT) (EXTERNAL/INTERNAL) approx. 250 public facing/Internal applications/APIs	2			
4	Fees APPLICATION AUDIT	1			
5	Fees for Process Audit	1			
6	Fees for NETWORK ARCHITECTURE REVIEW	1			
7	Fees for FIREWALL RULE BASED REVIEW	2			
8	Fees for SOURCE CODE AUDIT/REVIEW	1			
9	Fees for DATABASE AUDIT	1			
10	Fees for KRIs and KPIs Prepared by CISO OFFICE	4			
11	Fees for VA/PT OF INTERNET CONNECTED PCs	2			
12	Fees for SECURITY AUDIT OF CLOUD SERVICES	1			
13	Fees for PERFORMANCE TESTING	1			
14	Fees for AUDIT OF CHANGE LOGS	4			
15	Fees for VENDOR AUDIT & SITE AUDIT	1			
16	Fees for SECURE CONFIGURATION REVIEW/AUDIT	1			
17	Fees for GOVERNANCE AUDIT	1			
18	Fees for AUDIT OF STORAGE OF PAYMENT SYSTEM DATA	1			
19	Fees for SYSTEM AUDIT REPORT (SAR) NSDL	1			
20	Fees for IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)	1			
21	Fees for AUDIT OF DIGITAL LENDING	1			

22	Fees for CYBER SECURITY FRAMEWORK REVIEW	1			
23	Fees for CYBER SECURITY FRAMEWORK Limited audit	2			
24	Fees for SWIFT Customer Security Program (CSP) Assessment	1			
25	Fees for AUDIT OF VIRTUAL MACHINES (VMs)	1			
26	Fees for Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	1			
27	Fees for Audit/Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)	1			
28	Fees for Sustenance of Information Security Management System (ISMS) for ISO 27001:2022 Certification	1			
29	Fees for Cyber Security Audit/ Assessment/ Risk Assessment as per C-RAF framework of HKMA for Hongkong Branch	1			
30	Fees for MAS Cyber Audit/ Risk Assessment as per TRM framework of MAS for Singapore	1			
31	Fees for Security cum Functional audit of new applications (approx. 200 Applications)	200 (As and when required - Conduct of Audit & Compliance Review/ to be paid on per application basis)			

Table B: Items for which auditing is not required at regular interval

Sl. No	Particulars	Amount including all expenses excluding GST (A)	GST as per the current rate applicable (B)	Amount (C) = (A)+(B)
1	Forensic Audit for 200 man-days			
2	Migration Audit (As & when required)			
3	Other Audit Man-day cost for 1000 man-days			
Total Cost (In figures)				
Total Cost (In words) _____				

Table-C TCO Calculation

Sl. No	Particulars	Amount including all expenses excluding GST (A)
1	Total Cost of Table A	XXXXX
2	Total Cost of Table B	XXXXX
3	TOTAL COST OF OWNERSHIP (TCO in figures) (Sl. No. 1 + Sl. No. 2)	XXXXX
4	TOTAL COST OF OWNERSHIP (TCO in words) (Sl No. 1 + Sl. No. 2)	XXXXX

The above quotation is subject to the following considerations: -

- a) Prices quoted are inclusive of Review Audit
- b) L1 bidder would be determined based on the Total Cost of Ownership (TCO) quoted by the bidder in **Table C** given above.
- c) The calculation for arriving at TCO is properly mentioned in the appropriate columns and we confirm that the above-mentioned rates are accurate. In case of any anomalies in the calculation for arriving at TCO, the Bank will have the right to rectify the same and it will be binding upon our company.
- d) GST will be paid at actuals at the time of resultant billing.
- e) The prices quoted above are for TCO (**Total Cost of Ownership**) calculation purposes only. Payment will be done on actual basis for completion of each activity as quoted above.
- f) The rate arrived shall be valid for the entire contract period.
- g) No counter condition/assumption in response to commercial bid will be accepted. Bank reserves the right to reject such bid.
- h) 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.
- i) 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.
- j) Providing commercial proposal in other than this format may lead to rejection of the bid.
- k) The fees amount submitted against each line-item will be frozen for two years (contract period)
- l) For calculation of TCO, Forensic Audit cost for 200 man-days is included. However, payment will be made on the actual no. of man-days incurred.
- m) For calculation of TCO, Security cum Functional audit of new applications (approx. 200 applications) is included. However, payment will be made on the actual no. of applications audited.
- n) If the man-days mentioned in point no. 3 of the above table B get exhausted, then the selected bidder has to keep the man-day cost valid for other audits for an additional 100% of the mentioned man-days
- o) We have ensured that the price information is filled in the Commercial Offer at appropriate column without any typographical or arithmetic errors. All fields have been filled in correctly.

- p) We have not added or modified any clauses / statements / recordings / declarations in the commercial offer, which is conditional and / or qualified or subjected to suggestions, which contain any deviation in terms & conditions or any specification.
- q) We have understood that in case of non-adherence to any of the above, our offer will be summarily rejected
- r) If the cost for any line item is indicated as zero or blank, then Bank may assume that the said item is provided to the Bank without any cost.
- s) Bank has discretion to keep any of the line item mentioned above as optional as per Bank's requirement.
- t) Present Rate of tax, if applicable, should be quoted in respective columns. The Bank will pay the applicable taxes for the above-mentioned tax type ruling at the time of actual delivery of service/implementation and resultant billing. However, no other tax type will be paid. The Octroi / Entry Tax will be paid extra, wherever applicable on submission of actual tax receipt.
- u) Please note that any commercial offer which is conditional and / or qualified or subjected to suggestions will also be summarily rejected. This offer shall not contain any deviation in terms & condition or any specifications, if so such offer will be summarily rejected.
- v) All prices should be quoted in Indian Rupees (INR) only.
- w) Bank will not communicate with OEM / OSD for any queries
- x) We have ensured that the price information is filled in the Commercial Offer at appropriate column without any typographical or arithmetic errors. All fields have been filled in correctly.
- y) In case of any discrepancy between figures and words, the amount in words shall prevail.
- z) The TCO (Total cost of ownership) will be inclusive of GST and other applicable taxes. However, the GST and other applicable taxes will be paid as per actuals



Place:

Date:

Signature of Bidder: _____

Name: _____

Business Address: _____

Details of Core Audit Team Member**Sub: Selection of IS Audit Firm/Organization**

Sl	Member Name	Working in firm/ organisation since	Major Projects handled
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			

We certify that the members of core team(as mentioned above) are permanent employees of our firm/organisation who hold Industry Standard Certifications CISA/ DISA/ CISSP/ CEH/ CISM/ CA (valid as on date) and requisite experience (minimum 3 years) to handle the work as per the scope.

Place:**Date:****Name:****AUTHORISED SIGNATORY****Designation:**

CV of Core Audit Team Member

Sub: Selection of IS Audit Firm/Organization
(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	

Place:**Date:****Name:****AUTHORISED SIGNATORY****Designation:**

Undertaking to abide by all by-laws / rules / regulations

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

To

Deputy General Manager (DIT-Procurement & Infrastructure)

UCO Bank, Head Office-II,

3&4, DD Block, Sector-I

Salt Lake, Kolkata -700064

Sub: Declaration-Cum-Undertaking regarding compliance with all statutory requirements

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, By-Laws, Guidelines, Notifications etc.

We hereby undertake and agree to abide by all the terms and conditions stipulated by the Bank in this bid including all annexure, addendum, corrigendum and amendments, if any. We certify that the services offered shall be in conformity with the terms & conditions and Scope of Work stipulated in the annexures of the said RFP.

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.

We also confirm that payment to the engaged employees shall be made in consonance with the Minimum Wages Act in vogue and their duty hours will also be as per applicable labour laws of country.

Dated this _____ day of _____, 2025 .

Place:

For M/s. [Seal and Signature(s) of the Authorized Signatory (s)]

(TO BE PROVIDED ON Rs.100/- STAMP PAPER)**Self-Certificate for Local Content****Tender name & reference number:** _____

Date: _____

I _____ S/o, D/o, W/o _____ resident of _____ do hereby solemnly affirm and declare as under:

That I will agree to abide by the terms and conditions of the Public Procurement (Preference to Make in India) Policy vide GOI Order no. P-45021/2/2017-PP (B.E.-II) dated 15.06.2017 (subsequently revised vide orders dated 28.05.2018, 29.05.2019 and 04.06.2020) MOCI order No. 45021/2/2017-PP (BE II) Dt.16th September 2020 & P- 45021/102/2019-BE-II-Part (1) (E50310) Dt.4th March 2021 and any subsequent modifications/Amendments, if any and

That the local content for all inputs which constitute the said item/service/work has been verified by me and I am responsible for the correctness of the claims made therein.

