

Corrigendum-1 to GeM Bid ref no. GEM/2024/B/4988346 dated 28/05/2024 for Selection of Vendor for End-to-End Implementation of Audit Solution in Bank for a Period of 5 Years.

It is decided to amend the following in respect of the above GeM bid:

GeM bid document (Bid End date/ Bid Opening Date, Page no. 1 of 7):

Description	Existing details	Amended details
Bid End Date/Time	20/06/2024, 15:00:00	<u>28/06/2024</u> , 15:00:00
Bid opening Date/Time	20/06/2024, 15:30:00	<u>28/06/2024</u> , 15:30:00

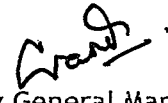
Sl No.	Section/Annexure/Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1	Annexure-2 Pre- Qualification Criteria	Annexure-2 Pre- Qualification Criteria	Existing Annexure	Amended Annexure 2: Pre-Qualification criteria as attached along with this Corrigendum.
2	Annexure-3 Bidder's Profile	Annexure-3 Bidder's Profile	Existing Annexure	Amended Bidder's Profile as attached along with this Corrigendum.
4	Annexure-8 Scope of Work	Annexure-8 Scope of Work	Existing Annexure	Amended Scope of Work as attached along with this Corrigendum.
5	Annexure-10 Technical Evaluation Criteria	Annexure- 10 Technical Evaluation Criteria	Existing Annexure	Amended Technical Evaluation Criteria attached along with this Corrigendum.

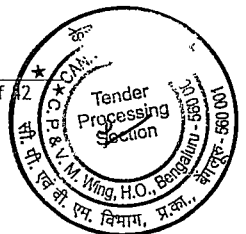
All the other instructions and terms & conditions of the above GeM Bid shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject GeM bid.

Date: 20/06/2024

Place: Bengaluru


Deputy General Manager



Annexure-8
Scope of Work

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of Vendor for end to end implementation of Audit Solution in Bank for a Period of 5 Years

Ref: GEM/2024/B/4988346 dated 28/05/2024.

This scope of work represents our objectives and expectations for the audit package software/Solution. Our primary objective is to augment the effectiveness and efficiency of our audit processes with enhanced transparency, while aligning with regulatory standards and industry best practices. We envision a solution that streamlines workflows, facilitates comprehensive risk assessment and furnishes actionable insights for decision-making.

The audit package must seamlessly integrate with our existing systems, ensuring minimal disruption to our operations. It should be user-friendly, empowering our Inspection Wing to conduct audits with ease and precision. Additionally, robust security measures are imperative to safeguard sensitive data and uphold confidentiality.

The proposed audit software package is a web based application with centralized database and is browser independent, installed centrally and configured within Bank's internal environment. The audit software package should have off-site functioning capability and features of automated work-flow across all processes covering the entire audit activity, risk assessment, monitoring and reporting.

1. Objective:

1.1. Business Objective:

- 1.1.1. Streamline internal audit process to improve efficiency, effectiveness and productivity by minimizing manual effort and increasing transparency.
- 1.1.2. Strengthen the risk management practices and ensure adherence to regulatory requirements.
- 1.1.3. Facilitate decision making through real time access of audit information and insights.

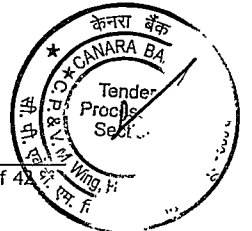
1.2. Technical Objective:

- 1.2.1. Develop a secure and scalable software solution equipped with robust access control mechanisms to safeguard sensitive Banking information.
- 1.2.2. Ensuring scalability and performance to accommodate evolving audit requirements and user expansions.
- 1.2.3. Integrate advanced analytics and reporting functionalities to furnish actionable insights for decision making purpose.

2. Audit Coverage:

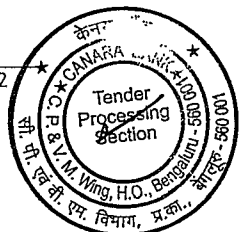
The audit software will comprise of following audit automation:

Internal



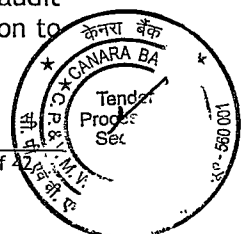
- 2.1. RBIA (Risk Based Internal Audit)
 - 2.1.1. Audit of Branch
 - 2.1.2. Audit of Units (RAH, MSME Sulabh, Currency Chest, ARM, ACC, CPH)
 - 2.1.3. Audit of Regional Office and Circle Office
 - 2.1.4. Audit of Foreign Branch (New-York, London, Dubai, GIFT City-Ahmedabad)
- 2.2. Regular Inspection
 - 2.2.1. Audit of Wing and Vertical
 - 2.2.2. Audit of Zonal Inspectorate
 - 2.2.3. Misc regular audits (Due diligence of outsourced activity, liquidity risk management framework at RM wing, etc.)
- 2.3. Concurrent/Continuous Audit
 - 2.3.1. Audit of Branch
 - 2.3.2. Audit of Units (RAH, MSME Sulabh, Currency Chest, ARM, ACC, CPH)
 - 2.3.3. Audit of Accounts opened in CPH and VCIP
 - 2.3.4. Audit of Regional Office
 - 2.3.5. Audit of Wing and Vertical (MSME, CAM, TM, Recon Vertical, CPCFT, CPCIT, Treasury-Domestic, Treasury-Forex, Card Division, CPPC)
- 2.4. Revenue Audit
 - 2.4.1. Quarterly Income Audit
 - 2.4.2. Expenditure Audit of Wing/Vertical Section
 - 2.4.3. Recovery of Income Leakage identified in various audit of all Branch & Unit
- 2.5. Management Audit
 - 2.5.1. Audit of Wing/Vertical
 - 2.5.2. Audit of Regional Office
 - 2.5.3. Audit of Circle Office
 - 2.5.4. Audit of Zonal Inspectorate Audit
 - 2.5.5. Audit of Associate/Subsidiary
 - 2.5.6. Audit of Regional Rural Bank
 - 2.5.7. Audit of Foreign Branch
 - 2.5.8. Audit of MD/ED Secretariat
- 2.6. IS Audit
 - 2.6.1. Audit of Wing/Vertical
 - 2.6.2. Audit of Circle Office
 - 2.6.3. Audit of Branches/Units (Sample Based by Specialized IS auditor)
 - 2.6.4. Application Audit (Pre-implementation and Post-Implementation)

Inter si

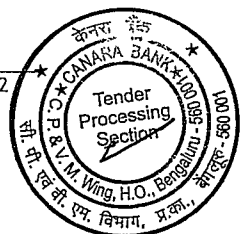


- 2.6.5. Audit of ATM Switch
- 2.6.6. Audit of SWIFT
- 2.6.7. Audit of Associate/Subsidiary including HEFA.
- 2.6.8. Audit of Regional Rural Bank
- 2.6.9. Audit of Units (Data Centre, Data Recovery Centre, All type of Treasury audit, SOC, Global Parameters - FCR Advance, FCR Deposit & FCC-FCUB, Data Warehouse)
- 2.7. Other Audit
 - 2.7.1. Audit of KYC/AML
 - 2.7.2. Snap Audit- MRRBA
 - 2.7.3. Short Inspection
 - 2.7.4. Special Report
 - 2.7.5. Off-site Audit
 - 2.7.6. Thematic Audit based on requirement
- 2.8. Risk Based Internal Audit (RBIA):
 - 2.8.1. Conduct risk based internal audit to assess and prioritize audit engagements based on inherent risk and criticality involved in operation and management of business portfolios.
 - 2.8.2. Develop and implement a comprehensive risk matrix customized according to the Bank's risk appetite and tolerance levels. Business Risk and Control Risk are two major components of risk matrix for arriving final risk grade.
 - 2.8.3. Marking of deviated/irregular observations for accounts as well as audit unit wise mandatory checkpoints determine the final score in control risk.
 - 2.8.4. Conduct risk assessment utilizing recognized methodologies such as COSO (Committee of Sponsoring Organization) framework and ISO 31000 according to the internal policy of Bank.
 - 2.8.5. Integrate the risk matrix into the audit software to facilitate assessment and prioritizing the audit alignments with organizational objectives and regulatory obligation.
 - 2.8.6. Risk matrix framework delineating risk categories, scoring criteria and risk rating methodologies, articulated in banking-specific terminology.
 - 2.8.7. Risk assessment by the software should indicate the level of risk as High, Moderate and Low as well as the trend of risk in terms of increasing, decreasing or stable/Risk movement and analysis. Risk assessment and assignment of Risk grade to the auditee unit to be formulated by the software only without any manual intervention from auditor/admin unit. Modification of risk rating on identification of fraud in the auditee unit before commencement of subsequent RBIA can be done through wing admin only. On modification of risk rating by Wing admin, audit planner will be modified accordingly and software has the provision to prompt such cases in the dash-board.

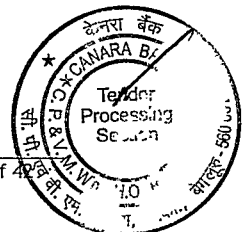
Internal



- 2.8.8. Risk assessment report called as RPRR (Risk Profile cum Risk Rating) report will be furnished with identified risks, impact analysis and risk mitigation strategies tailored to banking operations.
- 2.8.9. Identification of recurring and persisting observations, KRI (Key Risk Indicator) and Significant observations, performing quality audit (compliance audit), Rating of Inspecting officials, Marking Single query/check point for multiple accounts, detection of income leakage, closure of audit with carry-over remarks and closure of audit without carry over observations are some of the key functionalities in assessing the risk parameters.
- 2.8.10. One Inspecting official will be made as team leader while conducting RBIA. Only the team leader can access to queries/checklists raised by other Inspecting Official for alteration. Team Leader has the option to fill executive summary and close the audit. Role of team leader can be mapped to any of the inspecting official of team members during the conducting of audit, managed by respective Zonal Inspectorate.
- 2.8.11. Automatic sampling of loan accounts to be considered under current RBIA. (As per Bank's policy which is updated from time to time.) There should be provision for an auditor to manually add / select an account if he/she identifies observation / irregularity in account which is not included in above sample list.
- 2.8.12. Marking single query for multiple accounts option to be available for Inspecting officials to mark common deviations in the advance related accounts based on scheme code. An option to add/delete any scheme code to be made available at front end for Wing admin user.
- 2.8.13. Certain information like risk rating of auditee unit, overdue of audit etc. to be floated on T+1 basis to BD 360 (Business Dashboard 360) of Bank for consolidation in Daily Dash Board.
- 2.9. Regular Inspection:
- 2.9.1. Regular Inspection is applicable to Head Office Wings & Verticals and Zonal Inspectorate to evaluate compliance with regulatory requirements, assess operational effectiveness and address organizational functional objectives.
- 2.9.2. Risk assessment is not applicable to regular inspection and remaining functionalities are same as RBIA.
- 2.10. Concurrent Audit:
- 2.10.1. Conduct real-time monitoring of transactions and operations to unearth and deter non-complied activities and operational irregularities. Frequency of concurrent audit is monthly or quarterly. Concurrent audit is carried out by both Internal and external auditors.
- 2.10.2. Deploy automated monitoring tools to scrutinize transnational data and detect anomalies or suspicious activities in real-time, supported by banking-specific risk parameters.



