ODISHA GRAMYA BANK
Information Technology Department
Head Office, Gandamunda, P.O. Khandagiri, Bhubaneswar-30

RFP Ref No. OGB/RFQ/ITD/VAPT/012/2021-22 Dated 03rd February 2022
REQUEST FOR QUOTATION (RFQ) FOR ENGAGEMENT OF CERT-IN EMPANELED AUDITOR FOR AUDIT OF INFORMATION SECURITY (IS) AND VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT) OF ODISHA GRAMYA BANK DATA CENTERS, DISASTER RECOVERY CENTERS AND WEBSITE

INTRODUCTION

Odisha Gramya Bank invites close competitive quotations/bids from all eligible bidders/ Firms/ Organizations for IS Audit at Data Centre (DC), DISASTER RECOVERY (DR) and Website.

Project specific terms & conditions and General terms & conditions and Annexures relating to this RFQ are furnished hereunder.

1. PROJECT SPECIFIC TERMS & CONDITIONS:

1.1 SCHEDULE OF BIDDING PROCESS:

S.No	Description of Information/ Requirement	Information / Requirement
1.	Tender Reference Number	OGB/RFQ/ITD/VAPT/012/2021-22
2.	Date of Issue of RFQ	03rd February 2022
3.	Bid Submission Mode.	Through manual Tendering process
4.	Last Date and Time for submission of bids along with supporting documents through the above	14th February 2022 15:00 Hrs
5.	Date, time and venue for opening bid.	14th February 2022 16:00 Hrs at the Bank's Information Technology Department, Bhubaneswar.
6.	Address for Communication / Submission of Bids	The General Manager, Information Technology Dept., Odisha Gramya Bank, Head Office, AT-Gandamunda, P.O:- Khandagiri Bhubaneswar – 751030.
7.	Contact officials for any clarification.	B. K. Patra- General Manager Telephone – 0674-2353038 S. S. Acharya - Senior Manager Telephone – 0674-2353045 A. Patra – Sr. Manager Telephone – 0674-2353025
8.	Contact e-mail ID	itd@odishabank.in

1.2 BIDDER'S QUALIFICATION CRITERIA:

The documentary evidence of the Bidder's/ Firms qualifications to perform IS Audit.

1. The bidder's Firm/Organizations is registered as a company or Proprietorship firm in India as per Companies Act, 1956/2013. The Certificate of Incorporation or Certificate of Proprietorship issued by the Registrar of Companies is to be submitted along with bid. (Documentary proof should be attached).

2. The Bidder's Firm/Organizations should have in the list of cert-in empaneled IS Auditing Organization and should have ISO certification. (Documentary proof should be attached).

3. The bidder's Firms/organization should have 10+ years' experience in Information Security Audit and should work in various banking and Financial Sector Projects.

4. The bidder's Firm/organization should provide the list of Freeware Tools and Commercial Tools to be used if any for the IS Audit.

5. The bidder's Firms/organization should submit a letter of undertaking stating to abide by all the terms and conditions stipulated by the Bank in the RFQ as per Annexure-C.

6. The bidders/Firms/organization should not have been blacklisted/ de-empaneled by Odisha Gramya Bank or in any Central Government / PSU / Banking / Insurance company in India as on date of the RFP. Bidder to submit the Self Declaration certificate as per format provided in Annexure D of the RFQ along with the technical bid.

The bidder shall furnish relevant documents / self-declaration supporting the above eligibility qualification criteria along with the bid.

1.3 SCOPE OF WORK

1. **Area of Operations:**
   1. IS and VAPT audit at DC, Chennai.
      Address:
      Odisha Gramya Bank, DC
      MSDC Coral,
      Nxtra Data Limited,
      Plot No# F8, SIPCOT IT Park , Siruseri,
      Chennai - 603103.
      Ph: 044-47492064.