Tick (✓) and Fill the Appropriate Category	
<input type="checkbox"/>	I/We _____ [name of the supplier] hereby confirm in respect of quoted items that Local Content is equal to or more than 50% and come under “Class-I Local Supplier” category.
<input type="checkbox"/>	I/We _____ [name of the supplier] hereby confirm in respect of quoted items that Local Content is more than 20% but less than 50% and come under “Class-II Local Supplier” category.

The details of the location (s) at which the local value addition is made and the proportionate value of local content in percentage is given below:

Address	Percentage (%) of local content

For and on behalf of _____ (Name of firm/entity)

Authorized signatory

Name,

Designation

Contact No.

[Note: In case of procurement for a value in excess of Rs. 10 Crores, the bidders shall provide this certificate from statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.]

ESCALATION MATRIX OF ALL VERTICALS

(To be submitted on company letter head)

The escalation matrix up to top level of company is tabulated below in hierarchy-

Sr. No.	Particulars	Level-1 Escalation	Level-2 Escalation	Level-3 Escalation
1		Name: Phone No: Cell No: Email:	Name: Phone No: Cell No: Email:	Name: Phone No: Cell No: Email:

Yours faithfully,

Authorized Signatory (Name)

(Designation)



Note- Kindly mention escalation matrix of all verticals (services and support of the company). There should be a single point of contact of senior level for verticals.

TENDER OFFER FORWARDING LETTER

To,
Deputy General Manager (DIT-Procurement & Infrastructure)
UCO Bank, Head Office-II,
3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir,

Ref.: Selection of IS Audit Firms/Organizations for Information Systems Audit

With reference to the above RFP, having examined and understood the instructions including all Annexures, terms and conditions forming part of the Bid, we hereby enclose our offer for Selection of IS Audit Firms/Organizations for Information Systems Audit, as mentioned in the RFP document forming Technical as well as Commercial Bids being parts of the above referred Bid.

In the event of acceptance of our Technical as well as Commercial Bids by the Bank we undertake to commence work as per the terms & conditions of your purchase orders.

In the event of our selection by the bank for undertaking for RFP, we will submit a Performance Bank Guarantee for a sum equivalent to 10% of the project cost/Total Cost of Ownership (TCO) valid for a period of 27 months (24 months + claim period of three (3) months) from the date of SLA/Purchase Order (PO) for indemnifying any loss to the Bank.

We agree to abide by the terms and conditions of this tender offer till bid validity period from the date of bid opening and our offer shall remain binding upon us which may be accepted by the Bank any time before expiry of bid.

Until a formal contract is executed, this tender offer, together with the Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive

Dated this day of 2025

Signature: (In the Capacity of) Duly authorized to sign the tender offer for and on behalf of _____



UCO BANK

Department of Information Technology
Selection of IS Audit Firms/Organizations for Information Systems Audit

GeM Bid No: GEM/2025/B/6476847 dated 21.07.2025

Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s) Published on 14-08-2025

Sl. No	Bid Page No.	Bid Clause No.	Original Clause	Query sought/ Suggestions of the Bidder	Banks Response
1.		Existing Environment	Environment Control	What's the estimated number of systems/devices (servers, firewalls, endpoints, routers, etc.) expected to be covered in VAPT and config review?	The total no. of system/ Devices will be 1000-1200 approximately
2.	NA	General	Annexures to be submitted on non-judiciary stamp paper.	Kindly clarify whether all annexures that are required to be submitted on a non-judicial stamp paper of requisite value and duly attested by a notary can be provided on ₹100/- stamp paper.	Please refer stamp act of respective state where the agreement will be signed.
3.		Data Transfer Restrictions	General	Are there any legal or Bank-imposed restrictions on the export/transfer/storage of audit data (e.g., logs, code, screenshots) outside India or from servers to auditor systems?	The data cannot be carried out outside the Bank premises.
4.			General Queries	Is the vendor expected to perform retesting and verification audits post-mitigation? If so, how many cycles are included in the initial engagement.	Atleast one cycle of retesting and verification audit is to be completed after every mitigation.

5.	11	Functional Audit Retests	Security cum Functional Audit	Is there a limit to the number of retests for applications failing initial Security cum Functional Audit? What is the expected Bank turnaround on closure of gaps before the next audit round?	Atleast one cycle of retesting is to be completed. Expected turnaround time on closure of gaps will be as per criticality of the observation (15 days, 20 days, 30 days or 40 days) as per industry standard practice.
6.			General Queries	The RFP mentions integration with ITGRC—please specify the tool (e.g., Archer, ServiceNow, etc.) and expected format (CSV, API, etc.) for audit data upload.	The tool is Archer and expected format is CSV and .xlsx
7.			General Queries	Will the Bank maintain a pre-approved tool list (e.g., Nessus, Burp, etc.)? What is the expected approval timeline for new tools not on the CERT-IN list?	All tool is to be provided by the auditor. The bidder has to use standard tool only.
8.	General Query	General Query	General Query	Any security feature used for application? A. If others, please specify: B. Can this security feature be disabled for testing purpose: (Yes / No) Suggested Sample Answers SSL / Encryption/ Captcha / Digital Signature / OTP etc.	The details will be shared with selected bidder.
9.	General Query	General Query	General Query	Application Architecture Diagram Suggested Sample Answers and architecture diagram Please share the server details & detailed architecture diagram	The details will be shared with selected bidder.
10.	General Query	General Query	General Query	Arrangements for performance testing environment and its scale compared to the Production Environment	The details will be shared with selected bidder.

				Suggested Sample Answers e.g. 1/2 of Prod or 2/3 of Prod or if 1:1 is feasible?	
11.	General Query	General Query	General Query	<p>Business Process (scenarios) OR Scope of testing</p> <p>A. Total Number of key business processes or scenarios for Performance Testing (in scope)</p> <p>B. Do they have interdependency (i.e. Workflow model): (Yes / No)</p> <p>C. Transaction Rate: Transactions per hour (TPH)</p> <p>D. How many screens does each scenario have</p> <p>Suggested Sample Answers <u>Guidelines:</u> The number of processes needs to be identified based on Pareto's 80-20 rule i.e. using 20% of critical scenarios that contribute to 80% of total load, needs to be simulated e.g.: at any instant there are 200 concurrent (i.e. 10% of total active users are taken i.e. assume 2000 active users) 20% of main Scenarios which contribute maximum load and their rate given below: <Scenario> <Screen-count> <Transaction-rate></p> <p><u>Sample Answer:</u></p>	Details is already shared in RFP

				<p>A: 4 main scenarios: order create, modify, delete and file upload</p> <p>B: Yes: Orders created generate Order numbers which need to be used in 'order cancellation' scenario</p> <p>C: 500 Transactions per hour for the application (50% of this order creations' load and rest distributed in other scenarios)</p> <p>D: Create order [this scenario has 5 screens]</p> <p>Delete order[flow of 6 screens]</p> <p>modify order[flow of 7 screens]</p>	
12.	General Query	General Query	General Query	<p>Count and Names of the Applications to be tested.</p> <p>Please provide a brief description of the business purpose and functionality of the application to be Load & Performance tested</p> <p>Suggested Sample Answers</p> <p>user-facing web application</p> <p>user-facing mobile app</p> <p>mobile app for delivery team</p>	<p>Load and performance is to be tested for Public facing Mobile Banking Applications</p> <p>Other relevant details will be shared with selected bidder.</p>
13.	General Query	General Query	General Query	<p>Count, name/type & OS of Application Server? Please share the version details.</p> <p>Suggested Sample Answers</p> <p>4 app servers Apache Tomcat 7.0.34</p> <p> SUSE Linux Enterprise Server 11 64 bit</p>	<p>Application servers has MS Windows and/or Linux as OS.</p> <p>Other relevant details will be shared with selected bidder.</p>
14.	General Query	General Query	General Query	<p>Count, name/type & OS of DB Server? Please share the version details.</p> <p>Suggested Sample Answers</p> <p>1 DB server MySQL 5.6 Red Hat Enterprise Linux 6 64-bit</p>	<p>The details will be shared with selected bidder.</p>

15.	General Query	General Query	General Query	<p>Count, name/type & OS of Web Server? Please share the version details.</p> <p>Suggested Sample Answers 2 web servers Microsoft IIS 8.0 Microsoft Windows Server 2012 R2 Enterprise 64bit</p>	The details will be shared with selected bidder.
16.	General Query	General Query	General Query	<p>Do you need a detailed RCA of the performance issues. Want us to drilldown the issues at method-level or query-level</p> <p>Suggested Sample Answers e.g. Yes, it will be nice to have RCA and recommendations and we are ready to avail the benefits of this additional paid service</p>	<p>Only performance testing is required to detect the performance issue.</p> <p>Detailed RCA is not the Bank's requirement.</p>
17.	General Query	General Query	General Query	<p>Would you be interested in continuing the RCA service after GO-LIVE, to monitor the production servers 24*7 for few months? Note: This will be a separate service & proposal will be shared for this separately</p> <p>Suggested Sample Answers e.g. Yes, it will be nice to monitor Production servers during initial months after the release</p>	No
18.	General Query	General Query	General Query	<p>Load balancers used if any? Please share the version details.</p> <p>Suggested Sample Answers F5 Load balancer / Software Load balance, etc.</p>	The details will be shared with selected bidder.