- 2.10.3. Conduct continuous transaction monitoring and pattern recognition to identify risks involved in unrealistic business growth and control deficiencies.
 - 2.10.4. Identification of Branches/Units for conducting Concurrent Audit based on Business provision for approving the annual audit plan, generation of appointment letter etc. to be automated in the software.
 - 2.10.5. Evaluate internal controls and compliance measures to ensure efficacy in mitigating risks and preventing anticipated fraud according to regulatory context.
 - 2.10.6. Concurrent audit reports are furnishing findings, recommendations, and risk ratings (applicable for quarterly concurrent audit) tailored to banking operations for management review and remediation.
 - 2.10.7. Appraisal of ECA (External Concurrent Auditor) and evaluation of annual performance on key parameters for renewal or termination of contract for auditing of Branches/units to be facilitate in the software solution.
 - 2.10.8. Remaining functionalities are similar to RBIA.
 - 2.10.9. Certain information like overdue of audit to be floated on T+1 basis to BD 360 (Business Dashboard 360) of Bank for consolidation in Daily Dash Board.
- 2.11. Revenue Audit:**
- 2.11.1. To identify income leakages across diverse banking operations and ensure legitimate income of the Bank is recovered. Income leakage detection and recovery will be covered in RBIA, Concurrent/continuous Audit and Quarterly Income Audit.
 - 2.11.2. Frequency of audit varies based on auditee category and audit type.
 - 2.11.3. Scrutinize revenue-generating processes encompassing lending, deposit, fee-based services, and treasury operations, employing banking-specific metrics and benchmarks.
 - 2.11.4. Implementation plans and monitoring mechanisms to track the efficacy of income leakage recovery initiatives.
 - 2.11.5. Devised several reporting systems to consolidate information regarding income leakage detection and recovery on real time basis.
 - 2.11.6. Information regarding revenue audit to be floated on T+1 basis to BD 360 (Business Dashboard 360) of Bank for consolidation in Daily Dash Board.
- 2.12. Management Audit:**
- 2.12.1. To assess management practices, organizational structures and strategic initiatives to evaluate governance effectiveness and operational efficiency.



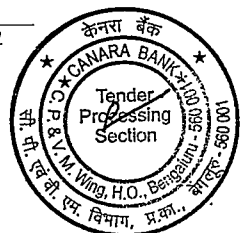
- 2.12.2. To evaluate the efficacy of internal controls and risk management practices in accomplishing organizational objectives and mitigating operational risks.
- 2.12.3. To scrutinize management policies and procedures vis-à-vis human resources, finance, and procurement to ensure compliance with regulatory prerequisites and industry best practices.
- 2.12.4. Assigning of marks to all key parameters by auditor and calculation of risk matrix as defined in Inspection policy to be system based.
- 2.12.5. Action Taken Report (ATR) will be prepared by Inspection Wing and submitted to respective auditee unit for compliance. Auditee unit replies the compliance of ATR points and admin unit based on hierarchy will accept/pushback the auditee reply.
- 2.12.6. Presentation of organogram of auditee unit in pictorial format is one of the key feature in reporting system of Management Audit.

2.13. Information System (IS) Audit:

- 2.13.1. To evaluate IT systems, infrastructure, and controls to safeguard the integrity, confidentiality, and availability of critical banking information.
- 2.13.2. Review IT governance frameworks, policies, and procedures to ensure alignment with banking objectives and regulatory mandates.
- 2.13.3. Assess the efficacy of internal controls in terms of IT policy and Cyber Security policy and risk management practices in realizing organizational objectives and mitigating operational risks.
- 2.13.4. Evaluation of disaster recovery and business continuity plans to ascertain the organization's preparedness for IT disruptions and incidents.
- 2.13.5. IS audit reports replete with findings, recommendations, and risk ratings vis-a-vis IT governance, risk management, and compliance (GRC) frameworks.
- 2.13.6. Action plans and remediation strategies calibrated to address control deficiencies and mitigate IT risks highlighted during the audit.
- 2.13.7. Inclusion of Risk matrix for audit of all wings/verticals with Risk Level being calculated with the parameters Likelihood and Impact. Based on risk matrix calculation Risk grade is awarded and periodicity will be determined through the system by implementing the Bank policy and guidelines.

2.14. Other Audits:

Other audits conducted by the Bank are requirement basis and annual plan is prepared on beginning of financial year. Audit is performed either by Internal or External auditor. Alerts and escalation mechanism by way of SMS/Email/Watts app Message for various events and milestones as required/defined by the Bank should be included in the software.



2.14.1. Audit of KYC/AML:

KYC/AML audit to be conducted in the auditee unit on sample basis as defined in the audit planner to verify the compliance of KYC and AML guidelines for CASA and deposit account opened by the Branch.

2.14.2. Snap Audit - MRRBA:

Snap Audit is conducted in Moderate Risk rated branches where credit growth and cash recovery in NPA accounts is abnormal. Advances and cash recovery made by branch are verified.

2.14.3. Short Inspection:

Short Inspection is conducted in case of VRS/Resignation/Superannuation of bank employees. All the aspects verified during RBIA of branch/unit are verified for the period from date of completion of previous RBIA to date of VRS/Resignation/Superannuation.

2.14.4. Special Reports:

2.14.4.1. Special reports are given in the matter of fraud/suspected fraud, misconduct, major deviation in processing of credit, detection of high income leakage and regulatory infringements etc.

2.14.4.2. Special report are submitted during RBIA, Concurrent Audit, QIA etc. To be consolidated in a single module for further proceedings and actions.

2.14.4.3. Compliance to audit observations to be attended in the consolidated module with in the time frame.

2.14.5. Thematic Audit:

Thematic audit is applicable with respect to compliance with regulatory requirements, assess operational effectiveness, and address specific audit objectives.

2.14.6. Off-site Audit:

Aspects that can be verified without visiting the auditee unit and conducting verification centrally at Head Office.

3. Audit Life Cycle:

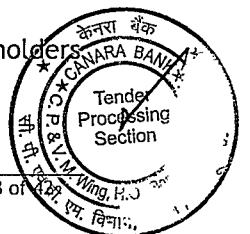
The audit software will cover of following audit life cycle:

3.1. User Management:

3.1.1. User Managements shall be provided for Bank Employees, Ex-Employees and ECA (External Concurrent Auditor).

3.1.2. Proposed Audit package has primarily two type of users/stakeholders i.e. Inspection Wing/Admin Unit and Auditee units.

Internal

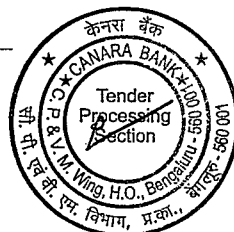


- 3.1.3. Software system should provide login and password management facility and maintain logs for activity of the user on the platform.
- 3.1.4. Bank admin(s) at different hierarchies should be able to add new users, update and remove existing users to/from designated audit unit/branch, roles as per user rights. Also the user/roles of the uses to be integrated with Bank HRMS / Attendance System wherever applicable.

USERS AND ROLE

Sl. No.	USER/S	MAJOR ROLE
01	SUPER ADMIN	<ol style="list-style-type: none"> 1. User profile maintenance of HO Admin 2. Reopen of Audit 3. Checker for Addition/ Deletion/ Modification of Checkpoints 4. Authorization of Re-risk Rating 5. Mapping of newly added Branches/Units 6. Providing access control to end users 7. Extension of Audit (Checker) 8. Report/Dashboard view
02	INSP WING, HO ADMIN	<ol style="list-style-type: none"> 1. User profile maintenance of HO Admin, ZI Admin 2. Authorization of Audit Report, If applicable 3. Checker for Addition/ Deletion/ Modification of Checkpoints 4. Commencement, Closure of Audit, wherever applicable. 5. Authorization of Re-risk Rating 6. Extension of Audit (Checker) 7. Report/Dashboard view
03	INSP WING, HO PROCESSOR	<ol style="list-style-type: none"> 1. User profile maintenance of HO Admin, ZI Admin 2. Processing of Audit Report, If applicable 3. Maker for Addition/ Deletion/ Modification of Checkpoints 4. Commencement, Closure of Audit, wherever applicable. 5. Report/Dashboard view
04	ZI ADMIN/ PROCESSOR	<ol style="list-style-type: none"> 1. User profile maintenance of Auditor/Inspecting Officer/ECA, CO Admin and RO Admin

Internal

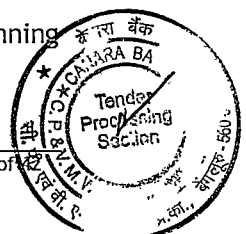


		<ol style="list-style-type: none"> 2. Commencement, Closure of Audit, wherever applicable 3. Pushback of Audit Reply made by Auditee after accepted by RO/CO. 4. Request for extension of Audit. (Maker) 5. Request for re-open of audit. 6. Rating of Inspecting Officer/ECA 7. Report/Dashboard view
05	INSP OFFICER/ ECA	<ol style="list-style-type: none"> 1. Marking of Audit Findings 2. Accept/Deny of Branch/units reply 3. Quality Audit 4. Finalization of Audit Closure report 5. Completion of Audit 6. Dashboard/Report view
06	RO/CO ADMIN	<ol style="list-style-type: none"> 1. User profile maintenance of RO User/ Branch or Units Admin 2. Accept/Deny to Audit findings 3. Report/Dashboard view
07	RO/CO USER	<ol style="list-style-type: none"> 1. User profile maintenance of Branch or Units Admin 2. Accept/Deny to Audit findings 3. Report/Dashboard view
08	BRANCH OR UNITS ADMIN/USERS	<ol style="list-style-type: none"> 1. User profile maintenance of Branch/Unit users. 2. Reply to audit findings 3. Other Compliance 4. Report/Dashboard view
09	REPORT VIEW USERS FROM OTHER WING	<ol style="list-style-type: none"> 1. Report/Dashboard view

3.2. Audit Planning:

- 3.2.1. The Audit software to be automated for mapping of branch and units directly with Bank Branch master to retrieve branch and units profile.
- 3.2.2. Advanced algorithms and decision support tools for auto calculating of audit plan based on audit scope, classification of audit units and risk assessment. The Audit software solution will utilise past and current information to assign risk ratings to the auditee units through AI & ML.
- 3.2.3. Integration of organizational calendars and resource management systems to optimize audit scheduling and resource allocation.
- 3.2.4. Implementation of machine learning algorithms to assess the planning for newly opened auditee unit.