   2. IS and VAPT audit at DRC, Hyderabad.
      Address:
      OGB Cage Area
      Floor- 1st
      STT GLOBAL DATA CENTERS LTD.
      MADHAPUR
      HYDERABAD TELENGANA STATE

   3. CBS Help Desk at Bhubaneswar, Odisha

Address:
IT Department,
2nd Floor,
Odisha Gramya Bank,
Head Office,
Gandamunda, Khandagiri,
Bhubaneswar - 751030

4. Data Base, Operating System, Application Audit of critical application.
5. Network Management
6. Delivery Channel Audit
7. Vulnerability / Threat Assessment of all servers, ATM Switch, network equipment, security equipment installed
8. Penetration Testing for external facing applications/servers
9. Audit of Outsourcing Arrangements (all IT related services)
10. Audit of all hardware's at DC at Chennai, DRS Hyderabad as per RFP.

2. Generally the IS Audit / Review shall take into account the following:

1. The Auditors are required to verify for compliance, status of the previous Audit Reports for which Audits were conducted
2. Auditors should follow Risk Based approach in all areas
3. To ensure that Data Integrity across various systems is maintained
4. To ensure compliance of Information Technology (IT) Act 2000, Information Technology (Amendment) Act-2008 and other Information System related guidelines.
5. To ensure compliance to all applicable guidelines issued by NABARD and applicable to Regional Rural Bank till the date of Audit.
6. Application in terms of its functionality, controls and change management systems
7. Physical Security controls and environmental controls for the relevant servers / production environment
8. Logical Security controls, User Management Process, Systems Administration, Access Control Measures
9. Operational Security Controls including troubleshooting / help desk
10. Proper People Management and controls
11. In terms of establishing proper Segregation of duties and other administrative controls
12. Vulnerability Assessment and Penetration testing.
13. Operating Systems, Database review in case of servers including patch management for OS etc.
14. Network and security review including anti-virus and VAPT
15. Review of Outsourced activities
16. Adequacy of audit trail, history of access to database, Monitoring Mechanism
17. Business Continuity preparedness / Disaster Recovery Preparedness/ Backup (for Data, Systems, Personnel etc.,)
18. Documentation, Manuals, Job Card availability.
19. The adequacy of existing Guidelines and Procedures in the relevant area
20. The adequacy and effectiveness of internal control systems
21. Audit the Services of all Service Providers to ensure they adhere to the contracted levels of services set out in the Service Level Agreement (SLA).

22. Audit the compliances by the service providers to various regulatory and statutory requirements.
23. Protection from Distributed Denial of Service attacks
24. Utilization of servers
25. Database management

3. Brief Details about Application Audit:

The Successful Bidder should conduct IS audit of all the Applications used by the Bank. Some critical applications are listed here below:

1. Core Banking Application – "FINACLE" software on Oracle 10c Database
2. Aadhaar Enabled Payment System – Switch of Atyati for Micro ATM Transactions
3. Email Solutions
4. Bank's website www.odishabank.in
5. Bank's intranet website
6. Active Directory

The audit of Applications will be with reference to

1. Auditing Application Architecture
2. Study CBS and other applications for adequacy of Input Processing and Output controls and conduct various tests to verify existence and effectiveness of controls.
3. Review / audit the presence of adequate security features in CBS application to meet the standards of confidentiality, reliability and integrity required for the application supporting business processes.
4. Logical access control, User maintenance and password policies being followed are as per Bank's IT security policy.
5. Authorization mechanism and control such as concept of maker checker, exceptions, overriding exceptions and error conditions.
6. Controls over automated processing /updation of records, review or check of critical calculations such as interest rates, levying of various charges etc., review of the functioning of automated scheduled tasks, batch processes, output reports design, reports distribution, etc.
7. Review of all controls including boundary controls, input controls, communication controls, database controls, output controls, and interfaces controls from security perspectives.
8. Review effectiveness and efficiency of the Applications. Identify ineffectiveness of the intended controls in the software and analyze the cause for its ineffectiveness. Review adequacy and completeness of controls
9. Identify gaps in the application security parameter setup in line with the Bank's security policies and leading applicable practices.
10. Auditing, both at client side and server side, including sufficiency and accuracy of event logging, SQL prompt command usage, Database level logging etc.
11. Complete Review of Application Parameterization.
12. Backup/Fallback/Restoration procedures and contingency planning.
13. Review of segregation of roles and responsibilities with respect to application software to improve internal controls.
14. Review of documentation for formal naming standards, design process for job roles, activity, groups and profiles, assignment, approval and periodic review of user profiles, assignment and use of super user access