19.	General Query	General Query	General Query	Please extend bid submission by 2 weeks.	Please refer corrigendum
20.	1	GeM Bid Document	Bid End Date/Time 12-08-2025 16:00:00	We would kindly request the Bank to extend it till 18 August 2025 16:00:00 allowing us to evaluate potential risk such as conflict of interest.	Please refer corrigendum
21.	General Query	General Query	General Query	<p>Pls share the frequency of testing for performance testing. Specify that commercials need to be submitted for how many rounds of PT</p> <p>Suggested Sample Answers e.g. Yes, just one time in a year. Give cost for 1 project (for 1 time) considering 2 rounds i.e. 1 before and 1 after tuning/optimizations</p>	Frequency of testing for performance testing is once in a year.
22.	General Query	General Query	General Query	<p>Type of application: Browser based / Client Server / Others/Mobile (native app or hybrid)</p> <p>A. Is the application accessible through Web Browser like IE,Firefox? B. If others, pls. specify C. Application access channels: (Intranet / Internet / Both) D. Are Cookies used in the application? E. Any dynamic values are getting generated in the application?</p> <p>Suggested Sample Answers Browser based, accessible through Chrome and firefox. Intranet application. Cookies are used. Yes, dynamics values are generated</p>	The details will be shared with selected bidder.

				like sessionIDs to maintain different sessions	
23.	General Query	General Query	General Query	<p>What application development platform or programming languages are used in developing the application? i.e. Business logic runs on which technology</p> <p>Suggested Sample Answers ASP.NET/J2EE/PHP etc. OR Android/iOS (if it's a mobile app)</p>	<p>Standard application development platform is being used for developing the application. Other relevant details will be shared with the selected bidder.</p>
24.	General Query	General Query	General Query	<p>What are the Success criteria for Performance Testing</p> <p>A. Expected Business Transactions per Hour (TPH)</p> <p>B. Pass percentage for each business process</p> <p>C. Page Response Time at LAN & over WAN (in sec.)</p> <p>D. Hardware Utilization (CPU & Memory)</p> <p>Suggested Sample Answers e.g. Response times < 5 secs CPU < 80%</p>	<p>The bidder has to perform Performance testing of the Mobile Banking Application as per the Bank's criteria.</p>
25.	General Query	General Query	General Query	<p>What is the authentication mode used by the Application?</p> <p>Suggested Sample Answers LDAP / Form based / SSO etc.</p>	<p>Different application has different mode of authentications. The details will be shared with selected bidder.</p>
26.	General Query	General Query	General Query	<p>What is the expected numbers of Concurrent Users for Load Test?</p> <p>a) Expected concurrent users which will access the application through Web</p>	<p>The bidder has to perform stress testing as per the Bank's criteria.</p>

				<p>b) Expected concurrent users which will access the application through Mobile App (if any)</p> <p>What is the expected numbers of Concurrent Users for Stress Tests? (1.5X or 2X of Load)</p> <p>Suggested Sample Answers <u>Guidelines:</u> 10% of total active users are considered for concurrent user count i.e. assume there are 2000 active users, then 200 users concurrent tests can be targetted.</p> <p><u>Sample Answer:</u> 100 / 200 / 500 / 1000 etc.</p>	
27.	2	I-6	Firewall Rule Based Review	<p>Number of firewalls and make to be covered in this scope.</p>	<p>There are approximately 20 firewalls to be covered in this scope. Other relevant details will be shared with the selected bidder.</p>
28.	2	I-7	Source Code Audit	<p>Any possibility to get bifurcation of in house developed software and outsourced software. Lines of codes for in house developed software. This will help us to estimate right efforts. Also confirm whether we need to perform source code review or we need to review the reports and certificates for the same.</p>	<p>Please refer page 27 of ATC for further details related to "Source Code Review".</p> <p>Clause is self-explanatory.</p>
29.	4	3. Eligibility Criteria , SI# 6	Bidder should have industry-wide presence and expertise in conducting Information Systems (IS)	<p>(i) Requesting to include [State Cooperative Banks] in addition to SCBs, SFBs, Payment Banks.</p>	<p>Clause stands as per RFP.</p>

			<p>Audit including VA-PT, Business understanding related to Banking sector, good track record and must have prior experience of conducting such audit/ special audit, mentioned below, of any Bank in India (SCBs, SFBs, Payment Banks) in last 5 years.</p> <p>The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last two financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India.</p>	<p>(ii)The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last two financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India / [State Cooperative Bank]</p>	
30.	4	5	<p>The bidder must be having core audit team of minimum 20 members having permanent employees who hold Industry Standard Certifications CISA/DISA/ CISSP/ CEH/ CISM/ CA (valid as on date) and requisite experience (minimum 3 years) to handle the work as per the scope.</p>	<p>Kindly modify as below</p> <p>The bidder must be having core audit team of minimum 20 members having permanent employees who hold Industry Standard Certifications CISA/DISA/ CISSP/ CEH/ CISM/ CA/eJPT/Ewpt,emapr, Security+, Any other cybersecurity certification (valid as on date) and requisite experience (minimum 3 years) to handle the work as per the scope.</p>	<p>Clause stands as per RFP.</p>

31.	4	Part -I, Clause 3, point 4	<p>The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last two financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India.</p>	<p>We are engaged by multiple scheduled commercial Bank for IS audit however, most of the projects are on-going. Given the fact, we would request the Bank to amend the clause as follows:</p> <p>The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last three financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India.</p> <p>We would also request the Bank to consider below as the part of completion of the project:</p> <ol style="list-style-type: none"> 1. Completion Certificates 2. Project Sign-Offs 3. Satisfactory client certificate 4. Completed payment receivable certificate from CA firm 	Clause stands as per RFP
32.	4	Part -I, Clause 3, point 4	<p>The bidder should also have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed at least one full cycle of Information Systems (IS) Audit in last two financial years, for a minimum of one (01) no. of Scheduled commercial Bank in India.</p>	<p>We, "The Bidder" understood that last two financial years is financial years 2022-23 & 2023-24. Kindly confirm.</p>	Bidder's understanding is correct.

33.	4	Part -I, Clause 3, point 4	The bidder should be an empanelled Security Audit Firm with CERT-IN as on bid submission date.	<p>Given the scope of the audit and the risk in the project, we would request the Bank to amend the clause as follows:</p> <p>The bidder should be an empanelled Security Audit Firm with CERT-IN as on bid submission date since last 3 years.</p>	Clause stands as per RFP.
34.	4	Part -I, Clause 3, point 2	<p>The bidder should have a minimum annual turnover of Rs. 2.5 Crore per year during the last three financial years i.e. 2021-22, 2022-23 & 2023-24 .</p> <p>This must be the individual company turnover and not of any group of companies.</p>	<p>Given the scope of the audit and the risk in the project, we would request the Bank to amend the clause as follows:</p> <p>The bidder should have a minimum annual turnover of Rs. 25 Crore per year during the last three financial years i.e. 2021-22, 2022-23 & 2023-24 .</p> <p>This must be the individual company turnover and not of any group of companies.</p>	Clause stands as per RFP.
35.	4	3. Eligibility Criteria , Sl# 2	The bidder should have a minimum annual turnover of Rs. 2.5 Crore per year during the last three financial years i.e. 2021-22, 2022-23 & 2023-24. This must be the individual company turnover and not of any group of companies.	Requesting to reduce the minimum turnover from 2.5 Cr to 2 Cr per year 2021-22, 2022-23 & 2023-24.	Clause stands as per RFP.
36.	5	7	Bidder should not have conflict of interest in carrying out the Audit. i.e. The firm should not have been engaged with the Bank in	we respectfully request that this clause be reconsidered or relaxed to allow our continued participation in the current bidding process	Clause stands as per RFP.

			any form either direct or indirect assignment except concurrent audits in the past two years as on date of bid submission.		
37.	5	Part -I, Clause 3, Point 7	Bidder should not have conflict of interest in carrying out the Audit . i.e. The firm should not have been engaged with the Bank in any form either direct or indirect assignment except concurrent audits in the past two years as on date of bid submission.	We, are empanelled by UCO Bank to conduct ad-hoc information system audits upon request through standard price negotiation. As we are not fully engaged in any audits, we would like to request the Bank to confirm our eligibility as a potential bidder for this Request for Proposal (RFP).	Clause stands as per RFP.
38.	6	Point 12	Eligibility Criteria- The bidder should ensure that there are no legal proceedings / inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	The bidder should ensure that there are no legal proceedings / inquiries / investigations have been commenced / pending against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	Clause stands as per RFP.