Internal



3.2.5. The System will disable editing of audit findings and replies after the closure of audit engagement. Reopening of audit engagement will be facilitated within the solution itself to Super Admin.

3.2.6. The Audit solution will maintain history of previous engagements and admin user can track the audit planner for all phases of audit engagement.

3.3. Data Extraction:

3.3.1. The audit package must possess robust functionality to extract pre - audit data and statistical information related to Business from various sources such as the Enterprise Data Warehouse (EDW) as per BD 360, Core Banking Solution (e.g., Flexcube), LAPS, different modules of SAS etc.

3.3.2. To ensure efficiency and compatibility, data extraction from various systems should be facilitated through the use of ready connectors. These connectors must be adept at extracting diverse data types efficiently, streamlining the extraction process and ensuring accuracy.

3.3.3. Pre-audit data and information primarily consists of a variety of data types essential for audit assessments. These may include:

- Existing reports: Reports generated from different banking solution.
- Transaction data: Detailed records of financial transactions.
- Queries and Checklists: Non-complied/carry over queries or checklists of previous audit and data for quality audit.

3.3.4. Data extraction is executed through scheduler on daily/monthly/Quarterly basis based on requirements in audit modules.

3.3.5. The proposed software solution should be capable of matching and triggering the auto-populated verified data from above said modules with audit findings through machine learning concept.

3.3.6. Existing audit reports like closure report, RPRR report (except RBIA-Branches/Units), Jotting Sheet of Query and Checklist, Query Summation sheet from all modules to be migrated to proposed audit package. Also, DB information of past and current ongoing audit to be migrated to the schema of new DB of proposed audit package.

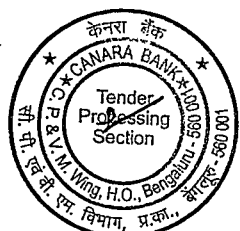
3.4. Audit Execution:

3.4.1. Implementation of secure protocols and encryption mechanisms for collection, storage and transmission of statistical business information and advance account details.

3.4.2. Implementation of secured storage facility for audit findings, compliance and audit evidence.

3.4.3. Adoption of distributed task management frameworks to facilitate efficient audit exercise and data collection processes.

Internal



- 3.4.4. Capturing of immutable audit trail for all activities involved in audit process.
- 3.4.5. Implementation of risk matrix and auto calculation of scores for finalizing of risk grade for the auditee units as per the Bank policy and guidelines.
- 3.4.6. The system should maintain historical audit risk rating, risk profile of auditee units for future reference.
- 3.4.7. Machine learning to be adopted for persisting and recurring audit finding by referring the past audit conducted in the auditee unit.
- 3.4.8. Identification of non-complied items of previous audit to conduct quality/compliance audit.
- 3.4.9. The package should have provision for uploading of support documents by auditee unit/inspecting official.
- 3.4.10. The system facilitates the collection of feedback from auditee units on audit team at the conclusion of audit engagement.

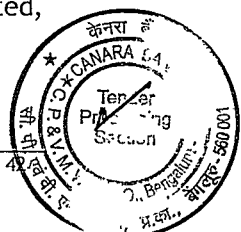
3.5. Audit Follow-Up:

- 3.5.1. Deployment of automated workflow engines to track pending audit findings, corrective actions and associated follow up activity.
- 3.5.2. Utilization of predictive analytic capabilities to anticipate audit trends and proactively address the compliance issues.
- 3.5.3. Machine learning techniques to be implemented for keeping track of carry over audit findings and its compliance within time frame.
- 3.5.4. Various consistency functionalities to be engineered in the software for assurance of correct closure of audit report.

3.6. Audit Reporting:

- 3.6.1. Development of customized report templates leveraging industry standard reporting frameworks to ensure consistency and accuracy.
- 3.6.2. Incorporation of data visualization techniques and interactive dashboards to facilitate intuitive analysis and presentation of audit findings
- 3.6.3. Integration with advanced analytic tools (e.g. Power BI, Tableau) for dynamic MIS reporting and trend analysis for decision making and follow up.
- 3.6.4. Output should be a printable format with full alignment of text, images & tables.
- 3.6.5. Audit software package should have the capability to host and generate template documents like Audit Closure Report, Risk Rating Report, Query/Checklist Summary & Detailed Report, Income leakage detected,

Internal



recovered and pending for recovery report by extracting data from various modules, Query/checklist Jotting Sheet etc.

3.6.6. Major MIS reports required in the audit modules are:

- Audit Status report on daily basis
- List of Risk Rating of Auditee Branch/Units
- Overdue report for various stage of audit
- Spot Rectification Report before completion and after completion
- Audit Planner report
- Search report of Audit findings dump
- Risk Rating cum Risk Profile report
- Re-risk rating report
- Audit Trail Report
- Any other ad-hoc report required at the time of implementation & later on.

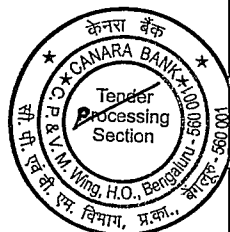
3.7. Audit Integration:

- 3.7.1. Provision of robust APIs and middleware solutions to facilitate seamless integration with existing enterprise systems. Integration with existing Bank software is one way and carried out on batch process. Details of integration to be discussed after finalization of bidder.
- 3.7.2. Implementation of data mapping and transformation logic to enable interoperability and data exchange between disparate systems like BD 360, Data warehouse, SAS, LAPS, HRMS and Other packages of the Bank.
- 3.7.3. Provision to be made for conducting offsite audit from remote place through API integration with various platforms available within the Bank.
- 3.7.4. Supporting for industry standard messaging and email protocols for real time data integration and communication.

3.8. Audit Universe:

- 3.8.1. The audit universe represents the auditable units of the Bank and mapped to the organizational structure. This serves as a centralized platform where the annual audit planner, audit stages, and achievement percentages of audit conducted for the financial year are compiled on single interface.
- 3.8.2. It provides an overarching view of the organization's audit activities and progress, facilitating the development of an effective audit strategy.

Internal

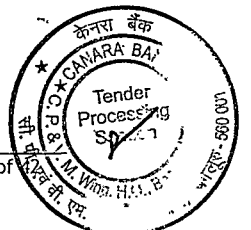


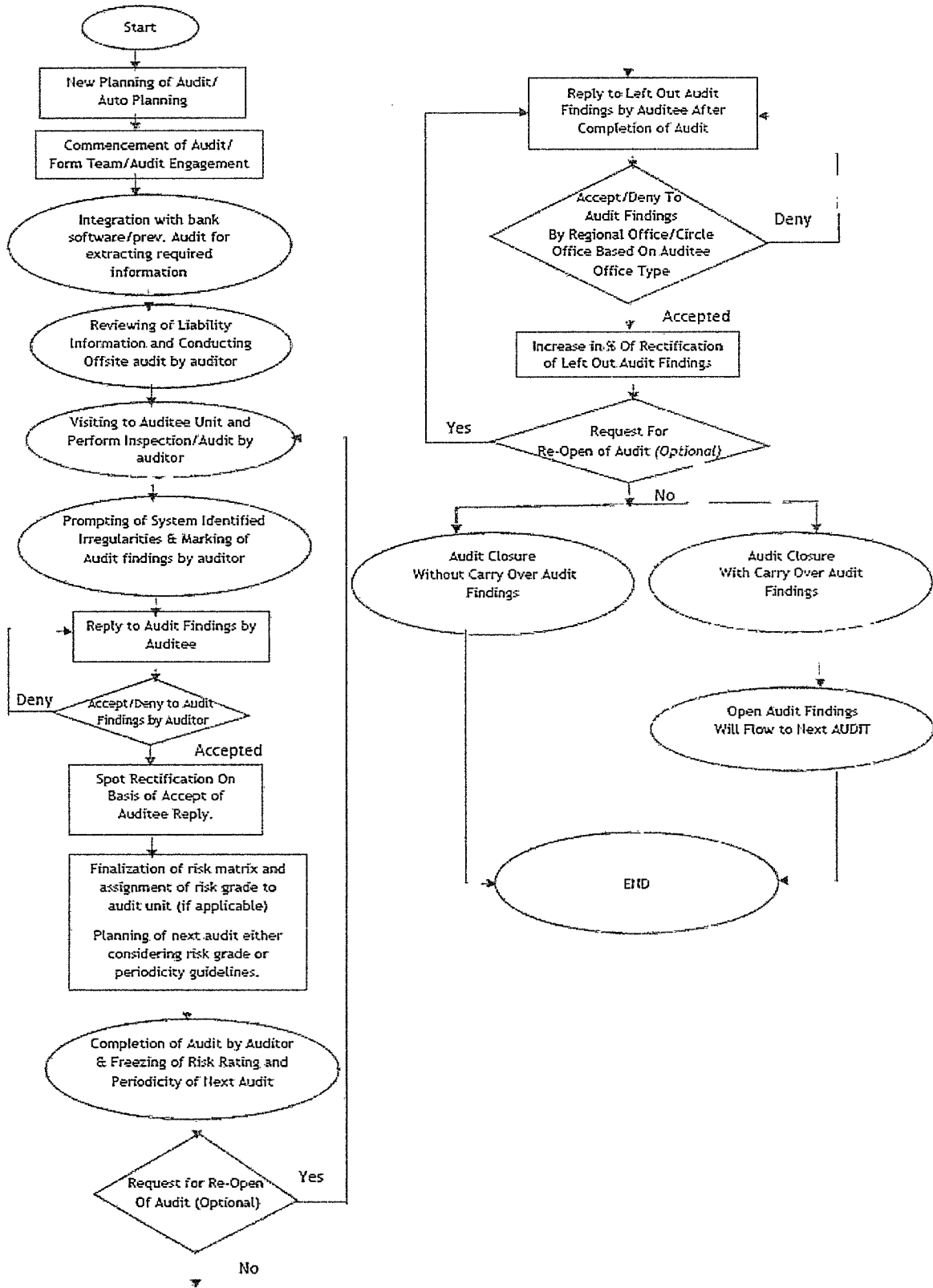
3.8.3. Branch profile to be integrated with Bank Branch master to keep record of Live and closed auditee units. Audit status from all audit module to be assembled and provide an abstract and detailed view for audit universe.