15. Manageability with respect to ease of configuration, transaction roll backs, time taken for end of day, day begin operations and recovery procedures
16. Special remarks may also be made on following items - Hard coded user-id and password, Interfacing of software with ATM switch, EDI, Tele Banking server, Web Server and Other interfaces at Network level, Application level, Recovery and restart procedures
17. Sufficiency and coverage of UAT test cases, review of UAT defects and tracking mechanism deployed by vendor and resolution including re-testing and acceptance Review of customizations done to the software and the SDLC policy followed for such customization. Proposed change management procedure during conversion, migration of data, version control etc.
18. Review of Software benchmark results and load and stress testing of IT infrastructure performed by the Vendors
19. Adequacy of Audit trails and meaningful logs
20. Adherence to Legal and Statutory Requirements.
21. Configuration of System mail
22. Compliance of Previous IS Audit Report
23. Review of Information Systems Support & Compliance to Service Level Agreement (SLA).
24. Issues pending with the Vendor age-wise and progress there on.
25. Network Controls
26. Major events during the month
27. Backup and DRP review
28. Review of Systems Development, Acquisition and Maintenance
29. Hardware Maintenance
30. Storage and Media Controls
31. Logical Security
32. Application Level Controls
33. Review of logs
34. Adequacy of hardening of all Servers and review of application of latest patches supplied by various vendors for known vulnerabilities as published by CERT, SANS etc.

35. Application-level risks at system and data-level include, system integrity risks relating to the incomplete, inaccurate, untimely or unauthorized processing of data; system-security risks relating to unauthorized access to systems or data; data risks relating to its completeness, integrity, confidentiality and accuracy; system-availability risks relating to the lack of system operational capability; and system maintainability risks in terms of adequate change control procedures.

As part of documenting the flow of transactions, information gathered should include both computerized and manual aspects of the system. Focus should be on data input (electronic or manual), processing, storage and output which are of significance to the audit objective.

Consideration should be given to audit of application interfaces with other systems or interface of other systems with application.

4. **Functional Audit of CBS impacting Bank's revenue**
    1. Check integrity between source and GL
    2. Any new GL Code and Sub Code added with proper authentication and they are correctly tagged.

3. Changes made in the interest rates/fees and charges table and changes are in accordance with written instructions from business departments.
4. Posting of correct processing charges/interests rate in the system and posting correct amount in accounts (Sample verification of accounts)
5. Creating/modification of new products in Advances/Deposits.
6. Review exception reports for unusual transactions due to system/ close of business and action taken thereon
7. Check consistency of data when transferred from other systems or standalone systems to and from CBS
8. Review of parking accounts like Suspense, Sundry Depositors, Inter branch, Cash Management account etc
9. Checking any transactions not verified and remained in entered (un-posted) status.
10. Review control reports generated to ensure integrity of the transactions and ensure the transactions are in conformity with Bank's guidelines/system of authorizations (maker checker).
11. Carrying out Standing Instructions and vouching of Offline transactions
12. Review of controls surrounding the operational environment of the Core Banking Operations and identify any weakness therein.
13. Adequacy of the existing Policy, Procedure like Incident handling procedure, Log Monitoring, Access Control Procedure etc.,
14. Review of Access Control Mechanism.
15. Robustness of CBS Administrative practices and Help-Desk Management & Procedures.
16. Business Continuity preparedness / Disaster Recovery Preparedness / Backup (Data, Systems, Personnel etc.,)
17. Database controls – Physical Access and Protection, Integrity and Accuracy, Administration and House Keeping
18. Verification of Interfaces / Links with other systems such as ATM server, Net Banking / Mobile Banking server, RTGS/NEFT etc., and observation with regard to failure of one or more interfaces
19. Problems faced by Users and redressal mechanism for such problems
20. Management of Help Desk
21. Change Management procedures
22. Documentation relating to User requirements, specifications
23. Version Control

5. **DC and DRC Environment controls**

All servers are hosted in DC and DRC. The board cope of audit of DC and DRC infrastructure are as under:

1. Conduct a review of controls surrounding the two data centers of the Bank located in the premises of different Service Providers (Data Centers situated at Chennai & the Disaster Recovery site at Hyderabad) and identify any weaknesses therein. Security review is required to the extent of segregation of duties between different layers of the users and administrators and network security administration functions.
2. Adequacy of the existing Procedure like Physical and Environmental Security Procedure, Incident handling procedure, Log Monitoring, Patch management Procedure, Change Management Procedure, Configuration Management Procedure, Vulnerability assessment procedure etc.,
3. Verification of data updation, fall back systems & procedures, data synchronization

4. Review the availability of Disaster Recovery Mechanism and the preparedness of DR team etc.
5. Review to know whether written down procedures are available
6. Whether sufficient number of employees are trained in the DR Mechanism
7. The conformance of the Back Up / Recovery Plan with the prevailing standards, regulatory stipulations and/or government regulations
8. The effectiveness of the plan, by reviewing the results, from the tests carried out
9. The conformance of the recovery site with the security and environment controls
10. The ability and readiness of personnel to react and respond quickly, in situations of disaster
11. Review of the outsourcing arrangement.
12. Adequacy of Networking and Redundancy for the same vis-à-vis industry standards.
13. Identification of Critical Business for BCP/DR purpose
14. Owned and shared resources with supporting function for BCP/DR
15. Risk assessment on the basis of Business Impact Analysis (BIA)
16. Formulation of Recovery Time Objective (RTO) and identification of Recovery Point Objective (RPO)
17. The adequacy of the Practices in force in comparison with industry standards.

6. Vulnerability Assessment and Penetration Tests (VAPT):

The scope includes conducting Vulnerability Assessment and Penetration Tests (VAPT) covering all servers, operating systems, database, networking and Security Infrastructure and various on-line applications facing customers as detailed in List of assets given below which is illustrative. In case of need, they can conduct the VAPT on other servers and applications, with the concurrence of the Audit Department.

List of Assets / Processes that may be covered for IS Audit under this RFP:

1. Core Banking related Systems:
2. Enterprise Wide Network covering all its branches and offices spread across the 13 districts of Odisha State including network equipment and security equipment.
3. Bank's Finacle Core Banking Solution including application, operating system, databases, interfaces, DR site at Hyderabad and DC at Chennai etc.
4. IT Security Setup, with multiple layered firewalls, Network based and Host based intruder detection and prevention systems, two factor authentication systems, anti-virus systems, Patch Management system, Network Access Control systems etc. Bank has also created VLANs, militarized and de- militarized zones in the process.
5. Corporate email setup/Mailing Solution.
6. Bank's internet web site.

Review of Network Security:

The Bank's network support is outsourced and the personnel from the company manage the network from our premises. A MPLS-VPN network supports the Bank's CBS with redundancies built in at device level, media level and service provider level. All the Regional network nodes and two data centres are provided with dual MPLS VPN Connectivity sourced from two different service providers.

Additional SCOPE:

1. Conduct a review of controls surrounding the current network security within the Bank's network, and identify any weakness therein. Security review is required to the extent of

segregation of duties between users, network administration and network security administration functions.

2. Adequacy of the existing Procedure like Incident handling procedure, Downtime analysis, Log Monitoring, Patch management Procedure, Router-Switch-Firewall- IDS Management Procedure, Antivirus procedure, Vulnerability assessment procedure etc.,
3. Effectiveness and Efficiency of the Anti-Virus Software Implementation vis-à-vis industry standards.
4. Effectiveness and Efficiency of the Network Monitoring Tool Implemented.
5. Review of the outsourcing arrangement (SLA) in totality vis-à-vis industry standards.
6. E-Mail rules and requirements – Information storage and retrieval
7. Review of Network vulnerabilities
8. Verification of weak/default passwords in Network devices
9. Review of security of Data in transmission
10. Review of Network performance issues
11. Adequacy of capacity of communication facilities and Hardware
12. Review of security of Email Solution and its penetration & vulnerability test.
13. Penetration & Vulnerability test of web site.

1.4 SCOPE OF WORK

Bidder / Firm/Organisations will be selected on the basis of L1 for a period of 2 years and in each year the IS Audit will be conducted by the Bidder / Firm/ Organisations. Bank may extend the rate of contract for another period of one year subject to satisfactory performance of bidder. The IS Audit as per scope should be completed within 3 months.