39.	8	Part II - Scope of work	<ul style="list-style-type: none"> ▪ Data Centers at Bengaluru (Primary site for CBS and non-CBS applications) NOC, SOC at Kolkata. ▪ Disaster Recovery Sites for CBS applications and non-CBS applications at Kolkata, NDR-Bengaluru. ▪ Treasury Division, SWIFT Center at Bengaluru/Kolkata/Mumbai. ▪ Digital Banking Facilities at Bengaluru/Kolkata. ▪ Bank's CTS Centers at Delhi, Chennai & Mumbai. ▪ Bank's Contact Centers/ Call Centres at Kolkata/New Delhi/Bengaluru. ▪ Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements at Bengaluru/Mumbai/Kolkata /Chennai or any other Bank's office/ Vendors location. ▪ Other HO divisions/ Service Providers at Bengaluru / Mumbai/ Kolkata/ Chennai or any other Bank's office at 	<p>Please let us know if we will be expected to physically visit centres outside Kolkata.</p> <p>Will the bank reimburse expenses outside Kolkata?</p> <p>Are we expected to travel outside India for the audit? Please provide list of overseas locations.</p> <p>Will the bank bear the cost of overseas travel?</p>	<p>The bidders have to physically visit centres outside Kolkata (except overseas locations).</p> <p>No additional cost will be given by the Bank.</p>
-----	---	-------------------------	--	--	---

			any place, where critical application/ IT infrastructure is installed or may be installed in future. ▪ Locations of Service Providers to whom specific services are outsourced.		
40.	8	Part II - Scope of work	During the execution of Audit work, the bidder must station auditor onsite until completion of Audit work and for checking compliance without additional charges to Bank. Remote access will not be given to the vendor	Please let us know the number of auditors expected onsite.	Please refer corrigendum.
41.	8	Vendor/Third Party Audits	Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements at Bengaluru/Mumbai/Kolkata /Chennai or any other Bank's office/ Vendors location.	For third-party and vendor-hosted infrastructure, will Bank ensure all necessary access and permissions (physical and logical) for the auditor?	The bidder has to co-ordinate with the third party-vendor. Bank will only assist the bidder in getting the permission. Relevant travelling/ lodging/ boarding cost to be borne by the bidder.
42.	8	Tools for Audit	The bidder has to complete the audit onsite using proven methodologies & tools for conduct of audit. The bidder has to supply all essential tools for audit and bank will	Is there a pre-approved list of audit and security tools (for VA/PT, etc.) accepted by the Bank, or will the Bank need to approve each proposed tool individually for each assignment?	It is clarified that selected bidder need to carry their own CertIN approved list of tools for conducting Audits. Bank will cross check the same.

			only provide support for its utilization/use		
43.	8	Onsite Requirement	The bidder has to complete the audit onsite using proven methodologies & tools for conduct of audit. The bidder has to supply all essential tools for audit and bank will only provide support for its utilization/use	With remote access not allowed, how will audits for cloud-hosted/branch systems at distant locations be arranged logistically? Is any secure remote access permitted under exceptional controls?	For application hosted at Bank's premises, bidder can conduct Audit from Bank's premises. For application deployed outside the Bank's premises, the bidder has to visit the cloud service premises physically for audit.
44.	09	Broad Areas of Audit, (I.Regular IS Audits)Point# 03	Application audit shall be conducted for all applications within the bank.	(i) Are we expected to review third-party developed applications, or only in-house? (ii) Is there a direction for black-box, gray-box, or white-box approaches for application audits? (iii) For applications under review, are there any integrations with third-party APIs, payment gateways, or microservices that also need to be tested as part of the audit?	i) Both In-House and Outsourced applications. ii) The bidder may use any approach of Black-box or gray-box for application audit. iii) Yes
45.	09	Broad Areas of Audit, (I.Regular IS Audits)Point# 05	Network design of critical network architecture and infrastructure performance controls shall be reviewed.	For network architecture reviews, will we receive design documents and firewall configs, or is it a live discovery task?	The network architecture diagram as well as firewall configuration doc. Will be showcased to the selected bidder during the course of audit
46.	9	Source Code Audit Scope	Source Code Audit	Will the Bank provide comprehensive source code and supporting documentation for all in-scope applications? What is the average size (lines/modules) of such applications?	The details will be shared with selected bidders.

47.	9	7.	Source Code Audit or Secure Code Review, as applicable, of inhouse-developed packages or outsourced applications.	We request UCO Bank to clarify the approx. lines of code and the method of access to be provided to bidder for the Source Code Review.	The details will be shared with selected bidders.
48.	9	7.	Source Code Audit or Secure Code Review, as applicable, of inhouse-developed packages or outsourced applications.	We request UCO Bank to provide details on the technology stack (eg. Java, .NET, SAP, Python) used in in-house and outsourced applications for source code review.	The details will be shared with selected bidders.
49.	9	Scope of Work	SOURCE CODE AUDIT/REVIEW - Source Code Audit or Secure Code Review, as applicable, of inhouse-developed packages or outsourced applications.	Could you please share how many applications are in scope for Source Code Review (SCR), and whether they are in-house or third-party developed?	Please refer page 27 of ATC document for further details.
50.	9	Scope of Work	SOURCE CODE AUDIT/REVIEW - Source Code Audit or Secure Code Review, as applicable, of inhouse-developed packages or outsourced applications.	If the Bank already has licensed source code review tools, can those be used by the auditor?	No, bidder has to use CertIN approved/ CertIN listed tools for audit. Also, the tool must be approved by the Bank.
51.	9	Scope of Work	SOURCE CODE AUDIT/REVIEW - Source Code Audit or Secure Code Review, as applicable, of inhouse-developed packages or outsourced applications.	Will the SCR need to be carried out entirely onsite, or would the Bank allow secure remote access under monitored conditions?	NO remote access will be allowed. Bidder will have to carry out SCR entirely onsite (i.e. bank Premises)

52.	9	1	Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.	The frequency of assessment which is mentioned is for the complete list of asset or entire asset is to be divided on quarterly basis for an year?	It is clarified that audit of all the assets deployed at DC, Cloud and DR is to be completed in each audit cycle.
53.	9	I. 1	Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.	We request UCO Bank to clarify whether remediation audit or revalidation is within the scope and how many rounds of such audits are expected	Atleast one cycle of retesting and verification audit is to be completed after every mitigation.
54.	9	I. 1	Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System	We request UCO Bank to clarify whether the list of 1200-1500 devices for Vulnerability Assessment (VA) will remain constant throughout the engagement period or we can do it in a phased manner as per the defined frequency.	Please refer point 4 at page 28 of ATC. No, it cannot be completed in phased manner.

			(IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.		
55.	9	I. 1	Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.	We request UCO Bank to confirm whether secure VPN or VDI access will be provided for remote audit activities for Assessments?	NO remote access will be provided to the bidder.
56.	9	I. 1	Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.	We request UCO Bank to specify whether we need to perform credential based scanning (including OS, databases, network devices, etc.)	YES
57.	10	Cloud	SECURITY AUDIT OF CLOUD SERVICES	Are any hybrid cloud workloads (public/private) in scope? If yes, what kind of security posture assessments are expected?	As of now, there is no hybrid cloud workloads.

					The bidder has to carry out security posture assessment based on standard cloud security controls logical as well as physical.
58.	10	Broad Areas of Audit, (I.Regular IS Audits)Point# 17	AUDIT OF STORAGE OF PAYMENT SYSTEM DATA - Bank shall conduct audit to ensure that the entire data relating to payment systems operated by them are stored in a system only in India.	For cloud assets, are there cross-region deployments, and how will we verify geographic data residency for payment system data?	Auditor has to audit the bank's payment system as per RBI's guideline related to data localization of payment system.
59.	10	Scope of Work	SECURE CONFIGURATION REVIEW/AUDIT	What is the expected frequency of activities like VAPT and configuration audits? Are these one-time or recurring engagements?	Please refer page 38 clause "Frequency of Audits"
60.	10	Scope of Work	SECURE CONFIGURATION REVIEW/AUDIT	Will all audit activities VAPT, Source Code Review, and Configuration Review to be carried out at a single location or multiple Bank offices?	VAPT & Configuration audits at single location whereas for source code audit may have to visit multiple locations.
61.	11	International Branches	27. Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong 28. MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore	For MAS (Singapore) and C-RAF (Hong Kong) Cyber Audit, is local, onsite presence expected, or is remote review permissible? Will the Bank assist with any cross-border compliance/coordination?	Audit has to be conducted from INDIA only, the Bank will provide necessary support.

62.	11	3rd Party/Cloud Limitation	SECURITY AUDIT OF CLOUD SERVICES	If a cloud/third-party denies access due to their internal policies, how will this be managed and will the auditor be indemnified for any missed controls due to such restrictions?	Bank will provide necessary support for conducting security audit of cloud services.
63.	12	Reporting	Reports	Apart from technical findings, do you also require summarized executive dashboards or board-level risk briefs?	Yes
64.	12	Scope of Work	Reports	Are there any applications identified as high risk by the Bank that need more detailed or prioritized audits?	Bank has list of application on criticality basis.
65.	12	Reporting	Reports	Does the Bank follow a specific format for audit reports and risk ratings, or can we use our own standard format?	No, Bank has no fixed format, but the bidder has to submit report as per latest CertIN guideline/ format.
66.	12	Report Formats	Reports	Is there a mandated format/template for all VA/PT, application, and process audit reports?	No, Bank has no fixed format, but the bidder has to submit report as per latest CertIN guideline/ format.
67.	12	31.	Security cum functional audit of new applications	We request UCO Bank to clarify the estimate of applications per year for Security cum Functional Audit.	Approximately 100 applications per year
68.	12	Reports	The various audit reports/ templates should be got integrated with the Bank's ITGRC Application.	Kindly specify the frequency of updating the audit reports in the banks ITGRC. Kindly provide details of the ITGRC application. Is the bidder expected to procure and deploy the tool.	The bidder has to provide audit reports & compliance reports on completion for uploading to ITGRC portal. Bank uses Archer application for the same.
69.	13	MIS Reporting Integration	MIS	Are there technical/API requirements for integrating auditor reports/tools with Bank's ITGRC system?	Bank prefers to automate ITGRC system with the help of API.
70.	13	Reports ,	The various audit reports/ templates should be got	(i) Will the Bank provide access to its ITGRC application for report uploading and integration?	i) Yes

			integrated with the Bank's ITGRC Application.	(ii) What level of integration is expected with the ITGRC – manual upload, API-based, or templated format?	Currently it supports manual uploads, however Bank prefers automate/ API based upload
71.	13	GRC Tools	Report	Will we need to integrate our findings with your existing GRC or ticketing systems, or will standalone reports be enough?	Currently it supports manual uploads, however Bank prefers automate/ API based upload
72.	12	Auditor Training Delivery	Training	For bi-annual training, is there a Bank preference for onsite, virtual, or hybrid delivery? Are regional offices included? Will Bank organize participant & trainer logistics?	Please refer clause "Training" at page 12 of ATC
73.	12	Training	Training	How many people are expected to be trained, and what is the expected frequency, once a year or more often?	Please refer clause "Training" at page 12 of ATC
74.	12	Training Effectiveness	Training	Will the training audit also involve measuring the effectiveness of past sessions and looking at employee feedback?	No
75.	12	31.	Training is to be given to internal IS Audit team on uses of Tools used for Audit purpose, understanding scripts to be run on server, conducting VAPT, preparation of the Reports based on the identified vulnerabilities (i.e. identifying Risk Impact and Recommendation to mitigate the identified risks).	We request UCO Bank to clarify the periodicity and intended audience for the in-scope trainings.	Please refer clause "Training" at page 12 of ATC

76.	13	MIS	Successful bidders will use some tools preferably Web Based (cost if any, should be included in audit fee) , which shall be capable of providing audit report, and which should support dashboard format (Major gaps with subsequent details through links). It should be capable of presenting reports sorted on following major domains and presentable in pie chart/ graphs/excel sheet. Bank will have the right to use that tool.	We would request that the Bank clarify whether they are exclusively seeking a web-based tool, or if alternative solutions, such as Power BI, would be acceptable for presenting a comprehensive summary of vulnerabilities and their associated risks.	Clause stands as per RFP
77.	13	MIS	Successful bidders will use some tools preferably Web Based (cost if any, should be included in audit fee), which shall be capable of providing audit report, and which should support dashboard format (Major gaps with subsequent details through links). It should be capable of presenting reports sorted on following major domains and presentable in pie chart/ graphs/excel sheet. Bank will	Will the tool be deployed at the banks premises. Will the tools license belong to the bank or the bidder? Are only Vulnerability Assessment reports to be uploaded or also GRC related observations to be uploaded in the tool.	<p>CertIN approved/listed tool should be deployed at Bank's premises.</p> <p>License of tool will belong to the bidder and Bank reserves the right to use the same during the contract period without any extra expenditure.</p>

			have the right to use that tool.		
78.	14	2.1.1	Process Audit shall cover but not limited to the following units- Point No. I to xxxix	a) Please share the approx. number and types of applications to be covered under process audit. b) Some of the areas in process audit are overlapping with the scope in other areas, E.g. SDLC and Change Management, Vendor & SLA management, IT outsourcing related controls, VAPT of OS, Database and Network devices. Given the fact that there could be two service providers performing the task, how bank will ensure that there are no scope and commercial overlaps?	A) Will be shared with selected Bidder B) Will be shared with selected Bidder
79.	15	Mobile Audit	Mobile Banking /UCO mBanking plus/Corporate mBanking Audit	How many mobile apps are included in scope, and are both iOS and Android platforms involved? Is code review part of this too?	Please refer clause 9 at page 9 of ATC. Both for android & IOS.
80.	15	Branch Audit	Mobile Banking /UCO mBanking plus/Corporate mBanking Audit	How many Bank branches are in scope for audit? Will it be full coverage or based on representative sampling?	Approximately 10 Branches of the Bank are in scope of audit. Other relevant details will be shared with the selected bidder
81.	16	Sampling	Automated Teller Machine (ATM)/Cash Recycler & Digital Banking Unit:	For devices like endpoints or ATMs where there are large numbers, will sampling be allowed for VAPT or config checks?	Yes, sampling will be allowed for VAPT or config checks.

82.	16	Scope of Work	Automated Teller Machine (ATM)/Cash Recycler & Digital Banking Unit:	Will the audit cover key digital banking platforms like Internet Banking, Mobile Banking, and UPI services?	Yes, details is already mentioned in ATC.
83.	16	Sampling	Automated Teller Machine (ATM)/Cash Recycler & Digital Banking Unit:	What is the minimum sampling size that would be acceptable for endpoint/ATM configuration checks?	Minimum 5 samples in different geographical regions is to considered for audit.
84.	19	Asset Mgmt	Asset Management	Will an updated asset inventory be provided for us to plan the scope of VAPT and configuration audit activities effectively?	Details will be shared with the selected bidder.
85.	20	Awareness	IT Operations Audit	Are we expected to include simulated phishing campaigns or social engineering drills as part of the awareness program audit?	No
86.	24	SOC Review	Security Operating Centre (SOC)	Will the audit include access to the SOC setup, tools, incident logs, and evaluation of alert monitoring practices?	Yes
87.	24	Tool Integration	Security Operating Centre	Will the auditor need to integrate with any existing SIEM, SOAR, or ticketing platform like Splunk or ServiceNow?	Yes
88.	24	SOC Review	Security Operating Centre	Does the SOC audit also include assessment of log retention policy, alert thresholds, and response SLAs?	Yes
89.	27	Source Code Audit	The in-house developed Applications/ Outsourced application approx. 250(+/- 20%) application/API /	Can the Bank share a detailed inventory: application technology stack, system criticality, device types (OS, DB, appliances) for the stated	Details will be shared with the selected bidder.

			Customization and any outsourced applications if required.	"250(+/-20%)" applications and "1200-1500" devices?	
90.	28	17	AUDIT OF STORAGE OF PAYMENT SYSTEM DATA	Total Number of Applications to be covered in this scope.	Details will be shared with the selected bidder.
91.	28	VAPT Scope	Penetration Testing	For network and infrastructure VAPT, can the audit be conducted using a Grey Box method with shared credentials, or is it strictly Black Box?	For network and infrastructure VAPT, audit can be conducted using a Grey Box method or Black box method
92.	28	VAPT Scope	Penetration Testing	Will the Bank require Black Box testing for applications, or will a Grey Box approach.	Bank requires Black box testing for Applications.
93.	28	5	Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.) throughout their lifecycle (pre-implementation, post-implementation and/or after major changes). Penetration Testing (External) shall be conducted mandatorily on all public facing applications/URLs/Website/APIs/Cloud Applications exposed to the internet.	Kindly clarify whether external PT will be carried out from the Bank premises or over a secure ISP channel? Please share the expected number of internal IP in the scope of testing.	External PT should be carried out from outside the Bank's premises.
94.	28	5	Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.)	We request UCO Bank to confirm the timeline and periodicity for public facing applications/API assessment.	Public facing applications will be part of VAPT and is to be audited on half yearly basis.

			throughout their lifecycle (pre-implementation, post-implementation and/or after major changes). Penetration Testing (External) shall be conducted mandatorily on all public facing applications/URLs/Website/APIs/Cloud Applications exposed to the internet.		
95.	28	16	SECURE CONFIGURATION REVIEW/AUDIT	Total number of Secure configuration documents to refer for this scope. Total Number of Servers, Network Devices and Security Devices to be covered in this scope.	Details will be shared with the selected bidder.
96.	28	15	SECURITY AUDIT OF CLOUD SERVICES	Details of Cloud Services to covered in this scope.	Details will be shared with the selected bidder.
97.	28	18	SYSTEM AUDIT REPORT (SAR) NSDL	Total Number of controls in the checklist provided by NSDL.	Details will be shared with the selected bidder. Auditor is also to be guided by the CSCRf guideline by NSDL.
98.	28	4	The Vulnerability Assessment (VA): VA of IT assets (applications, systems and infrastructure) deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers,	We request UCO Bank to provide an approximate number of devices or applications that fall under PCI DSS compliance scope and require quarterly VA and Grey/White Box PT.	Approximately 32 applications and 150 servers falls under PCI DSS compliance scope.

			Operating Systems, Data Base Systems, IOSs, Clouds, etc. through their life cycle (pre-implementation, post implementation, major changes etc.) shall cover a minimum of 1200-1500 (+/- 10%) devices on half-yearly basis and VA of IT infrastructure related to PCI DSS compliance will be done on Quarterly basis. A list of Servers/devices in different locations will be given to the selected vendor.		
99.	28	4.	The Vulnerability Assessment (VA): VA of IT assets (applications, systems and infrastructure) deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc. through their life cycle (pre-implementation, post implementation, major	We request UCO Bank to provide the locations (city-wise) of all Data Centers, Disaster Recovery Centers, and offices where audit activities such as forensic investigations, secure configuration review, or physical access may be required.	Please refer to page no. 29-30, clause no. 6.1.2 of RFP.

			changes etc.) shall cover a minimum of 1200-1500 (+/- 10%) devices on half-yearly basis and VA of IT infrastructure related to PCI DSS compliance will be done on Quarterly basis. A list of Servers/devices in different locations will be given to the selected vendor.		
100.	28	VAPT Scope	Vulnerability Assessment	Is application VAPT expected to be conducted on both authenticated (logged-in user) and unauthenticated views?	Yes, on case to case basis.
101.	28	VAPT Scope	Vulnerability Assessment	Will the Bank provide test credentials or dummy user accounts for conducting authenticated application testing?	Yes
102.	29	6. Vendor & Site Audit: 6.1.2 Site Audit for Various IT Infrastructure/Facilities like Data Centre, Treasury, CTS Centers, ATM vendor site etc	<ul style="list-style-type: none"> • POS Infrastructure Facility • SMS system, • SWIFT centers • Vendor's Sites wherever applicable 	Please provide list of all the sites. Please mention the complete list of vendor sites.	Details will be shared with the selected bidder.
103.	29	DR Site	Site Audit for Various IT Infrastructure/Facilities like Data Centre, Treasury, CTS Centers, ATM vendor site etc	Will we have access to both the primary DC and DR site to verify controls, including BCP/DR drills?	Yes

104.	29	Clause 6	Vendor & Site audit- Pls provide site locations for following: 1 POS Infrastructure facility 2 SMS system 3 SWIFT centers Vendor's sites wherever applicable	Please provide location details for the mentioned site audits. Also, we understand sample based vendor sites shall be audited. Please provide list of such sites.	Details will be shared with the selected bidder.
105.	29	Vendor Risk	Vendor Audit	Will third-party audits include checking SLAs, cloud vendor risk posture, and contract-level security clauses?	Yes
106.	30	Existing Environment	Environment Control	Could you provide a list of the cybersecurity tools currently deployed across your infrastructure like SIEM, DLP, WAF, etc.?	Details will be shared with the selected bidder.
107.	30	Clause 7	Application Audit- CBS (Domestic & Overseas), Internet Banking (Domestic & Overseas), ADC channels, GBM, LAPS, MMS, NEFT, RTGS, SWIFT, UPI, BBPS, IMPS, DMS, Mobile Banking, CTS, Biometric Authentication System (BAS), AEPS etc.	Request you to confirm on the in-scope application as the current listing is open ended.	An indicate list is already given in RFP. Exact Details will be shared with the selected bidder.
108.	30	25	Audit/Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)	Please confirm do we need to refer and validate SBOM and CBOM reports generated from SBOM and CBOM tool.	Yes, bidder need to refer and validate SBOM and CBOM reports generated both manually and from SBOM and CBOM tool.
109.	31	29	VA/PT OF INTERNET CONNECTED PCs	Total Number of Internet connected Desktops/ PCs Corporate Departments Wise.	Details will be shared with the selected bidder.

110.	32	9	Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications	We request UCO bank to clarify if the open source tool required to do the performance testing will be allowed in the environment?	Industry standard tool should be used with prior approval of Bank.
111.	32	9.	Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications:	We request UCO Bank to confirm whether dedicated staging environment will be provided for load/stress/spike/capacity testing of applications.	Yes
112.	32	9	Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications	We request UCO bank to kindly confirm if NOC report for Performance and availability of network devices will be provided for review?	Yes
113.	32	9.	<p>The Network audit shall cover but not limited to the following aspects:--</p> <ul style="list-style-type: none"> ➤ Overall Network architecture ➤ Overall Network management ➤ Review of detailed Network architecture ➤ Network traffic analysis and base lining ➤ Virtual LANS (VLANs) & Routing. ➤ Evaluate procedures adopted for: <ul style="list-style-type: none"> i. Secured transmission of data through leased line/VPN/VSATs/ MPLS, Wireless etc. 	We request UCO Bank to clarify the periodicity of network devices audits and if it involves all the devices or a certain percentage.	Yearly

			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.		
114.	32	9.	The Network audit shall cover but not limited to the following aspects:-- ➤ Overall Network architecture ➤ 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/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.	We request UCO Bank to confirm if the bidder will be granted access to perform live database queries and configurations reviews using their own tools, or if the Bank has specific tooling or protocols to be followed.	Auditor will not be granted access to live queries. Auditor has to use his own tool for audit.

115.	33	KPIs/KRIs Documentation	Assessment of KPI & KRI	Will Bank supply historical documentation, measurement basis, and access to systems required for KRI/KPI validation, as per RBI mandates?	Yes
116.	33	ISO 27001	Audit for Sustenance of ISO-27001 Certification for DC-DR Operations	Are we expected to assess the Bank's control implementation maturity aligned with ISO 27001:2022?	Yes
117.	33	13	Auditor for Internal Audit shall provide onsite handholding support to Bank prior to the Surveillance Audit(s) and liaise with the External Auditor, each year, for sustenance of ISO-27001 Certification. During the course of Certification, broadly following documents have been provided / created and shall be made available for the on boarded Auditor:	As an empanelled Internal Auditor, our role is to conduct independent assessments in line with ISO 27001 requirements. However, the above scope also includes handholding and liaising with the certification auditor, which could lead to a conflict of interest, as the same auditor cannot both guide implementation and independently assess compliance. we respectfully request clarification or re-alignment of responsibilities so that internal audit and certification support roles are segregated.	Bidder can be guided by "conflict of interest" clause of the RFP.
118.	34	Cloud Infra	SECURITY AUDIT OF CLOUD SERVICES	Can you share details of the cloud services in use (IaaS, PaaS, SaaS), and how many cloud-hosted assets are in scope for the audit?	Details will be shared with the selected bidder.
119.	34	16	SECURE CONFIGURATION REVIEW/AUDIT	Please specify the number and types of devices to be covered.	Details will be shared with the selected bidder.
120.	34	Cloud Audit Access	SECURITY AUDIT OF CLOUD SERVICES	For cloud-hosted assets, will direct console access and necessary credentials be provided, or will audits	Both, case to case basis.

			IS Audit of Cloud Services shall be conducted for assurance on deployment of cloud security on systems hosted in clouds. It shall also be conducted as and when any new IT Infrastructure or application is introduced or migrated to cloud.	rely on screenshots/data supplied by Bank staff?	
121.	34	15	SECURITY AUDIT OF CLOUD SERVICES	We request UCO Bank to clarify the type and approx. count of cloud environments and assets required to be tested.	Details will be shared with the selected bidder.
122.	34	Audit Units/Areas:	SECURITY AUDIT OF CLOUD SERVICES	We would request the Bank to confirm the name of the cloud service provider (CSP) such as GCP, AWS, Azure, any other private along with number of subscription or user license.	Details will be shared with the selected bidder.
123.	36	Cloud API	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Are APIs hosted on cloud platforms included in the scope of external VAPT?	No
124.	36	Cloud Infra	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Will the Bank allow external-facing VAPT to be performed remotely from the auditor's secure environment, with appropriate IP whitelisting?	Yes

125.	36	Audit Timing	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Will the Bank define specific maintenance windows or downtimes during which we can schedule audits?	Yes
126.	36	Clause 24	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Most of the SoW is covered in other scope areas and appears to be repeat scope. Please clarify the expectation. Also, as two service providers shall be involved, how bank expect service provide to have unique delivery and commercial to each bidder.	RFP clause is self-explanatory.
127.	36	24	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	should we conduct PT of application or we conduct review only	RFP clause is self-explanatory.
128.	36	27	MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore	Need more understanding of this point	Cyber security /risk assessment/audit to be carried out based on Technology Risk Management (TRM) guidelines of Monetary Authority of Singapore (MAS).
129.	37	Environment	MIGRATION AUDIT	Are legacy systems included in scope, and if yes, are there specific limitations or integration risks we should be aware of?	Yes
130.	37	30	IS Audits i.e. Vulnerability Assessment, Penetration Testing, External Assessment, Configuration Audit, Data Migration Audit, Application security Audit etc.	We request UCO Bank to clarify whether Black Box Testing is to be performed on all external-facing infrastructure and whether internal application will also require Black Box or Grey Box testing?	Yes

131.	37	30	SECURITY CUM FUNCTIONAL AUDIT OF NEW APPLICATIONS	1).How frequently are new applications expected to go-live during the contract? 2).Will these applications be custom-developed or off-the-shelf? Is test/staging access available?	1). 15 days 2). Yes
132.	37	29	VA/PT (Vulnerability Assessment and Penetration Testing) of Internet connected Desktops/ PCs of Corporate Departments shall be done.	Kindly clarify the total number of PCs to be tested. Will testing be conducted on-site or will test agents be allowed under bank supervision?	10-15 PCs Approximately VA is Onsite PT is external.
133.	38	31	Forensic Audit/ Forensic Analysis/Investigations	Kindly confirm if this scope is on-demand and whether it will be incident-triggered during contract tenure. Should pricing be included in commercials, or will this be handled on a case-by-case basis? Also can we provide our commercial for this scope on man hour basis?	The scope is "On demand". Prices are to be included in Commercial in Table C.
134.	38	Forensics	Forensic Audit/ Forensic Analysis/Investigations:	In case of a live cyber incident, how quickly is the audit team expected to respond onsite or remotely?	Within 1 hour
135.	38	Forensics	Forensic Audit/ Forensic Analysis/Investigations:	Is there any tool preference or forensic methodology the Bank would want the auditor to follow?	No. Industry standard tool/methodology should be used.
136.	38	Forensic Audit	Forensic Audit/ Forensic Analysis/Investigations:	What is the estimated minimum number of man-days expected for forensic audit/investigation?	Will be mutually decided. Varies from incident to incident depending upon the severity.
137.	38	Network Infra	NETWORK ARCHITECTURE REVIEW	Will the Bank share high-level network architecture diagrams to support	High level network diagram will be showcased during Audit.

				planning and execution of the infra audit?	
138.	38	"As & When" Audits	TYPES OF AUDIT & FREQUENCY OF AUDIT	For new deployments/infrastructure, what minimum advance notice will be given to schedule "as & when required" audits?	15 days
139.	38	Audit Frequencies	TYPES OF AUDIT & FREQUENCY OF AUDIT	Please clarify the frequency of "one-time yearly" CBS audits vs. "as & when" limited audits. What is the expected number of both types in a year?	Annual basis Audit to be completed for all applications. Further, audit should be also conducted as and when any major change happens to Application.
140.	38	VA/PT of Endpoints	TYPES OF AUDIT & FREQUENCY OF AUDIT	VA/PT for Internet-connected PCs is specified as "half yearly." How many endpoints per round are expected, and how is this distributed geographically or by department?	Details will be shared with the selected bidder.
141.	39	Forensic Response	TYPES OF AUDIT & FREQUENCY OF AUDIT	Is the "1 hour" deployment TAT for forensic incidents applicable pan-India or only at Kolkata/Bengaluru?	PAN India
142.	40	EMD	Earnest Money Deposit	We wish to highlight that we have annual turnover of more than ₹ 500 Crore, in all of the past three completed. financial years. We are exempt from submitting the bid security as per the General Terms & Condition on GeM 4.0 (Version 1.23) dated 5th March 2025 (Clause 4.xiii.(m).v).shows we are exempt from submitting the EMD for this RFP. Request you to please confirm the same that we can submit our bid without submitting the EMD	Yes, bidder can submit bid without EMD in such case.

143.	40	PART-III 1. Earnest Money Deposit	Following categories of Bidder(s) however, be exempted from furnishing bid security: ➤ Micro and Small Enterprises (MSEs) who are holding valid Udyam Registration and are manufacturer of the offered Product or Service (Primary Product / Service - in case of bunch bid with total value wise evaluation) and give specific confirmation to this effect at the time of bid submission and claim EMD exemption.	We are registered as Medium entity under Udyam. Request you to exempt us from providing the EMD	Clause stands as per RFP.
144.	40	PART-III Earnest Money Deposit	Rs. 10,00,000/-	As per MSME clause, an organisation (comes under MSME) is exempted from paying EMD cost. Our Company comes under MSME Medium enterprises category Hence; we request you to exempt us from paying EMD cost.	Clause stands as per RFP. Exemption is allowed to MSE organizations. Please refer clause 1 at page 40 of ATC for further clarification.
145.	41	Audit Calendar/Scheduling	The proposed audit should be started within 15 days of receiving the purchase order and to be completed as per IS Audit plan and calendar which is mutually agreed between Bank and Vendor. After receiving initial reports, Bank will complete	Will the Bank provide a master calendar with expected concurrency (parallel audits)? What are dependencies on business schedules or application turnovers?	Bank will share the Master calendar along with concurrency with the selected bidders.

			the compliance. Post compliance auditor will review the compliance and submit a compliance certificate to the Bank within one month		
146.	43	Penalty, i) Penalty for not initiation of project on time:	Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value, as penalty, a sum equivalent to 0.5% of the services for each week or part thereof of delay in starting of actual audit works as specified in the agreement up to 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.	<p>We would request to amend the clause as follows allowing the mutual termination:</p> <p>Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value, as penalty, a sum equivalent to 0.5% of the services for each week or part thereof of delay in starting of actual audit works as specified in the agreement up to a maximum deduction of 5% of the order value. Once the maximum is reached Bank may consider cancellation of the order and the Performance Security submitted may be invoked.</p>	Clause stands as per RFP.
147.	44	SWIFT Payments &	Paying Authority	Are systems like SWIFT, RTGS, and NEFT in scope? If yes, should the review align with RBI and SWIFT CSP guidelines?	Yes.
148.	77	Clause - 62		<p>Request to add below clause:</p> <p><i>"Any audit shall be subject to the following: (i) the audit shall be restricted to the engagement and shall be conducted with prior reasonable notice (ii) Bank or its authorized</i></p>	RFP clause stands

				<p><i>representatives shall execute a Non-Disclosure Agreement before such audit which shall govern the conduct of the audit and any results thereof; (iii) the auditors or the representatives of Bank for the audit shall not be the Vendor's competitors; (iv) the audit shall not be conducted more than once in a calendar year and twice in entirety; and (v) any findings during the audit, shall be shared with the Vendor and be discussed and agreed mutually between Bank and the Vendor for its closure."</i></p>	
149.	82	67. Blacklisting	<p>The Bank will have the discretion to disqualify the Bidder/Vendor and/or initiate the process for blacklisting the Bidder/Vendor and may also entail forfeiture of performance security furnished by the Bidder/Vendor.</p>	<p>We would request to amend the clause as follows allowing the mutual termination:</p> <p>The Bank will have the discretion to disqualify the Bidder/Vendor and/or initiate the process for blacklisting the Bidder/Vendor with proper justification and may also entail forfeiture of performance security furnished by the Bidder/Vendor.</p>	Clause stands as per RFP.
150.	85	<p>Clause 70 (b) (Page 85) & Point 4 (Return of Confidential Information) (Page 106)</p>	<p>The parties shall return confidential information and will sign off and acknowledge the return of such confidential information.</p>	<p>Request to add below clause: <i>"Notwithstanding anything to the contrary, we shall be allowed to retain sufficient documentation as part of our professional records to support and evidence the work performed by us. Such retention shall be subject to obligations of confidentiality".</i></p>	Clause stands as per RFP.

151.	88	Annexure-I Eligibility Criteria Compliance, point no 3	Bidder should have maintained a Positive Net-Worth during the last three financial years i.e. 2021-22, 2022-23 & 2023-24	We suggest Bank to change the Current clause as- Proposed clause The bidder should have positive net profit in the last three financial years i.e., 2021-22, 2022-23 and 2023-24.	Clause stands as per RFP.
152.	90	8	Bidder should have proven methodologies & tools for conduct of audit. Tools should be as Industry Standard and free from bugs and vulnerabilities.	We request the UCO Bank to clarify whether the bidder is required to provide licenses for all security audits or if the Bank already have tools in place that can be utilized.	No, Bidder has to provide all tools with licenses.
153.	90	8	Bidder should have proven methodologies & tools for conduct of audit. Tools should be as Industry Standard and free from bugs and vulnerabilities.	We request UCO Bank to confirm whether any specific VA/PT tools are mandated or if the bidder is free to use industry standard licensed tools of their choices, subject to Bank approval.	The bidder is free to use industry standard licensed tools declared listed on CertIN site, subject to Bank approval.
154.	118	ANNEXURE – XII Point 30	Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong	We would request the Bank to confirm if physical visit is needed for Hongkong branch audit.	No
155.	118	ANNEXURE-XVII	Local Content is equal to or more than 50% and come under “Class-I Local Supplier” category.	If physical visit is required for both Hongkong and Singapore, we would request the Bank to confirm if same can be performed with Indian professionals or local professionals to be engaged to adhere the Annexure XVII.	No physical visit required.

156.	118	ANNEXURE – XII Point 30	MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore	We would request the Bank to confirm if physical visit is needed for Singapore branch audit.	No physical visit required.
157.	119	15	Fees for VENDOR AUDIT & SITE AUDIT	Details of vendor location and number of vendor to be audited	Details will be shared with selected bidder.



UCO BANK

Department of Information Technology
Selection of IS Audit Firms/Organizations for Information Systems Audit

GeM Bid No: GEM/2025/B/6476847 dated 21.07.2025

Corrigendum

Sl.	Existing Clause	Modified Clause
1	Last date of Bid Submission: 12.08.2025, 4:00 PM Bid opening Date and Time: 12.08.2025, 4:30 PM	Last date of Bid Submission: 22.08.2025, 4:00 PM Bid opening Date and Time: 22.08.2025, 4:30 PM

Addendum

Sl.	Existing Clause	New Added Clause
1.	Scope of work	As and when required, at least 2 number of auditors, one having knowledge for VAPT is to be stationed physically at audit site/Bank's site.



UCO BANK

Department of Information Technology
Selection of IS Audit Firms/Organizations for Information Systems Audit

GeM Bid No: GEM/2025/B/6476847 dated 21.07.2025

Clarifications to Queries raised by the Bidder(s) Published on 21-08-2025

Sl. No	Bid Page No.	Bid Clause No.	Original Clause	Query sought/ Suggestions of the Bidder	Banks Response
1.	9	I. 1	Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.	We request UCO Bank to specify whether we need to perform credential based scanning (including OS, databases, network devices, etc.)	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 56)
2.	28	5	Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.) throughout their lifecycle (pre-implementation, post-implementation and/or after major changes). Penetration	We request UCO Bank to confirm the timeline and periodicity for public facing applications/API assessment.	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 94) It is also clarified that periodicity for public facing applications/API assessment will be Half-Yearly (except PCI DSS related assets for which periodicity is quarterly)

			Testing (External) shall be conducted mandatorily on all public facing applications/URLs/Website/APIs/Cloud Applications exposed to the internet.		
3.	37	30	IS Audits i.e. Vulnerability Assessment, Penetration Testing, External Assessment, Configuration Audit, Data Migration Audit, Application security Audit etc.	We request UCO Bank to clarify whether Black Box Testing is to be performed on all external-facing infrastructure and same to be confirmed for internal facing application and infrastructure.	It is clarified that Black Box testing is to be performed for External facing infrastructure. Whereas Grey Box testing is to be performed for Internal facing infrastructure.
4.	28	4	The Vulnerability Assessment (VA): VA of IT assets (applications, systems and infrastructure) deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc. through their life cycle (pre-implementation, post implementation, major changes etc.) shall cover a minimum of 1200-1500 (+/-10%) devices on half-yearly basis and VA of IT infrastructure related to PCI DSS compliance	We request UCO Bank to provide an approximate number of devices or applications that fall under PCI DSS compliance scope and require quarterly VA and PT.	Approximately 400

			will be done on Quarterly basis. A list of Servers/devices in different locations will be given to the selected vendor.		
5.	34	15	SECURITY AUDIT OF CLOUD SERVICES	We request UCO Bank to clarify the type and approx. count of cloud environments and assets required to be tested.	Type of cloud - Public and Private cloud. Count of cloud environments – Approximately 10
6.	32	9.	Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications:	We request UCO Bank to confirm whether dedicated staging environment will be provided for load/stress/spike/capacity testing of applications.	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 111)
7.	28	4.	The Vulnerability Assessment (VA): VA of IT assets (applications, systems and infrastructure) deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc. through their life cycle (pre-implementation, post implementation, major changes etc.) shall cover a minimum of 1200-1500 (+/-10%)	We request UCO Bank to provide the locations (city-wise) of all Data Centers, Disaster Recovery Centers, and offices where audit activities such as forensic investigations, secure configuration review, or physical access may be required.	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 99)

			devices on half-yearly basis and VA of IT infrastructure related to PCI DSS compliance will be done on Quarterly basis. A list of Servers/devices in different locations will be given to the selected vendor.		
8.	32	9	Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications	We request UCO bank to clarify if the open source tool required to do the performance testing will be allowed in the environment?	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 110)
9.	34	16	SECURE CONFIGURATION REVIEW/AUDIT	Please specify the number and types of devices to be covered.	Please refer response to sl. No-19 below.
10.	37	29	VA/PT (Vulnerability Assessment and Penetration Testing) of Internet connected Desktops/ PCs of Corporate Departments shall be done.	Kindly clarify the total number of PCs to be tested. Will testing be conducted on-site or will test agents be allowed under bank supervision?	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 132) It is also clarified that testing is to be conducted on-site physically and no-test agents will be allowed.
11.	6	Point 12	Eligibility Criteria- The bidder should ensure that there are no legal proceedings / inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the	The bidder should ensure that there are no legal proceedings / inquiries / investigations have been commenced / pending against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 38)

			contract will get adversely affected / may get affected.		
12.	36	Clause 24	Comprehensive Cyber Security Audit- Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Most of the SoW is covered in other scope areas and appears to be repeat scope. Please clarify the expectation. Also, as two service providers shall be involved, how bank expect service provide to have unique delivery and commercial to each bidder.	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 126)
13.	38	31	Forensic Audit/ Forensic Analysis/Investigations	Kindly confirm if the commercial shared for Forensic Audit will also be considered during L1 Bidder identification?	Yes
14.			General Query	Kindly confirm whether the VAPT for the infrastructure should be credential-based or non-credential-based?	Credential Based
15.			General Query	Kindly confirm whether the application security assessment needs to be credential based or non-credential based?	Credential based testing.
16.			General Query	Please confirm the number of network architecture which needs to be reviewed?	It is to clarify that Bank has only one network architecture which is further sub divided into 9 parts (including DC and DR) Further, details will be shared with selected bidder.
17.			General Query	Please confirm what is the count of Internet connected PC for which VAPT needs to be performed? Also, confirm whether credential or non-	Please be guided by Pre-Bid responses published on 14.08.2025 (sl. No. 132)

				credential-based scan would be required.	Black Box for External Gery Box for Internal
18.			General Query	Kindly confirm the count of Asset for which Performance testing needs to be performed.	Approximately 10-13 Android & 10-13 iOS applications. Kindly refer clause 09 at page 32 of ATC/RFP for details.
19.			General Query	Kindly confirm the asset type and its count for which secure configuration review needs to be done.	Different Asset types are Server, Network Switch, Load Balancer, Storage, Router, Firewall, San Switches, Backup devices, Appliances etc. Approximate count of assets for which secure configuration review needs to be done is 1700.



UCO BANK

Department of Information Technology
Selection of IS Audit Firms/Organizations for Information Systems Audit

GeM Bid No: GEM/2025/B/6476847 dated 21.07.2025

Corrigendum

Sl.	Existing Clause	Modified Clause
1	Last date of Bid Submission: 22.08.2025, 4:00 PM Bid opening Date and Time: 22.08.2025, 4:30 PM	Last date of Bid Submission: 28.08.2025, 4:00 PM Bid opening Date and Time: 28.08.2025, 4:30 PM