3.9. Audit Process flow:

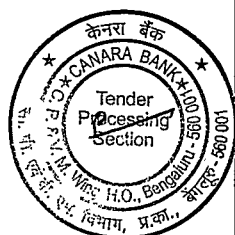
Audit process flow covering the major stages of audit described in below flow chart. The structure may change depending on the scope and functionalities required of audit module.

Internal





Note: Above process flow of audit is an overall understanding to audit life cycle, which may be changed based on the requirements or type of audit.



4. Business/Functional Requirements:

4.1. Common Business/Functional Requirements for Audit Software:

4.1.1. Workflow Engine:

A robust workflow engine is necessary to automate audit processes, manage task assignments, and track progress throughout the audit life cycle. It should support flexible workflow configurations to accommodate varying audit requirements and methodologies.

4.1.2. Checkpoints and Product/Scheme Mapping:

The software should incorporate predefined audit checkpoints and queries to ensure thorough and consistent audit execution. Checkpoints should cover key areas such as regulatory compliance, operational controls, and risk management practices. Parameters in audit checkpoints are divided into a) Credit Parameters and b) Non-Credit parameters.

Provide functionality for adding, editing, deleting and archiving checklists, ensuring data consistency and accuracy. Implement maker and checker concept where makers can propose changes to checkpoint/queries and checker reviews and approves these changes before it is finalized. Enable automated notifications to alert makers and checkers for pending actions and approval of changes.

Incorporate version control mechanisms to track and manage different versions of checkpoint/queries to ensure the effective date. Newly added/Modified/Deleted checkpoint/queries should not be retrospective effect on legacy data and should be implemented in ongoing/new audits.

Addition of new product or scheme launched (both deposit and advances) by the Bank to be incorporated from front end by the admin. Applicable queries to be mapped to the respective product or scheme code by the admin.

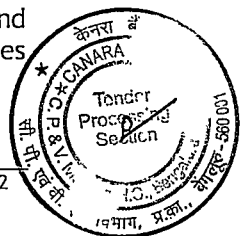
4.1.3. Risk Calculation:

Algorithms should facilitate risk calculation based on predefined parameters as prescribed in the Bank policy (Either Queries or Checklists or combination of both) and historical data. The software should provide mechanisms for assessing inherent risks, control effectiveness, and residual risks across various banking operations. Checkpoints and queries carry weightage to ensure inherent risk and probability of criticality and linked to risk rating of auditee unit.

4.1.4. Evidence Uploading:

Users should be able to upload supporting evidence, documents, and attachments directly within the software. This facilitates

lnema1



documentation of audit findings, substantiation of recommendations, and collaboration among audit team members.

4.1.5. Data Analysis:

Advanced data analysis tools should enable in-depth analysis of audit data, trends and patterns. The software should support various analytical techniques such as trend analysis, regression analysis, and outlier detection to identify anomalies and insights.

4.1.6. Audit Output:

The software should generate comprehensive audit reports, risk rating report, summaries and findings. Reports should include detailed descriptions of audit objectives, methodologies, findings and recommendations, along with supporting evidence and documentation as prescribed by the Bank.

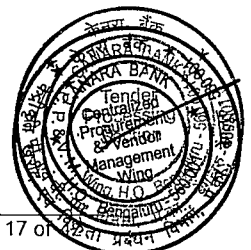
4.1.7. Report Generation:

The software should provide customized reporting templates, dashboards and visualizations. Reporting capabilities should support drill-down functionality, filtering options and interactive elements to facilitate stakeholder communication and decision-making. Facility to generate standard/ ad-hoc MIS reports on various parameters/ status on/ across various audits, say, in terms of domains / classification of observations / areas of audit activities, auditee wise, etc. with drill down/ across feature over more than one variable - Exceptions observed/ closed/ pending/ criticality - Branch/unit wise, Region/Circle wise, exception-wise, pending issue-wise, age-wise, Date wise, criticality wise and other parameters dynamically. The report generation tool should be user-friendly with drag & drop facility to add a new column or field. Use of Power Bi or comparable platform for the Audit output board is preferred.

4.1.8. Report Confidentiality:

There would be access control for viewing and downloading of the various reports. A report when downloaded should preferably contain timestamp and User Id of the user at the footer. It may be noted that the application should give an option to users at the time of downloading of reports whether user wants the report preferably in Word, Excel, PDF or any other format.

- i. A provision for the Auditor to give suggestions / learning points / highlights/ confidential inputs to the Top Management.
- ii. Search & MIS Report Generation: A facility to search Risk level reports / findings in terms of Departments / Offices / Areas or any other relevant parameters with required data protection and user access controls is required. Generation of reports related to status of compliance submission on user defined parameters.



Internal

- iii. The application should have the functionality of graphical representation and generation of reports of risk movement of the processes / audit units / Business Units, etc.
- iv. Notifications: The system would alert various stakeholders through e-mails at different levels at the time of generation of reports; reminders for non-submission; escalation of pending items to various higher levels, periodical pending status, etc. Additionally, system should also raise an alert as per the assigned parameters / crossing of deadline given by the auditee office in the audit report.

4.1.9. Risk Matrix:

The risk matrix should define risk grades for auditee units based on various business and control parameters. These parameters may include financial impact, regulatory compliance, operational complexity, and strategic importance. Criticality assessment is a key component of the risk matrix. It involves evaluating the criticality of each auditee unit based on its importance to the overall business objectives and control aspect.

4.1.10. Risk Monitoring:

Real-time monitoring features should enable ongoing tracking and monitoring of identified risks. The software should provide configurable alerts, notifications, and dashboards to notify stakeholders of significant risk events and deviations from expected norms.

4.1.11. Risk Mitigation:

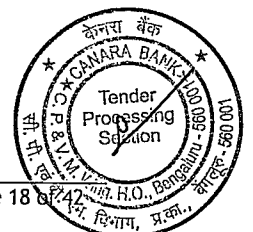
The software should facilitate the implementation and monitoring of risk mitigation strategies. This includes tracking action plans, assigning responsibilities, and monitoring progress towards risk mitigation goals.

4.1.12. Message Triggering:

Automated message triggering functionality notifies stakeholders of audit commencement, provisional completion dates, and distribution of risk rating reports. It enables customization, automation, and integration with audit processes, ensuring timely communication and coordination while maintaining an audit trail for accountability.

As and when a new audit is scheduled and a team is formed, New Audit System should send a system based intimation and intimation e-mail/WhatsApp Message to the Auditor of the audit assignment / team along with the Auditee team. The Audit supervisor should have the option of sending system based intimation and intimation e-mails/WhatsApp message to the team members about the audit assignment and allocation of areas for uploading.

Internal



4.1.13. Notification & Alerts:

Configurable notification and alert mechanisms should notify stakeholders of upcoming audit activities, overdue tasks, or critical audit findings in the package itself.

4.1.14. Document Management:

A new document management features should enable for secure storage, version control, and retrieval of audit-related documents and artefacts. The software should support document categorization, tagging, and search functionalities to facilitate document management and retrieval.

4.1.15. Statistical Modelling Techniques:

- (i) Analytics: The system should also include intelligent and actionable cross audit analytics by reading data from various audits (Credit Audit/ Concurrent Audit / Risk Based Internal Audit (RBIA) etc.)/ Incident Reports, exception reports from other applications, mainly AMS and throw up alerts / warning indicators.
- (ii) Statistical Modelling Techniques: The system should have ability to show trend analysis, predictive analysis, etc. based on Statistical modelling techniques.
- (iii) The system should be able to analyse the checklist / incident reports / Audit reports / RR over a period of time / data and be able to throw up areas where similar risks / procedural errors are happening on an on-going manner.
- (iv) Integration of all audit modules to consolidate the non-complied observations made by the Inspector for the review period to be analysed and available in dash board.

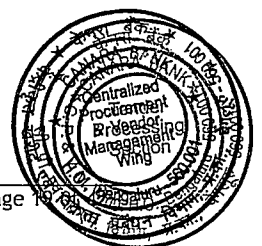
4.1.16. Escalation Ladder:

Escalation ladder in the audit package establishes a structured framework for addressing audit findings, overdue position, uncompleted items promptly. It defines clear criteria for escalating unresolved issues, outlines hierarchical escalation procedures and mandates timely resolution responsibilities for each level of authority. Communication protocols ensures stakeholders are informed of escalated findings efficiently, while monitoring tools track the status of escalated issues for oversight and decision making.

4.1.17. Compliance Tracking:

The software should track compliance with regulatory requirements, internal policies, Basel III norms and audit recommendations. Compliance tracking features should include automated reminders, status updates, and reporting functionalities to monitor compliance efforts effectively.

Internal



4.1.18. Audit Logs:

Comprehensive audit logs should record all audit activities, changes, and user interactions within the software. Audit logs should provide a detailed trail of audit actions, facilitating transparency, accountability, and audit trail integrity.

4.1.19. Training & Knowledge Transfer:

The software should provide training materials, user guides, and knowledge transfer resources to facilitate user adoption and proficiency. Training modules should cover software functionalities, audit methodologies, and best practices for audit execution.

4.1.20. Tracker Package:

A simple tracker package to be designed to keep track of encountered troubleshooting raised from Zonal Inspectorate and Inspection wing, HO and TAT (turnaround time) for resolution.

4.2. Audit specific additional functional requirement:

- 4.2.1. Provision to reopen audit, extension of audit period to be enabled in Audit software solution. The process involved for audit reopen and extension must be fully automated and audit planner to be modified accordingly.
- 4.2.2. Rating of inspecting official by auditee unit to be enabled in RBIA/Concurrent audit of branch/unit. A consolidated report to be made available for wing admin user.
- 4.2.3. Quality audit in RBIA/Concurrent audit of branches: Verification of compliances reported by branch/unit in the previous audit.
- 4.2.4. Provision to view specific OTM (Offsite Transaction Monitoring, already in use by the Bank) alert for the review period through API in RBIA and Concurrent Audit.
- 4.2.5. Machine learning technique to be implemented for identification of Significant audit findings.
- 4.2.6. There should be a provision for uploading process related instructions / circulars required by auditors or Auditee.
- 4.2.7. Provision for modification of risk awarded to auditee units by the Wing admin user.
- 4.2.8. Uploading the Bank's updated guidelines/ circulars/ manuals formats / checklists from where the user can refer for easy and ready reference / Facility to mark them to various types of audits.
- 4.2.9. System shall maintain and update the branch/auditee profile i.e. category, risk profile, etc. Provision to map with Live data of Bank's branch Master with version control to be available.

Internal

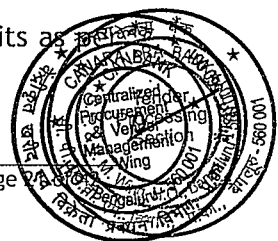


4.2.10. Audit Software should comply with the official language policy so that audit Report/Compliance can be submitted in Hindi also.

5. Technical Requirements:

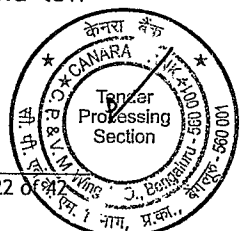
5.1. Common Technical aspects of the package:

- 5.1.1. The software infrastructure must facilitate access from both Internet and Intranet environments. Implementation of security measures, data encryption, secure authentication protocols (such as SSL/TLS), access controls to be ensured while accessing the data over internet.
- 5.1.2. The software solution shall have admin portal with functionalities like ability to configure/Addition/Deletion/Modification/Updation of Users and different types of Inspections/Audits and to configure general purpose work flow. It should be capable to handle the deviations and exceptions in the work flow. All event should have audit trail.
- 5.1.3. Provision for addition/deletion of menu according to role mapping of user to be provided in front end to Super Admin. The system provides a variety of layout options enabling the Super Admin to alter the user interface.
- 5.1.4. Record or field level formulas or calculations should be easily changeable/configurable by the Super Admin without assistance of the OEM/SI or professional services.
- 5.1.5. The solution shall support all the APIs required for collecting/verifying the particulars of the required data or integrate with Bank's APIs wherever the same is available. System should ensure that only authorized application can invoke such APIs.
- 5.1.6. Package shall have the capability to integrate with CBS, LAPS, Data Warehouse, Power BI,DMS,SMS Gateway,Email Gateway,Active directory ,Biometric API, various modules of SAS and other packages to extract data for processing, wherever required. Availability of the Middleware required for integration to be ensured by the bidder and ensure seamless integrations.
- 5.1.7. User Management in audit software should integrate with HRM software of the Bank. Implement role based access control (RBCA) mechanism to assign access rights and permissions based on role mapping as defined in the Bank's HRM system.
- 5.1.8. To trigger emails to various stakeholders of the audit package, proposed package should have functionality to integrate with our Bank's email server.
- 5.1.9. Package shall have the capability to integrate with the existing "DARPAN" package(existing audit package) for Inspection/Audit reference and archival of the data.
- 5.1.10. Package shall be capable of uploading documents/evidences as per bank requirement.
- 5.1.11. Checklist management for different types of Inspections/Audits as per bank requirement from time to time.



- 5.1.12. The proposed package should support Oracle database preferably or a compatible database. All necessary support related to DBs should be provided by the bidder. Bidder should provide all the necessary software/s to make the system live as per Bank's requirement.
- 5.1.13. System should support future integration of other applications as per Bank's discretion and as per need in future to efficiently carry out the inspection task.
- 5.1.14. The package shall provide configurable, on demand, real time reports and Dash boards showing the current status of the Inspections/Audits, user logs, exceptions etc. as per bank requirement.
- 5.1.15. The services shall be provided in "On Premises Model". Bidder should be able to provide the solution fully or partially on On-Premises as per Banks discretion. In case of conversion to any model, the same should be done at no extra cost.
- 5.1.16. The system should have proper Business Continuity Plan. As part of BCP, the system should have a DC/DRC set up.
- 5.1.17. The system should be incremental to meet any additional requirement as per bank's discretion.
- 5.1.18. Ability to upload the Bank's prescribed list to the solution in the standard formats.
- 5.1.19. Solution should support multi-server deployment for scalability, high availability load balancing and fault-tolerance.
- 5.1.20. The solution shall provide detailed audit trail for each activity/task executed in the package.
- 5.2. Hardware :
- 5.2.1. Bidder will procure, install and configure the hardware on-premises exclusively without cloud-based solution.
- 5.2.2. Hardware sizing must be compatible to support audit software and database size. It will support 5,000 concurrent core users and 4,000 non-core users at present and future expansion if any.
- 5.2.3. Hardware sizing (CPU, Cache, RAM, Hard disk etc.) should be measurable and efficient to cater services for next five years. Hardware sizing shall consider usage of several modules in the software solution along with legacy data of archive period as per Bank's policy.
- CPU - Multicore processors with High clock speeds and supporting hyper-threading technology. (Preferred Manufacturer : Intel Xeon or AMD EPYC)
 - Memory (RAM) - Large RAM capacity with high bandwidth for multitasking and data processing.
 - Storage (Hard Disk) - SSD/HDD with high data access and low latency.

internal



iv. Network Interface - Ethernet adapters of high speed and reliable network connectivity support advance network protocols and VLAN tagging.

5.2.4. Hardware will be deployed at both Data Center (DC) and Disaster Recovery (DR) sites with similar specifications and capacity. UAT server should be deployed by bidder for testing.

5.2.5. Installation of Hardware by the bidder must be operational within the Data Center environment of Bank by supporting permitted temperature and humidity level.

5.2.6. Hardware level security features such as Trusted Platform Module (TPM) for secure boot and data encryption. Integration with enterprise grade firewall solutions for network security to be ensured.

5.2.7. Throughput rates, Disk I/O Operations Per Second (IOPS) and Maximum Response Time for server must align with the software complexity and architecture.

5.3. Onsite/Offsite resources

5.3.1. The selected bidder should provide dedicated onsite / offsite resources. Bank reserve the right to claim change in the resource based on the performance of the resource.

5.3.2. The On-site resource will also be responsible for complete day-to-day activities such as end to end management including attending complaints, product related issues or any other issues etc., to the Bank as per SOW/SLA at no extra cost during contract period.

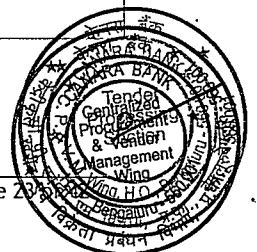
5.3.3. In case the resources go on leave/absent, replacements having equivalent or more experience and qualification has to be arranged by the selected bidder to ensure that regular functioning of the solution without any disruptions.

5.3.4. The onsite resources should be available on all the banking working days.

5.3.5. The Skill Set for the Resources shall be as follows:

Resource Type	Educational Qualification, Knowledge & Experience and Certification (if applicable)	Years of Experience
1 Nos of Onsite Resources (L1) 1 Nos of Onsite Resources (L2)	Graduate in Engineering/B.E./B-Tech/MCA or equivalent or higher qualification. Experience and knowledge: Should have prior experience in the proposed Solution. a. The resource must have adequate knowledge of the proposed platform. b. Basic understanding of banking domain and the financial services industry is essential.	2+ Years for L1 3+ year for L2

Internal



	<ul style="list-style-type: none"> c. Ability to work with databases, design schema, and use SQL to query data. d. Knowledge of security principles and best practices for designing and implementing the proposed Solution. e. Ability to create clear and concise documentation for the proposed Solution. f. Ability to communicate effectively with cross-functional teams & stakeholders. g. Ability to troubleshoot issues and identify solutions for technical problems h. L2 resource should be able to bug fixing, all config changes. 	
--	---	--

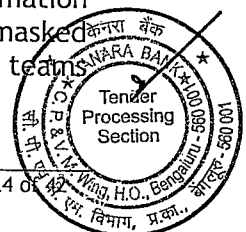
5.4. Regulatory Compliance:

- 5.4.1. The solution provided by the bidder should abide to the security requirements of the RBI, Government/other regulatory agencies and the Bank. Data security should not be compromised at any cost.
- 5.4.2. The bidder to assist the bank in adhering to compliance guidelines of the regulatory authorities and facilitate Bank from time to time.
- 5.4.3. The bidder should ensure that all the regulations of Information Technology Act, 2000, Information Technology (Amendments) Act, 2008 etc. apart from other applicable laws, as amended from time to time, are adhered to.
- 5.4.4. The bidder should provide the parameters to audit the solution by outside external auditors (for security) and any vulnerability observed shall be rectified by the bidder without any additional cost to the Bank. Points observed to be addressed without any additional cost.

5.5. Security Aspects

- 5.5.1. The entire process should be secure and end to end encrypted. All critical data should be encrypted at rest and in transit.
- 5.5.2. Solution should provide administrative portals with strong authentication and authorization mechanism and should provide secured Role Based Access Control (RBAC) modules.
- 5.5.3. The confidentiality of the customer's data must be ensured and the data must be protected and not be stored anywhere outside the Bank's infrastructure.
- 5.5.4. The solution must undergo software and security audit as per stipulations and all remarks/observations in the audit reports to be rectified/incorporated.
- 5.5.5. Bank reserves the right to conduct audits on the system provided by the bidder. Bidder to provide necessary arrangement and access control for the Bank.
- 5.5.6. The bidder should ensure that the Personally Identifiable Information (PII) is encrypted /masked, and all such PII should be masked accordingly in-line with access control mechanisms (for vendor teams

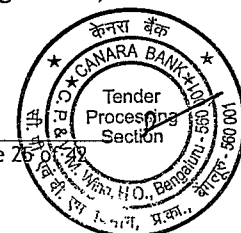
Internal



including Support Engineers L1, L2, L3) as specified by the bank. Should ensure PII data masking and isolation as per Bank's security standards/policies and other regulatory standards.

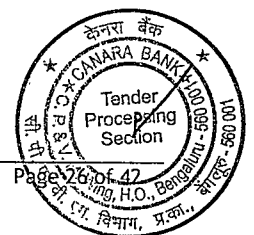
- 5.5.7. Application should have safeguards to protect itself from all injection based attacks or Command Injection Attacks.
 - 5.5.8. Application should have safeguards to protect itself from cross-site-scripting(XSS) attacks, CSRF (Cross site request forgery) attacks etc.
 - 5.5.9. Application should restrict upload to specific types of files extensions, file size and content type. File scan must be available before uploading any file in proposed solution.
 - 5.5.10. Application should demonstrate sufficient protection against redirection flaws, click jacking etc.
 - 5.5.11. Application makes use of available security protocols (e.g. HTTPS, SFTP/FTPS, LDAPS, SSH etc.) to protect sensitive data during transmission over private and public networks, if need be for future anticipation.
 - 5.5.12. Application should use encryption (or equivalent controls such as hashing) to ensure the confidentiality and integrity of user password in storage (usage of encryption technologies that have been thoroughly and publicly tested).
 - 5.5.13. Application should implement counter measures to protect against data leakage from side channels such as Web caches, Keystroke logging etc.
 - 5.5.14. It shall support security related features for taking the control of remote PCs, based on pre-defined policy and authorization.
- 5.6. Data integrity Management and Data Storage:
- 5.6.1. To share what compartmentalization techniques are employed to isolate Bank data from other customer's data, wherever applicable.
 - 5.6.2. To comply with data retention and destruction schedules/Policy provided by Bank, bidder to certify on Bank's request destroying all data at all locations including stack in data structures and on the media, wherever applicable. The Bank will have the right to audit this practice.
 - 5.6.3. Perform regular backup and recovery tests to assure that logical segregation of duties.
 - 5.6.4. To provide forensic Investigation Support (logs and audit trails) as and when required by Bank.
 - 5.6.5. To comply with Bank's RTO/RPO requirement and retention policy.
 - 5.6.6. In case of hybrid based solution customer sensitive information/PII information as well as Bank's data will not be saved or transferred.
 - 5.6.7. Solution should ensure that the log collection, storage, management, integrations are done in a secured and tamper proof manner.

Internal



- 5.6.8. The Bidder should not store or share any data outside the Bank's infrastructure.
- 5.6.9. Store transactional/alert/reports data securely in a centralized data repository.
- 5.6.10. Implement appropriate access controls and encryption mechanisms to safeguard sensitive data.
- 5.7. **Data Integration & collection:**
- 5.7.1. The solution should provide seamless integration with other software solutions through API support. Proposed solution must provide APIs for other applications used by various department of bank.
- 5.7.2. Bidder should be able to integrate with any third-party solution for performance monitoring of the proposed solution selected by the Bank at no additional cost to Bank.
- 5.8. **Work flow management**
- 5.8.1. Proposed solution should support Low-code No-code platform, which provides pre-built components that can be assembled to create functional applications and empowers the admin users to quickly and easily customize proposed solution as per various requirements or work flow.
- 5.8.2. Regularly review and update rule sets, checklist, scenarios, and models based on emerging risks and regulatory changes, wherever applicable.
- 5.8.3. Environment to perform regular testing and validation to assess the effectiveness of the monitoring system and incorporate any corrective measures to mitigate the same.
- 5.9. **User interface**
- 5.9.1. User friendly and customizable interface with access rights and modules based on User, Office etc.
- 5.9.2. Integration to Bank's Single Authentication System(SAS) for enabling User access and Biometric login solution.
- 5.9.3. All the components of the application should have the ability to be reused and replaced without affecting the rest of the system fostering ability, efficiency and resilience.
- 5.9.4. The Application should work in all major browsers like Google Chrome, Microsoft Edge and any other application as decided by the Bank.
- 5.9.5. Proposed solution must provide native mobile app for android and iOS.

Internal



5.10. Scalability:

- 5.10.1. Performance testing to be ensured.
- 5.10.2. Bidder to be in line with the racking and stacking of the physical IT infrastructure served by our Bank.
- 5.10.3. Visualized load balancer- should have complete virtual infrastructure to support.
- 5.10.4. Stage wise addition of new modules as per the Bank's requirement from time to time. It should not hamper the functioning of existing modules.
- 5.10.5. Proper training and support to the users.
- 5.10.6. To define the procedures for Patch Management, Centralized application Distribution including upgrades / Rollback / New Deployment etc. to all the distributed desktops, centralized Hardware / Software Inventory monitoring / Asset Intelligence, Remote Troubleshooting.

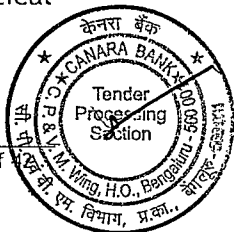
5.11. MIS & Analytics/Reporting & Documentation:

- 5.11.1. The Solution package to provide a console to view summary and detailed report/MIS of activities occurred. Bidder should be able to generate customizable report as per Bank's requirement which should be downloadable and exportable.
- 5.11.2. The solution/package to cooperate with our Bank's BA&IS vertical to automate the package for reducing TAT and hence efficiently use manpower.
- 5.11.3. Generation of error free reports for submission to regulatory authorities as per prescribed reporting formats and any other future revisions.
- 5.11.4. Maintenance of record of submitted reports, generation of customizable reports/dashboards for Decision making/Audit/Internal reporting purposes. Adaptability to changing regulatory requirements. Solution to include various reports in figures as well as graphical representation.
- 5.11.5. The solution should provide seamless integration with BD360, MIS, HRMS, CBS and other applications as per the Bank's requirement from time to time.
- 5.11.6. Tools and technique for handling high end data and big data to be incorporated in the audit software solution and support to be provided for addressing the technical issue to both high end data and big data.

5.12. Data Analysis:

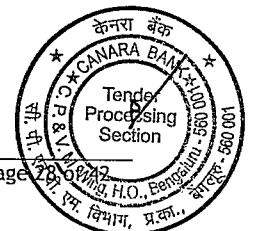
- 5.12.1. Automated analytical data analysis: The package shall leverage advance analytics to identify gaps in process controls and compliances based on the data available in electronic form.
- 5.12.2. Analytical analysis will be purely based on the predefined analytical checks /rules. The analysis shall give direct results /observations.

Internal



- 5.12.3. Facilitate analysis by Scrutiny of Audit data which will include results of analytical analysis and support documents uploaded by Auditee units.
- 5.13. **DRP/BCP/IRP (Disaster Recovery Plan, Business continuity Plan, Incident Response Plan)**
- 5.13.1. DR related documentation to be provided (Disaster Recovery Plan, Disaster Recovery Procedure, Disaster Recovery Test Plan).
- 5.13.2. Technical support to be provided by the bidder during DR drill activity of Bank.
- 5.13.3. Package is expected to have uptime of min 99.50% (excluding downtime explicitly not attributed only to vendor's fault) where penalty will be deducted for downtime of the system (Application failure).
- 5.13.4. Bidder to ensure that at no point of time hardware parameters like Memory, CPU utilization, etc. will cross the industry standards.
- 5.13.5. Robust data backup, recovery and storability procedures with offsite and onsite backup.
- 5.13.6. Incident response plan to be prepared with fixed TAT. (Turnaround Time)
6. **Deliverable:**
- 6.1. **Supply and Deployment of Hardware:** Procurement of server and other hardware appliances as per Bank specifications to be carried out to support the proposed audit software. Server to be installed by the bidder with help of DCM group, DIT Wing, HO. Bidder shall offer comprehensive warranty coverage and service level agreements to ensure timely resolution of hardware issues.
- 6.2. **Software Installation:** Seamless installation and configuration of the audit software package in accordance with organizational requirements and specifications.
- 6.3. **Documentation:** Provision of comprehensive technical documentation, Module wise SRS (Software Requirement Specification), manuals, and training materials to support implementation, operation, and maintenance activities.
- 6.4. **Support Services:** Provision of ongoing technical support, troubleshooting assistance, and software maintenance services to address any issues or concerns that may arise during and after the software ported in Live environment.
- 6.5. **Customization:** Customizing the software solution to meet specific organizational requirements by enhancing the usability and flexibility.
- 6.6. **Integration:** Integrating it seamlessly with existing systems, workflows and legacy audit reports.
- 6.7. **Data Migration:** Bidder should assist in migrating data from legacy systems or existing audit software to the new platform. Data migration services should be conducted efficiently and accurately, ensuring data integrity, consistency and compliance with regulatory requirements.

Internal

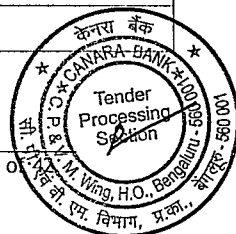


- 6.8. **Quality Assurance:** The vendor should conduct thorough quality assurance testing to validate the functionality, performance, and reliability of the audit software. This includes conducting regression testing, usability testing and security testing to identify and rectify any defects or issues prior to deployment.
- 6.9. **OEM Participation:** The bidder must guarantee the active participation of the Original Equipment Manufacturer (OEM) till the audit software is successfully deployed in the Live environment. This involve support for hardware integration, optimization and troubleshooting to major issues encountered in the software solution.

7. Compliance for Hardware to be ensured:

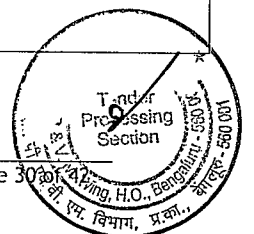
Sl. No.	Evaluation for Scope of Work for this project	Compliance (Yes/No)
1.	All necessary entitlements e.g. paper licenses/Key etc. for both hardware and software should be provided to the Bank.	
2.	The proposed bidder will need to ensure support of product & change of components @ zero cost in case of any part becoming obsolete/EOL & EOS during the warranty and AMC period	
3.	The bidder has to provide AMC/ATS for the all supplied Hardware and Software as per the Scope of Work post warranty period. During the warranty period and AMC period, the Bidder is bound to do all hardware spares replacement and upgrade/update of proposed hardware to next or required version without extra cost to the Bank covering all parts & labour from the date of acceptance of the systems by the Bank at the respective locations i.e. on-site comprehensive warranty. The Bank, however, reserves the right to enter into Annual Maintenance Contract (AMC) agreement either location-wise or from a single centralized location.	
4.	All supplied Hardware should have redundant Power Supply and necessary cables and Rack mounting Kit.	
5.	The warranty for the proposed hardware will start on the date when the operating system and any other provided software are installed, as mentioned in the Scope of Work for the specific hardware.	
6.	Bidder has to coordinate with Bank System Integrator while implementing the solution and during any point of time when ever issue is raised by the Bank.	
7.	Bidder should keep the Bank explicitly informed about the end of support dates on related products/ hardware and should ensure support during warranty & AMC period.	
8.	The Bidder should note that servers and other items being procured shall be delivered at locations as per requirements of the Bank.	
9.	The Configuration as per the technical and other specifications offered of all equipment & other items must be functional and installed from the day one.	
10.	All necessary cables and other accessories required for successful installation of the hardware items as per the scope of work to be supplied by the Bidder and the cost of the same to be added along with the respective Hardware items while quoting.	
11.	Bidder should follow a standard development process to ensure that proposed servers meets functional, security performance and regulatory requirements of the bank.	
12.	Bidder should comply as per the IT related policies of the bank.	