1.5 PAYMENT TERMS:

The invoice value of the IS Audit shall be paid on arrear after successful completion of IS Audit and submission of final Audit Report. Payment shall be released by Head Offices (ITD) on submission of GST complaint Invoice.

1.6 PRICES AND TAXES

1. The quoted fees shall be exclusive of all taxes.
2. Applicable taxes like TDS, if any will be deducted from the amount payable.
3. Quoted fees should be furnished as per Commercial bid in Annexure A.
4. Quoted fees submitted with an adjustable price quotation will be treated as non- responsive and will be rejected.
5. Quoted fees shall be quoted in Indian Rupees. Any reference made to variation in pricing due to appreciation / depreciation of Indian rupees against any other currency is not acceptable.
6. Quoted fees shall be valid for a period of 90 days from the last date for submission of bids. Bids submitted with a short validity period will be treated as non-responsive and will be rejected.
7. Quoted fees shall be submitted strictly as per the format given in the bid and any addition / deletion / change in the format will be summarily rejected.
8. Quoted fees without signature of authorized signatory of the bidder will be summarily rejected.

1.7 EVALUATON OF BIDS AND AWARDING THE CONTRACT:

1. **Evaluation of Bids :**

Bids will be opened and evaluated for awarding the contract. The Bank's evaluation of the bids will take into account the following factors.

a. Status of Compliance of terms and conditions of clause.
b. Submission of Bids strictly in the format specified in Annexure A to E of RFQ.

2. Determination of L1 Bidder and Awarding of Contract:

Bank will determine the L1 bidder through the bid submitted by the bidders/ Firms/Organisations:

a. The L1 bidder will be determined based on the lowest PRICE QUOTED excluding taxes as per ANNEXURE - A.
b. Bank reserves the right to negotiate on the L1 price.
c. The Bank reserves the right to reject the L1 bid if it finds the same as higher than market standard.

2. GENERAL TERMS & CONDITIONS:

2.1 SUBMISSION OF BIDS:

Bidders have to submit their bid in Tender Box located at IT Department of Bank / by hand or through post on or before the time line stipulated vide clause 1.1 of the RFQ.

Bank will not allow any bids to be submitted after the deadline for submission of bids. In the event of the specified date and time for the submission of bids, being declared a holiday for the Bank, Bank will receive the bids up to the appointed time on the next working day. Extension / preponement of submission date and time will be at the sole discretion of the Bank.

Bids submitted by any other means other stated above will not be accepted by the Bank.

2.2 SUBMISSION OF DOCUMENTS:

Bidder should submit the supporting documents in a sealed cover to the address notified in the clause 1.1 of the RFQ.

In case the above documents are not submitted on or before the schedule mentioned in clause 1.1 of the RFQ, the bid will be rejected even if the same is not submitted.

The above documents in a sealed cover should be put in the tender box kept in the Information Technology Department of the Bank's Head Office, Bhubaneswar on or before the date and time mentioned in the Schedule for bidding process given in clause 1.1of this RFQ or they may be handed over to the designated officer of the Bank's Information Technology Department, Head Office, Bhubaneswar mentioned in clause 1.1 of the RFQ.

2.3 BID OPENING PROCESS:

The bid submitted in Bank shall be opened in the presence of available authorized representatives of the bidders/Firms who chose to remain at the time, date and venue mentioned in clause 1.1 of this RFQ.

The evaluation of bid and selection of L1 bidder shall be based on the criteria set out in

Annexure A of this RFQ.

2.4 BANK'S RIGHT TO ACCEPT OR REJECT ANY OR ALL BIDS.

Notwithstanding anything contained in any of the clauses, Bank hereby reserves its right to accept or reject any or all the bids and to annul the bidding process 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 the Bank's action.

2.5 ACCEPTANCE OF CONTRACT.

Within 10 days (exclusive of holidays) of receipt of the Purchase Order, the successful Bidder/s shall sign, affix official stamp and date the duplicate copy / photo copy of the Purchase Order and return it to the Bank as a token of having accepted the terms and conditions of the Purchase Order. After receiving the work order, the L1 bidder/Firm/Organisation should execute NDA (Non-Disclosure Agreement) within 7 days of accepting the work order.

2.6 LIMITATION OF LIABLITY:

The liability of bidder under the scope of this RFQ is limited to the value of the relevant Order.

2.7 COMPLIANCE TO LABOUR ACT:

As per Government (Central / State) Minimum Wages Act in force, it is imperative that all the employees engaged by the bidder are being paid wages / salaries as stipulated by government in the Act. Towards this, successful bidder shall submit a confirmation as per format provided in Annexure E of the RFQ.

2.8 OTHER TERMS AND CONDITIONS

i) The Bank shall have the right to withhold any payment due to the Successful Bidder, in case of delays or defaults on the part of the Successful Bidder. Such withholding of payment shall not amount to a default on the part of the Bank.

ii) Successful Bidder/Firms shall hold the Bank, its successors, Assignees and administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to the Bank through the action of its technical resources, employees, agents, contractors, subcontractors etc. However, the Successful Bidder would be given an opportunity to be heard by the Bank prior to making of a decision in respect of such loss or damage.

iii) SUCCESS BIDDER / Firms (Successful Bidder) shall be responsible for managing the activities of its personnel and will be accountable for both. SUCCESS BIDDER shall be vicariously liable for any acts, deeds or things done by their technical resources, employees, agents, contractors, subcontractors etc. that is outside the scope of power vested or instructions issued by the Bank.

iv) SUCCESS BIDDER/ Firm shall be the principal employer of the technical resources, employees, agents, contractors, subcontractors etc. engaged by SUCCESS BIDDER and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of power or outside the scope of power, vested under the contract to be issued for this tender.

v) The indemnification is only a remedy for the Bank. The successful bidder 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.

vi) SUCCESS BIDDER/FIRM shall be held entirely responsible for the security and the protection of their workers at all times inclusive of non-working hours. They shall be deemed to have included for all costs associated therewith, including cost of insurance, medical expenses etc if any. SUCCESS BIDDER shall inform all his employees, technical resources, employees, agents, contractors, subcontractors etc associated in execution of the work awarded under this RFP, to work in the specified area and they should not move around at other places of premises without any specific reason.

vii) SUCCESS BIDDER or its authorized agents or its employees / technical resources shall not store or allow to store in the Bank's premises any goods, articles or things of a hazardous, inflammable, combustible, corrosive, explosive or toxic nature.

viii) SUCCESS BIDDER/ FIRM and its employees, technical resources, agents, contractors, subcontractors or its authorized agents shall provide full co-operation to other agencies working in the premises and shall follow the instruction of site in charge. No extra claims shall be entertained on account of any hindrance in work.

ix) SUCCESS BIDDER/ FIRM shall not be entitled to any compensation for any loss suffered by it on account of delays in commencing or executing the work, whatever the cause of delays may be including delays arising out of modifications to the work entrusted to it or in any sub-contract connected therewith or delays in awarding contracts for other trades of the Project or in commencement or completion of such works or for any other reason whatsoever and the Bank shall not be liable for any claim in respect thereof.

x) It is well defined and understood that the labour or any employee or technical resources of the SUCCESS BIDDER will have no right for claim of employment on the Bank.

xi) No extra claim shall be entertained on account of all the redo of work on account of SUCCESS BIDDER's/ FIRMs negligence and resulting into make good of the damages or damaged portions during executing the job. All such cost shall be borne by the SUCCESS BIDDER.

xii) SUCCESS BIDDER/FIRM shall indemnify the Bank from all the acts & deeds on account of negligence by his employees, agencies, representatives or any person acting on his behalf.

xiii) SUCCESS BIDDER/ FIRM shall take all risk Insurance coverage for its employees, technical resources, representatives or any person acting on his behalf during the contract period to cover damages, accidents and death or whatever may be.

xiv) SUCCESS BIDDER should indemnify the Bank for Intellectual Property Rights (IPR) / copy right violation, confidentiality breach, etc, if any.

Bidder/ FIRM should submit Commercial Bid (Annexure A) along with Annexure B to E.

ANNEXURE – A

Format for Commercial Bid

1. Name of Bidder :
2. Address of Corporate Office :

TABLE –I Format for Commercial Bid (Excluding Taxes)
IS Audit as mentioned in the scope of work

a. Audit Fees including all expenses:
b. Taxes (If any) :
c. TOTAL :

**** All price should be in INR (Indian Rupee).**

Note: L1 will be determined on lowest price quoted.

We certify that bid price quoted above is as per **Annexure-A** of the RFQ No. OGB/RFQ/ITD/VAPT/011/2021-22 dated 03rd February 2022 and prices quoted are all in compliance with the terms indicated in the RFQ No. OGB/RFQ/ITD/VAPT/011/2021-22 dated 03rd February 2022 . We also confirm that we agree to all the terms and conditions mentioned in this RFQ ref OGB/RFQ/ITD/VAPT/011/2021-22 dated 03rd February 2022.

Authorized Signatory **Name and Designation** **Office Seal Place:**
Date:

We certify that we are empanelled in the list of cert-in IS Auditing Firms/ Organisations and authorize to perform the IS Audit. We are having ISO certificate from the Appropriate Authority.

Authorized Signatory **Name and Designation** **Office Seal Place:**
Date:

ANNEXURE – B

The General Manager,
Information Technology Dept,
Odisha Gramya Bank, Head Office,
Gandamunda, Khandagiri,
Bhubaneswar – 751030

Dear Sir,
UNDERTAKING OF AUTHENTICITY FOR IS Audit

Dear Sir,

Sub: IS Audit (As per Scope)
Ref: Your RFP reference No: RFQ No. OGB/RFQ/ITD/VAPT/011/2021-22 Dated 03rd February 2022

With reference to the IS Audit as per scope/quoted to you in response to the above RFQ, we hereby undertake that all the components / Firmware/ software/tools to be used are the products of the bidder/firm/organisation or are of their third party approved vendors.

It will be our responsibility to complete the IS Audit as per scope within 3 months after signing of NDA.

Authorized Signatory **Name and Designation** **Office Seal Place:**
Date:

ANNEXURE – C

LETTER OF UNDERTAKING

The General Manager,
Information Technology Dept,
Odisha Gramya Bank, Head Office,
Gandamunda, Khandagiri,
Bhubaneswar – 751030

Dear Madam/Sir,

1. We hereby confirm that we agree to all the RFQ terms and conditions of the RFQ No. _____dated _____, its Annexure's, amendments made to the RFQ without any pre-conditions. Any presumptions, assumptions, deviations given or attached as part of RFQ will be treated as null and void.
2. We confirm that the undersigned is authorized to sign on behalf of the company /Firm /Organization and the necessary support document delegating this authority is enclosed to this letter.
3. We also agree that you are not bound to accept the lowest or any bid received and you may reject all or any bid without assigning any reason or giving any explanation whatsoever.

Dated at_____ this _____ day of _____ .

Yours faithfully,

For _____
Signature: _____
Name:_____

Authorized Signatory **Name and Designation** **Office Seal**

Place:
Date:

ANNEXURE -D

SELF DECLARATION – BLACKLISTING

The General Manager,
Information Technology Dept.,
Odisha Gramya Bank, Head Office,
Gandamunda, Khandagiri,
Bhubaneswar – 751030

Dear Madam/Sir,

We hereby certify that, we have not been blacklisted/ de-empanelled by Odisha Gramya Bank or by any Central Government / PSU / Banking / Insurance company in India as on date of the RFP.

Authorized Signatory **Name and Designation** **Office Seal Place:**
Date:

ANNEXURE -E

The General Manager,
Information Technology Dept,
Odisha Gramya Bank, Head Office,
Gandamunda,
Khandagiri,
Bhubaneswar – 751030

Dear Madam/Sir,

Sub: Confirmation for Government Rules relating to Minimum Wages:
Ref: RFQ No _____ dated _____

We refer to RFQ no._____ dated_____

In this regard we confirm that the employees engaged by our Company/Firm/Organisation to carry out the services in your bank for the above said contract are paid minimum wages / salaries as stipulated in the Government (Central / State) Minimum Wages / Salaries act in force. We also indemnify the Bank against any action / losses / damages that arise due to action initiated by Commissioner of Labour for noncompliance to the above criteria.

We further authorize the Bank to deduct from the amount payable to the Company under the contract or any other contract of the Company with the Bank if a penalty is imposed by Labour Commissioner towards non-compliance to the "Minimum Wages / Salary stipulated by government in the Act by your company.

Authorized Signatory **Name and Designation** **Office Seal Place:**
Date: