2012

Project Management Unit,
Board of Revenue,
Government of Sindh

FINANCIAL PROPOSAL

APRIL 12, 2012

Consultancy Services for Third Party Software Audit and Evaluation for LARMIS

Sidat Hyder Morshed Associates (Pvt) Ltd

Management Consultants

TABLE OF CONTENTS

I. PROJECT INTRODUCTION & BACKGROUND

Board of Revenue, Government of Sindh is entrusted with Enforcement and administration of Land Laws. Its functions include;

- Assessment and collection of Land Tax, development cess, surcharges, water rate and any other levy assigned by the Government.
- Maintenance of Record of Rights, tenure, tenancy and restrictions on title of properties.
- Conducting land surveys for land utilization.
- Registration of deeds, documents and collection of registration fee.
- Management of judicial and non-judicial stamps.
- Collection of court fee and stamp fee.
- Reassessment and settlement.

The Project Management Unit, Board of Revenue, Government of Sindh through its already approved PC-1 is in the process of automation of the functions of the Board of Revenue [BOR].

The project is aimed at establishing the 'Land Administration & Revenue Management Information System' – LARMIS. LARMIS involves;

- Revamping of the existing manual business processes of BOR through computerization of the land and property record and transactions taking place at BOR.
- Automation of the functions of Board of Revenue through development of customized software.
- Establishing better administrative controls, transparency and promotion of the culture of facilitation in public services.
- Establishing Facilitation Centers for one window operations for verification, registration, and mutation services for land and properties.
- Establishing 'Management Information System' containing all revenue record and transactions taking place at Board of Revenue.
- Generation of reports and information for effective public policy and optimization of revenue collection.
- Establishing 'Special Purpose Vehicle' – an entity in private sector owned by the Government of Sindh for management of the data base and providing services to the stake holders.

Under the project, customized software is being developed. PMU, BoR seeks reputed consultancy firms to conduct independent third party audit and evaluation of the software to be developed before completely rolling out the system.

Sidat Hyder Morshed Associates (Pvt.). Limited is pleased to submit this proposal for the providing consulting services for Third Party Software Audit and Evaluation for LARMIS.

II. PROJECT OBJECTIVES AND SCOPE OF SERVICES

A- Project Objectives

The objective of the third party Information System Audit (IS Audit) is to examine the controls within the proposed LARMIS through the process of collecting and evaluating evidence of organization's proposed LARMS information system, practices, and operations. Obtained evidence evaluation will ensure whether the organization's information system safeguard assets, maintains data integrity, and is operating effectively and efficiently to achieve the organization's goals or objectives.

The IS audit will focus on determining risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. The purpose of IS Audit is to review and evaluate organization's information system's availability, confidentiality, and integrity by answering the following questions:

1. Will the organization's computerized system be available for the business at all times when required? (Availability)
2. Will the information in the system be disclosed only to authorize users? (Confidentiality)
3. Will the information provided by the system always be accurate, reliable, and timely? (Integrity)
4. Overall security of the system (susceptibility to external/internal security threats)

B- Scope of Services

To achieve the overall objectives of the project, the IS Audit is envisioned to be performed in accordance with the following phases:

- Phase 1: Preliminary Review
- Phase 2: Audit Planning
- Phase 3: Risk Assessment and Business Process Analysis
- Phase 4: Performance of Audit Work
- Phase 5: Audit Reporting

Each phase is briefly described in the following paragraphs.

Phase 1: Preliminary Review

This phase of the IS Audit will allow the IS Auditor to set the scope and objectives of the relationship between the auditor and the PMU, BoR. The IS Audit engagement document will be reviewed and finalized to address the responsibility (scope, independence, deliverables), authority (right of access to information), and accountability (auditees' rights, agreed completion date) of the auditor.

During this phase of the audit, the IS Auditor will gather organizational information to form as a basis for creating their audit plan. The preliminary review will identify organization's strategy and responsibilities for managing and controlling computer applications. An in depth overview of organization's application system will be provided to the IS Auditor along with all relevant existing documents to establish which applications are significant at this phase. In order to plan the audit, a preliminary judgment about materiality and assessment of the business risks will be made to set the scope of the audit. Obtaining general data about the organization, identifying application areas, associated risks and controls will be outlined so that these are addressed in details in the audit plan phase.

Phase 2: Audit Planning

In this phase the IS Auditor will plan the details of the conduct of the audit and information system coverage to comply with the audit scope and objectives previously specified and agreed between the IS Auditor and the PMU, BoR and ensure compliance to all Laws and Professional Standards. The audit plan will document in details the purpose of the audit, the management responsibility, authority and accountability of the IS Audit to include the following:

1. Responsibility: define the mission, aims, goals and objectives of the Information System Audit. At this stage we also define the Key Performance Indicators and an Audit Evaluation process;
2. Authority: clearly specify the Authority assigned to the Information System Auditors with relation to the Risk Assessment work that will be carried out, right to access the information, the scope and/or limitations to the scope, the business functions to be audited and the auditee expectations; and
3. Accountability: clearly define reporting lines, appraisals, assessment of compliance and agreed actions.

In addition to the above, the IS Audit Plan will include a written representation from the PMU, BoR management acknowledging:

1. Their responsibility for the design and implementation of the Internal Control Systems affecting the application systems and processes.
2. Their willingness to disclose to the Information System Auditor their knowledge of irregularities and/or illegal acts affecting their organization pertaining to management and employees with significant roles within the internal audit department.
3. Their willingness to disclose to the IS Auditor the results of any risk assessment that a material misstatement may have occurred.

The audit plan will include in details:

- The IS Auditor's understanding of the organization.
- Potential audit risks.

- A basic framework for how the audit resources (budgeted audit hours) are to be allocated throughout the audit.
- Audit methodology and procedures to be performed.
- Audit reports to be produced.

The IS Audit Plan shall be agreed upon, approved and signed off by an appropriate level within PMU, BoR.

Phase 3 – Risk Assessment and Business Process Analysis

For the purpose of this proposed IS Audit, Risk is the possibility of an act or event occurring that would have an adverse effect on the organization and its information systems. Risk can also be the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. It is ordinarily measured by a combination of effect and likelihood of occurrence.

The following types of risks should be considered during this IS Audit:

Inherent Risk: Inherent risk is the susceptibility of an audit area to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls. In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls.

A pervasive IS Control are general controls which are designed to manage and monitor the IS environment and which therefore affect all IS-related activities. The IS Auditor will identify the applicable pervasive IS Controls which may include the following:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management
- Pressures on IS management which may predispose them to conceal or misstate information (e.g. large business-critical project over-runs, and hacker activity)
- The nature of the organization's business and systems (e.g., the plans for electronic commerce, the complexity of the systems, and the lack of integrated systems)
- Factors affecting the organization's industry as a whole (e.g., changes in technology, and IS staff availability)
- The level of third party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

A detailed IS control is a control over acquisition, implementation, delivery and support of IS systems and services. The IS auditor will identify, to the level appropriate for the audit area in question, detailed IS Controls which may include the following:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, and payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of the management and staff involved in applying the IS controls

Control Risk: Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume of logged information. The control risk associated with computerized data validation procedures is ordinarily low because the processes are consistently applied. The IS auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

Detection Risk: Detection risk is the risk that the IS Auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. In determining the level of substantive testing required, the IS auditor should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

Subsequent to the establishment of Risk Establishment, the IS Auditor will carry out the Business Process Analysis to include the following:

- Obtain an understanding of the Client Business Processes
- Map the Internal Control Environment
- Map the LARIMS Environment
- Identify areas of Control Weaknesses

Phase 4 – Performance of Audit Work

In the performance of Audit Work, the IS Auditor will provide supervision, gather audit evidence and document audit work. The objectives will be achieved through:

- Establishing an Internal Review Process where the work of one person is reviewed by another, preferably a more senior person.
- Obtain sufficient, reliable and relevant evidence to be obtained through Inspection, Observation, Inquiry, Confirmation and re-computation of calculations and activities.
- Document all work by describing audit work done and audit evidence gathered to support the auditors' findings.

At a minimum the following will be performed as part of the IS Audit Control Review:

General/Pervasive Control Review: Evaluate pervasive controls including the following:

- Review of IT Strategy and other Policy Documents
- Applicable Program Development Methodology
- System Implementation Methodology
- Business Continuity Planning and Disaster Recovery

Specific Controls Review: including the following:

- Application Control Review
    - Transactions
    - Controls
    - Environments
    - User Operations
    - Audit Trails
- Operating Systems Control Review
    - Vulnerability assessment of the installed Operating Systems
    - Review Access Controls within the OS
    - Review of System Capacity, Performance and Virus Controls
- Network Control Review
    - Attack on Pen testing
    - Review of Firewall and Intrusion Detection Systems
    - Review of Data Encryption Procedures and Security for both the Data held on Hosts and on the Network

- Review of Network Topologies, Internal Connectivity and Performance
- Review of External Connectivity and Websites
- Review of Penetration Test

For the purpose of this IS Audit, specific attention is to be given to the **Application Control Review.**

The envisioned Application Control Review will provide PMU, BoR management with reasonable assurance that transactions are processed as intended and the information from the system is accurate, complete and timely. An Application Controls review will check whether:

- Controls effectiveness and efficiency
- Applications Security
- Whether the application performs as expected

Review of the Application Controls will cover an evaluation of a transaction life cycle from Data origination, preparation, input, transmission, processing and output as follows:

1. Data Origination controls are controls established to prepare and authorize data to be entered into an application. The evaluation will involve a review of source document design and storage, User procedures and manuals, Special purpose forms, Transaction ID codes, Cross reference indices and Alternate documents where applicable. It will also involve a review of the authorization procedures and separation of duties in the data capture process.
2. Input preparation controls are controls relating to Transaction numbering, Batch serial numbering, Processing, Logs analysis and a review of transmittal and turnaround documents
3. Transmission controls involve batch proofing and balancing, Processing schedules, Review of Error messages, corrections monitoring and transaction security
4. Processing controls ensure the integrity of the data as it undergoes the processing phase including Relational Database Controls, Data Storage and Retrieval
5. Output controls procedures involve procedures relating to report distribution, reconciliation, output error processing, records retention. Ensures that computer output is not distributed or displayed to unauthorized users.

Phase 5: Reporting

Upon the performance of the audit test, the Information System Auditor is required to produce and appropriate report communicating the results of the IS Audit. The IS Audit report should:

1. Identify organization, intended recipients and any restrictions on circulation
2. State the scope, objectives, period of coverage, nature, timing and the extend of the audit work
3. State findings, conclusions, recommendations and any reservations, qualifications and limitations
4. Provide audit evidence

III. BID FORM

All commercial proposals must include a bid form signed by an individual legally authorized to bind the bidder to both its technical proposal and commercial proposal. Any exceptions to the Terms and Conditions stated in the Bidding Documents should be attached as an attachment to the Bid Form.

Note: As per the format given in the Request for Proposal (RFP), a Bid Form (containing two pages) on company letter head is attached here, duly signed by authorized representative and company seal.

IV. BID SECURITY

Note: As per the requirements given in the Request for Proposal (RFP), a Bid Security in the form of Bank Guarantee (containing one page) is attached here.

V. PRICE SCHEDULES

Firm price for services included in the total bid price to be provided as per the following template:

S. No.	Requirements	Quantity	Unit Price (PKR)	Total Price (PKR)
1	Submission of report on BOR organization structure, application areas along with associated risk & control	1 Job	299,000	299,000
2	Submission of audit plan (organizational & IS)	1 Job	299,000	299,000
3	Submission of "Risk Analysis Report"	1 Job	399,000	399,000
4	Submission of "Business Process Mapping" assessment report	1 Job	399,000	399,000
5	Submission of "Business Continuity Plan" assessment report	1 Job	199,000	199,000
6	Submission of assessment report on "IT Strategy & Policies"	1 Job	199,000	199,000
7	Submission of "System Audit Report" on LARMIS application	1 Job	1,799,000	1,799,000
8	Submission of assessment report on "System Data Security including Data Entry, Storage & Transport"	1 Job	399,000	399,000
9	Submission of assessment report on "System Implementation and Rollout Strategy"	1 Job	199,000	199,000
10	Submission of assessment report on network architecture and vulnerability assessment	1 Job	199,000	199,000
11	Project completion report	1 Job	499,000	499,000
			Total (PKR)	**4,889,000**
(Pak Rupees Four Millions Eight Hundred Eighty Nine Thousand Only – PKR 4,889,000/)				

VI. PAYMENT TERMS

The payment terms shall be as follows:

S. No.	Milestone	Timeline
1	Mobilization advance	20% of the total contract value to be paid at the signing of the contract against advance payment guarantee which would be adjusted within 6 months
2	Submission of report on BOR organization structure, application areas along with associated risk & control	5% of contract cost (mobilization will be adjusted accordingly)
3	Submission of audit plan (organizational & IS)	5% of contract cost (mobilization will be adjusted accordingly)
4	Submission of "Risk Analysis Report"	10% of contract cost (mobilization will be adjusted accordingly)
5	Submission of "Business Process Mapping" assessment report	
6	Submission of "Business Continuity Plan" assessment report	
7	Submission of assessment report on "IT Strategy & Policies"	
8	Submission of "System Audit Report" on LARMIS application	15% of contract cost (mobilization will be adjusted accordingly)
9	Submission of assessment report on "System Data Security including Data Entry, Storage & Transport"	10% of contract cost (mobilization will be adjusted accordingly)
10	Submission of assessment report on "System Implementation and Rollout Strategy"	10% of contract cost (mobilization will be adjusted accordingly)
11	Submission of assessment report on network architecture and vulnerability assessment	10% of contract cost (mobilization will be adjusted accordingly)
12	Project completion report	15% of contract cost (mobilization will be adjusted accordingly)

VII. RFP ADDENDA

RFP Addenda attached here (in the order as issued by the purchaser)