Final



13.	Bidder is responsible in installing the Hardware, Software and other items as per Technical Specifications and Scope of work in the bank environment. And as per the bank secure configuration documents	
14.	Bidder must generate and provide a complete holistic report before handover to ensure 100% serviceability of delivered hardware.	
15.	Bidder is responsible for collection of logs and submission of the logs for further analysis and providing the solution to resolve any hardware incidents.	
16.	Bidder must engage Bidder professional team/services onsite to implement/install Hardware, Software & other items.	
17.	Bidder is responsible to inform if any new version/update/Service pack/firmware/code upgrade/upgrade of proposed hardware is available by OEM, to the bank within seven days (7 days) of the release and provide the upgrade solution (software) within one month of such releases without any cost to the bank during the period of contract.	
18.	If any more additional licenses are procured by the bank through the successful bidder all such licenses are to be maintained by the bidder.	
19.	Bidder has to provide the escalation matrix to escalate any incident.	
20.	Bidder is responsible to provide the periodic reports of the proposed hardware health as per the bank requirement.	
21.	All installed hardware firmware must be of stable version and all recommended patches should be installed by the bidder and the same to be submitted to the bank on quarterly basis.	
22.	Bidder shall conduct preventive maintenance as may be necessary from time to time to ensure that equipment is in efficient running condition so as to ensure trouble free functioning.	
23.	All the connectivity for the hardware i.e. LAN and SAN switches need to be ensured by the bidder.	
24.	All proposed equipment's are required to connect existing SAN infrastructure.	
25.	The proposed hardware should be free from any kind of vulnerabilities.	
26.	Bidder should keep the bank explicitly informed the end of support dates on the related products/Hardware and should ensure a support during the warranty and AMC period.	
27.	Bidder must also provide the necessary power cables, LAN cables, FC cables from source to their provided rack as per the guideline of the Bank.	
28.	The Selected Bidder has to coordinate with existing vendor for the SAN cable lay, connectivity and Zoning of the SAN ports as required connecting the Proposed Hardware and Software.	
29.	Bidder support should include advice and help the bank in implementing controls for the risk advised by regulators/Govt. of India.	
30.	For delivery location, the Bidder has to provide items with the related hardware, all subsystems, operating systems, system software, software drivers and manuals etc.	
31.	The Bidder should note that Servers & Other Items being procured shall be delivered at locations as per requirements of bank and the Bidder will be required to support all such installations. The Bank reserves the right to change location by giving prior notice.	
32.	The Hardware and Software installation and configuration for the entire set up to be handled by the qualified/experienced personnel only.	

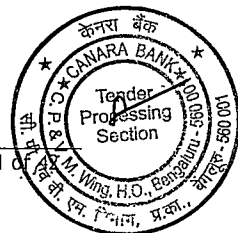
Internal





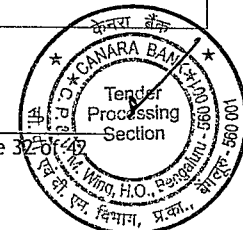
33.	During installation if the bank requires any new Software/OS/Utility, Bidder has to install without any cost where the licenses of the software are with the Bank.	
34.	The Bidder shall conform the integrity of the software supplied i.e. the software is free from bugs, malware, covert channels in code etc.	
35.	Bank will not provide any remote session like Team Viewer, WebEx etc. for any kind of installation, bug fixing, update and upgrade in entire project tenure.	
36.	The bidder should provide email, telephonic and onsite support.	
37.	The proposed server network interfaces ports should be compatible for connecting bank CISCO switches.	
38.	The proposed server FC HBA interface ports should be compatible for existing SAN Switch.	
39.	All hardware delivered to be rack mounted, powered on and configured properly including tape drive, tape library , server rack with PDU,TOR Switch etc., supplied as part of this RFP	
40.	All the devices supplied as part of this project should be accommodated in one rack space	
41.	<p><u>RACK DETAIL at DC SITE</u> Server rack mount power distribution unit 1Ph,230V,63A 50/60Hz with redundancy. 42 U Rack Frame with all necessary side panels, and rack size should be 600 mm*1200mm *2100mm (600mm - Width , 1200mm Depth , 2100mm Height) Mechanical lock with key for both front and back door Zero U standard with minimum 20 x C13 (20 power sockets with C13 type) and minimum 4 x C19 (4 power socket with C19 type) Per PDU Dual PDU should be made available for each rack PDU rating approximate 14KVA per PDU for single phase with 63A (4 MCB) Minimum 3 Meters IEC 309 input plug top Copper based Electrical Grounding / Earthing Strip</p>	
42.	Day to day activities like backup, monitor the infra, Patching, Firmware upgrades, configuration audit, server and storage hardening, OS hardening, application hardening, VAPT,Troubleshooting technical issues to be attended by the onsite team.	
43.	<p><u>RACK DETAIL at DRC SITE</u> Server rack mount power distribution unit 3Ph,230V,32A 50/60Hz with redundancy. 45 U Rack Frame with all necessary side panels 600 mm*1200mm (600mm - Width, 1200mm Depth) Mechanical lock with key for both front and back door Zero U standard with minimum 20 x C13 (20 power sockets with C13 type) and minimum 4 x C19 (4 power socket with C19 type) Per PDU. Dual PDU should be available for each rack. 16A MCB X 2 circuits - PDU rating approximate 8KVA Minimum 3 Meters IEC 309 input plug top Copper based Electrical Grounding / Earthing Strip</p>	
44.	Bidder should coordinate with our bank/SI team to integrate the supplied devices to SIEM/PIM/AV/backup solutions/DAM etc.,	
45.	Required power, fiber and network cables to be supplied along with the project	

M.C. 11



46.	Required TOR switch to be supplied as part of this project	
47.	Bidder should supply the backup and AV license required for the project	
48.	The Bidder will responsible for the following:	
a	Delivery of proposed hardware to Bank locations specified in BID.	
b	Safely Unpacking of shipped boxes at staging area.	
c	Physical movement of supplied hardware from staging area to Server Farm.	
d	Identification and labelling of hardware assets as per delivery invoices.	
e	Rack assembling, installation and power connectivity from industrial sockets and testing of required power rating.	
f	Mounting of servers, storages and network switches to server rack as per industry best practices.	
g	Server power on and cable dressing.	
h	Server Management connectivity.	
i	LAN and SAN Cable lay with proper labelling, tagging and cable dressing.	
j	Configuration of RAID as per requirement of bank in supplied Servers and storages	
k	SAN connectivity to bank existing SAN Switch	
l	LAN connectivity to bank existing network switch	
m	All activities related to Storage Administration assigned during the implementation period and till the project tenure (Warranty and AMC/ATS, if contracted) without any extra cost.	
Sl. No.	Evaluation for Scope of Work for Servers	Compliance Yes/No
1	Bidder has to install / re-install the operating system (if required), other software in the serves and support the same during warranty and AMC period without any extra cost to the Bank.	
2	Deployment of servers requires co-ordination with different project application vendors. The bidder should co-ordinate with the software vendors while installing and ensure installation and commissioning for running the applications for which these servers are procured.	
3	The Bidder should setup the partition as required by the Bank. The details of the setup will be provided during the setup to the successful bidder.	
4	The proposed hardware should be compatible with red hat Linux 8/9 or later and Windows 2016/2019/2022 and VMware hypervisor 7.X/8.x or later and Microsoft Hypervisor 2019 or later	
5	Hardening of the servers as per the bank secure configuration document based on the OS, Hypervisor and hardware flavours	
Sl. No.	Evaluation for Scope of Work for Storages	Compliance Yes/No
1	The proposed bidder needs to configure/implement the Storage as per the BANK policy. Need to provide the SOP with step-by-step procedure to BANK technical personnel. Need to provide document for each feature how to use/configure/admin it.	
2	Install & configure storage hardware and software components	

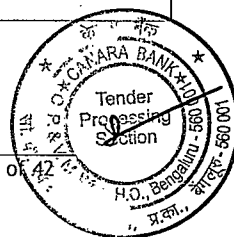
Internal



3	Integrate storage systems with existing infrastructure including servers, networks, and backup solutions	
4	Showcase the Monitor storage performance metrics including throughput, latency, and IOPS.	
5	Identify performance bottlenecks and implement optimization strategies such as load balancing, caching, or tiering.	
6	Tune storage configurations and parameters to maximize efficiency and responsiveness.	
7	Design and implement data protection strategies including backup, replication, and snapshotting.	
8	Implement security controls to protect sensitive data and prevent unauthorized access.	
9	Configure access controls, encryption, and authentication mechanisms according to industry best practices and regulatory requirements.	
10	Showcase Generate regular reports on storage capacity, utilization trends, and performance metrics as per bank requirement	
11	documentation on storage configurations, procedures, and troubleshooting guidelines.	
12	performing code upgrade on quarterly basis.	
Sl. No.	Evaluation for Scope of Work for Database	Compliance (Yes/No)
1	Installation and Configuration: Set up database servers and configure settings to ensure optimal performance and security.	
2	Security Management: Implement and maintain robust security measures to protect sensitive data from unauthorized access during the initial setup	
3	Disaster Recovery: DR Setup creation and replication to be configured	
4	Install and configure the Database as per banks security configuration document	
5	Setting up Server High Availability: Failover Cluster Instances as per requirement at DC and DRC sites	
6	Documentation: Maintain detailed documentation of database configurations, architectures, and best practices.	
7	Vendor Liaison: Work with vendors to resolve issues related to database products and services during the initial setup creation	
8	Documentation & Handover: Preparing the implementation and configuration handover documentation and providing handholding to our onsite team	

Technical Details	Technical Specification for servers & storages and other Hardware	Bidder's Compliance (Yes/No)
-------------------	---	------------------------------

Internal



Sl. No.	Technical Factor	Description	
1	Make	Bidder to specify	
2	Model	Bidder to specify	
3	Power Factor	Bidder to specify	
4	Form Factor	1U / 2U	

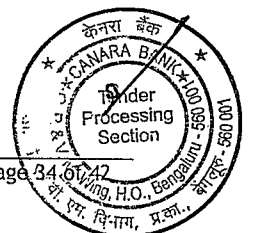
Note: The document outlines the project's scope broadly and is not exhaustive. Detailed functionality will be specified post RFP. All functionalities and any other modifications for the entire project will be included without any additional cost.

We hereby comply with the above Scope of Work without any deviations.

Date:
Place:

Signature with seal
Name:
Designation:

Canara



Annexure-3
Bidder's Profile

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

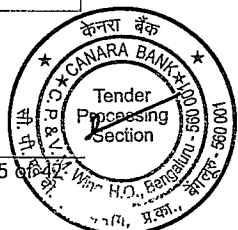
SUB: Selection of Vendor for end to end implementation of Audit Solution in Bank for a Period of 5 Years

Ref: GEM/2024/B/4988346 dated 28/05/2024.

Sl. No.	Particulars	Details
1)	Name of the Bidder Firm/ Company	
2)	Constitution (Ltd./Pvt. Ltd./ Firm etc.)	
3)	Date of Incorporation and / or Commencement of business with supporting documents	
4)	Certificate of Incorporation Number (CIN)	
5)	Proposed Audit Solution	
6)	Whether registered as MSE for the item under the RFP? (Proof of registration as MSE for the item under the RFP)	
7)	Whether recognized as a Startup by Department of Industrial Policy and Promotion (DIPP)? (Proof of such recognition, indicating terminal validity date of registration and Certificate from CA that the Turnover of the entity complies with Startup guidelines)	
8)	Address for Correspondence: Registered Office: Corporate Office:	
9)	Single Point of contact for this RFP Name: Designation: Mobile No.: Landline No.: Fax: Email-ID (any changes in the above should be informed in advance to Bank)	
10)	PAN number GSTIN <u>Beneficiary Bank Details</u> Beneficiary Name Beneficiary Account Number Type of Account (OD/OCC etc.) IFSC Name of the Bank and Branch address	

Wherever applicable submit documentary evidence to facilitate verification.

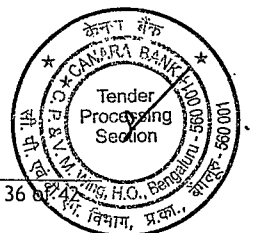
Internal



We hereby declare that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our Bid is liable to be rejected.

Date:
Place:

Signature with seal
Name:
Designation:



Annexure-2

Pre-Qualification Criteria

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of Vendor for end to end implementation of Audit Solution in Bank for a Period of 5 Years

Ref: GEM/2024/B/4988346 dated 28/05/2024.

We have carefully gone through the contents of the above referred RFP along with replies to prebid queries & amendment, if any and furnish the following information relating to Pre-Qualification Criteria.

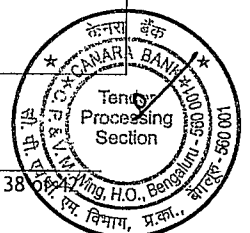
Sl. No.	Pre-Qualification Criteria	Documents to be submitted In compliance with Pre-Qualification Criteria	Bidders Response
1.	Signing of Pre-Contract Integrity Pact	The bidder should submit signed Pre Contract integrity pact on Non Judicial Stamp Paper of Rs.500/- or more (as per respective state Stamp Act) as per Appendix-F.	
2.	The bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020.	Certificate of local content to be submitted as per Annexure-5 as applicable.	
3.	The bidder should provide confirmation that any person/ Partnership/ LLP/ Company including any subsidiary or holding company/ proprietorship connected to bidder directly or indirectly has not participated in the bid process.	The bidder should submit letter of confirmation on the Company's letter head to this effect.	
4.	The Bidder should be a partnership firm registered under LLP Act, 2008/Indian Partnership Act, 1932 or Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 in operation at least of 3 years	Copy of Certificate of LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company (OR) Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.	
5.	The bidder/OEM should have implemented and maintaining Audit Solution in any Scheduled Commercial Banks in India during the last 3 years as on RFP date.	The bidder/OEM should submit purchase Order and satisfactory letter/reference letter from the customer duly mentioning the details of the solution.	

inter val



6.	The firm should have a pool of at least 15 professionals on payroll who have experience in Information Technology, Development of Software/Application for at least 2 turnkey projects for BFSI during the last three years (i.e. 2020-21 and 2021-22 and 2022-23).	Bidder to submit details in the company's letter head confirming that they are on payroll along with the profile of the professionals and copies of the relevant certificates.	
7.	Any bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India 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.	A declaration stating "We have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be submitted in Company's letter head. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]	
8.	Bidder should be the Original Equipment Manufacturer (OEM)/ Original Software Owner (OSO)/ Original Software Developer (OSD) of Solution. (OR) An authorized dealer/distributor of the proposed Solution	If the applicant is OSD/OSO, an Undertaking Letter has to submit in this effect. (OR) If the bidder is an authorized dealer/ distributor, an authorization letter from their OEM and OSO/ OSD to deal/market their product in India and it should be valid for entire contract period from the date of submission of the bid.	
9.	The bidder should have an average annual turnover of Rs.150 Crores during last 3 financial years (i.e., 2020-21, 2021-22 & 2022-23) from Indian operations. This must be the	Bidder should submit Audited Balance Sheet copies for last 3 financial years i.e., 2020-21, 2021-22 & 2022-23 along with certificate from the Company's	

Internal



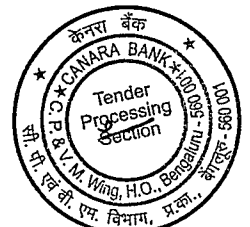


	individual company turnover and not of any group of companies.	Chartered Accountant to this effect with Unique Document Identification Number.	
10.	The bidder should have positive Net Worth as on 31/03/2023 and also should have not been eroded more than 30% in the last three financial years ending on 31/03/2023.	The bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect.	
11.	Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments on the date of submission of bid for this RFP.	The bidder should submit self-declaration on the Company's letter head to this effect.	
12.	The bidder should have support office in Bengaluru or Mumbai for 24x7 supports.	The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc.,	
13.	Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Power of Attorney or the Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection. All documentary evidence / certificates confirming compliance to Pre-Qualification Criteria should be part of the RFP.

Date:
Place:

Signature with seal
Name:
Designation:



Internal

Annexure-10

Technical Evaluation Criteria

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

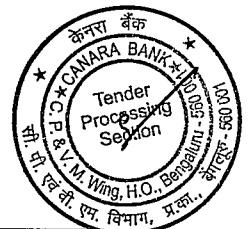
SUB: Selection of Vendor for end to end implementation of Audit Solution in Bank for a Period of 5 Years

Ref: GEM/2024/B/4988346 dated 28/05/2024.

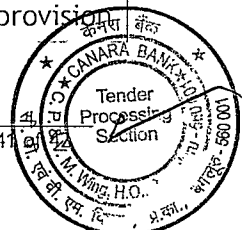
The technical evaluation of the bidder will be carried as per the details furnished below:

Sl. No.	Evaluation Parameters	Scoring Parameters	Max marks	Documents to be submitted
1.	<p>Capability: Implementation of Audit related Solution by the Bidder.</p> <p>The bidder should have implemented any Audit related Solution in any Scheduled Commercial Banks.</p>	<p>Number of Implementation:</p> <ul style="list-style-type: none"> 2 or more implementations - 10 marks 1 implementation - 5 marks 	10	The bidder should submit purchase Order/Contract Agreement along with satisfactory performance letter/reference letter from the customer duly mentioning the details of the solution.
2.	<p>The proposed audit solution/product should have been successfully implemented/used in any Scheduled Commercial Bank.</p>	<p>Number of Years:</p> <ul style="list-style-type: none"> 3 or more years - 10 marks 1 to 3 years - 5 marks 	10	Satisfactory performance letter/reference letter from the customer duly mentioning the details of the solution along with copy of purchase Order /Contract Agreement/ Work Order to this effect.
3.	<p>The Bidder/OEM must be recognized as a leader in the field of enterprise Audit - Risk and Operational Compliance.</p> <p>They must be at least in the Leader's Quadrant in any one of the report - Chartis, IDC, Gartner, Forrester for Risk Management Services</p>	<ul style="list-style-type: none"> If rated under leader quadrant or its equivalent - 15 Marks If rated in any other quadrant - 7 Marks 	15	Bidder to provide the related rating artifacts as documentary evidence

Internal



4.	The number of certified personnel employed by the Bidder on the proposed solution. (Note: Only those experiences will be counted which have duration of at least 1 year)	Number of employees: • For more than 20 employees -10 Marks • For 10 to 20 Employees - 5 Marks	10	Copy of relevant Certificate on the proposed Tool along with undertaking letter from HR.
5.	Bank's confidential analysis from existing users	5 Marks	5	Vendor to arrange for independent feedback from existing users of Audit solution
6.	Presentation by the Bidder: Note: The Presentation is as per the technical & functional requirement/scope of work/other terms as mentioned in RFP to the Bank.	Technical presentation will be evaluated on the following parameters: • IT architecture, Approach and Methodology (10 Marks) • Work plan and methodology covering complete scope of work (10 Marks) • Project Governance (5 Marks) • Security Aspects and Any Other features as per RFP Document. (5 Marks)	30	
7.	Out of the modules envisaged in scope of work, number of modules already available with the bidder/OEM.	Number of modules available • 2 or more modules already available - 10 Marks • 1 module available - 5 Marks	10	A satisfactory certificate from existing client/s or any other documentary evidence supporting implementation/availability of existing modules to be submitted by bidder/OEM. The same should be demonstrated during technical presentation.
8.	Feature of Low code - No code in existing solution.	• If Feature of Low code - No code is available and implemented with existing client - 10 Marks • If Feature of Low code - No code is available - 5 Marks	10	A satisfactory certificate from existing client/s or any other documentary evidence supporting availability of provision



	(Availability for Auto creation of work flow and user role mapping)		of Low code - No code to be submitted by bidder/OEM. The same should be demonstrated during technical presentation.
Total Marks		100	

Note: The bidder should score minimum 70% marks (i.e., 70 Marks out of 100 marks) total marks for qualifying under Technical Evaluation. The bidders qualified under Technical Proposal Evaluation will be eligible for commercial opening.

Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this RFP is liable for rejection.

Date:
Place:

Signature with seal
Name:
Designation:

