Expression of Interest
(EOI)

Title of Consulting Services: *Information System Audit, 2076*

Method of Consulting Service: National

Project Name: ***Nepal Rastra Bank(NRB) Information System Audit, 2076***
EOI: ***NRB/GSD/SOFTWARE/INFORMATION SYSTEM AUDIT/01/076/077***
Office Name: ***Nepal Rastra Bank(NRB)***
Office Address: ***Baluwatar, Kathmandu***
Issued on: 01.10.2076

Financing Agency: Internal Resources

Abbreviations

CV	-	Curriculum Vitae
DO	-	Development Partner
EA	-	Executive Agency
EOI	-	Expression of Interest
GON	-	Government of Nepal
PAN	-	Permanent Account Number
PPA	-	Public Procurement Act
PPR	-	Public Procurement Regulation
TOR	-	Terms of Reference
VAT	-	Value Added Tax

Contents

A. Request for Expression of Interest(EOI)

Nepal Rastra Bank
General Services Department
Baluwatar, Kathmandu, Nepal

Date: 2076.10.01
Name of Project: Nepal Rastra Bank Information System Audit, 2076

1. Nepal Rastra Bank has allocated fund ***toward the cost of Nepal Rastra Bank Information System Audit, 2076*** and intends to apply a portion of this ***fund*** to eligible payments under the Contract for which this Expression of Interest is invited for **National consulting service**.
2. The ***Nepal Rastra Bank*** now invites Expression of Interest (EOI) from eligible consulting firms ("consultant") to provide the following consulting services: ***Procurement of Consultancy Services for Information System Audit, 2076 of Nepal Rastra Bank .***
3. Interested eligible consultants may obtain further information and EOI document free of cost at the address ***General Services Department, Nepal Rastra Bank, Baluwatar, Kathmandu*** during office hours on or before **2076-10-15 12:00 Noon** or visit the client's website ***www.nrb.org.np***.
4. Consultants may associate with other consultants to enhance their qualifications.
5. Expressions of interest shall be delivered ***manually to the address***, ***General Services Department, Nepal Rastra Bank, Baluwatar, Kathmandu, gsd@nrb.org.np, +977-01-4419804/5(Ext 252,373)*** on or before ***2076.10.16 12:00 Noon*****.**
6. In case the last date of obtaining and submission of the EOI documents happens to be a holiday, the next working day will be deemed as the due date but the time will be the same as stipulated.
7. EOI will be assessed based on ***Qualification 50%, Experience 40%, and Capacity 10%*** of consulting firm and key personnel. Based on evaluation of EOI, only shortlisted firms will be invited to submit technical and financial proposal through a request for proposal.
8. Minimum score to pass the EOI is ***70.***

B. Instructions for submission of Expression of Interest

1. Expression of Interest may be submitted by a sole firm or a joint venture of consulting firms and the maximum number of partners in JV shall be limited to three.
2. Interested consultants must provide information indicating that they are qualified to perform the services *(descriptions, organization and employee and of the firm or company, description of assignments of similar nature completed in the last 7 years and their location, experience in similar conditions, general qualifications and the key personnel to be involved in the proposed assignment).*
3. This expression of interest is open to all eligible ***firm/company/organization*.**
4. In case, the applicant is individual consultant, details of similar assignment experience, their location in the previous 4 years and audited balance sheet and bio data shall be considered for evaluation.[1]
5. The assignment has been scheduled for a period of ***4 months.*** Expected date of commencement of the assignment is ***20-11-2076.***
6. A Consultant will be selected in accordance with the ***National*** method.
7. Expression of Interest should contain following information:
   (i) A covering letter addressed to the representative of the client on the official letter head of company duly signed by authorized signatory.
   (ii) Applicants shall provide the following information in the respective formats given in the EOI document:
      - *EOI Form: Letter of Application (Form 1)*
      - *EOI Form: Applicant's Information (Form 2)*
      - *EOI Form: Work Experience Details (Form 3(A), 3(B) & 3(C))*
      - *EOI Form: Capacity Details (Form 4)*
      - *EOI Form: Key Experts List (form 5).*
8. Applicants may submit additional information with their application but shortlisting will be based on the evaluation of information requested and included in the formats provided in the EOI document.
9. The Expression of Interest (EOI) document must be duly completed and submitted in sealed envelope and should be clearly marked as "EOI Application for Short-listing for the Nepal Rastra Bank Information System Audit, 2076. The Envelope should also clearly indicate the ***name and address of the Applicant***.
10. The completed EOI document must be submitted on or before the date and address mentioned in the **"*Request for Expression of Interest*".** In case the submission falls on public holiday the submission can be made on the next working day. Any EOI Document received after the closing time for submission of proposals shall not be considered for evaluation.

C. Objective of Consultancy Services or Brief TOR

TERMS OF REFERENCE FOR INFORMATION SYSTEM AUDIT

BACKGROUND

Nepal Rastra Bank (hereafter referred to as 'the Bank'), the Central Bank of Nepal was established in 1955 A.D. under Nepal Rastra Bank Act 1955, (replaced by Nepal Rastra Bank Act, 2002). The Bank is an apex institution in the financial sector of the country. It is an autonomous and corporate body, governed by its Board of Directors as mentioned in the Act. The Central Office is located at Baluwatar, Kathmandu. In addition to the central office, the Bank carries out its activities from various locations situated at Kathmandu and other principal cities of the country namely Biratnagar, Birgunj, Dhangadhi, Janakpur, Nepalgunj, Pokhara, Siddharthanagar and Surkhet. The main function of the Bank is to provide all central-banking activities including formulation and implementation of monetary policy, regulation and supervision of bank and financial institutions (BFIs). It is also responsible for the management of foreign exchange reserves, printing and issuing of currency notes. The Bank acts as a banker and advisor for the Government and other Government agencies.

The Information Technology is an essential and important part of the Bank's operation and internal control system. The system doesn't merely record business transactions, but actually drives the key business process and policies of the bank. In the present context, the bank has General Ledger System software (Olympic Banking System), HR Information System software, Online Bidding System software, Email system, Official website and other applications.

The bank has a separate Information Technology Department headed by a Director (IT). All of its IT systems, Data Center and DR sites are housed at the Bank premises at various locations.

The Bank plans to conduct Information System Audit of its existing IT system and infrastructure to get reasonable assurance that the operational and control objectives will be met; undesired events will be prevented or detected and rectified in a timely manner. Hence, this Request for Proposal (RFP) has been issued to Chartered Accountant firm either singly or in joint venture with other firm/company specialized in Information System Audit to do Information System Audit of the Bank's IT System and infrastructure. The purpose of this audit is to review and provide feedback, assurance and suggestions based on the audit conducted.

OBJECTIVES

The Bank believes that the Information System Audit is a part of the overall audit process, to ensure control maximization and risk mitigation. The objective of information system audit is to obtain reasonable assurance on confidentiality, integrity, availability of the Bank's information system. It seeks the status of overall IT security, identify control weakness and vulnerabilities in the IT environment and obtain recommendations and suggestions to mitigate such weakness and fraud if any. Other objectives of the audit are to verify the utilization of IT resources and provide suggestion on enhancing the efficiency; assess the status of information security education, information disclosure and grievance handling procedures. It also assess whether the issue related to data integrity and security are duly taken care of during the process and check compliance of IT security policy, guidelines, manual and procedures of the bank.

SCOPE OF WORK

The information system of the Bank has different functions and activities coupled with a number of computer and software installations at different geographical locations of the country. IS auditor is required to provide assurance on technology, infrastructure, application and associated internal control framework by assessing the computerized information system's functionality, efficiency and security through risk assessment, internal control evaluation and detailed testing of associated data.

The IS auditor is expected to adopt a risk-based approach for making audit plan. The auditor shall study the Bank's existing IT; and operation setups and perform IS audit as per internationally accepted standards on information system. The major elements of IS audit can be broadly classified:

a. Data Centre Facilities Audit:

To provide assurance on physical environment, building structure, power supply, power backups (UPS, Generators) access control at the data centre. It should further provide assurance on other data centre infrastructure such as network cabling, server/communication racks, power distribution units (PDU), KVM switches, Air Conditioner, Humidity Control System, Water Leak Detection, Suppression and Fire Fighting System. It should also cover the aspects of assets safeguarding, handling of movement of men, material, media, backup, software & hardware and surveillance systems.

b. IT Department Audit:

To review organizational structure for IT department, IT operation, information assurance within the departments and other related areas and evaluate the strength of employee to assess whether it is commensurate with the size, scale and nature of business activities carried out by the bank. The auditor shall assess the segregation of duty of IT operations periodic IT training requirement for IT personnel and performance monitoring & measuring system according to the IT functions of the Bank.

c. Operating System Audit:

To review various aspects of servers, database, network equipment, security system and storage area network such as operating system installed, its version, periodic patch management, set-up, configuration, maintenance of system parameters and change management, password management, user/group configurations, privilege account, log on/ log off process, generic share accounts, boot process, remote access, directories and files, logging/reporting/monitoring aspects of logical scalability, availability, evaluation of role, responsibility and accountability of IT process owners based on the principle of least privileged and "need to know" commensurate with the job responsibilities.

d. Application System Audit:

To provide assurance on the existing system/software of the bank; currently GL software (Olympic Banking Software) and other application software i.e. Online Bidding System Software, HR Management Information System Software, NRB Website, Email System and other systems including RTGS currently being used by the bank.

Further the audit would cover the following aspects of the application system:

- Functionality available and implemented vis-a-vis the Bank's requirements.
- Input, Processing and Output controls across various schemes of the Bank.
- Control for administering/performing parameter set-up of functionality across applications.
- Consistency, accuracy, adequacy and integrity of data in all reports and MIS.
- Availability of necessary audit logs and its accuracy and effectiveness of audit trail detailed enough to use it as forensic evidence and regulatory and legal requirements.
- Adherence of reporting to legal and statutory requirements.
- Automated batch processing, scheduled tasks, critical calculations, etc.
- Start of Day, End of Day and periodic closure operations including End of Month, End of Quarter and End of Year.
- Release of software governed by formal procedures–ensuring sign-off through testing, handover etc.
- Formal procedure for change management being adopted.
- Impact analysis of changes made.
- Associated documents and procedures–being to be updated accordingly
- Maintenance personnel have specific assignment and their work is properly monitored. Their system rights are controlled to avoid risk of unauthorized access to automated system.
- Access log is monitored.
- Control on user administration.
- Access controls and dual controls on transaction processing.
- To test Interface Compatibility between different software (eg: Olympic Software & RTGS and vice versa)
- Cost effectiveness of existing applications

e. Database Audit:

The audit would provide assurance on authorization, authentication, access control review, data integrity controls, data back-up management, review of database privileges assigned to DBAs/Users, security of database systems files, patch management. It would further review control procedures for changes to parameter files, sensitive DB passwords, procedures for purging of Data Files, Data Back-up, restoration, recovery and reliability of back up of data, purging of Data files, output reports and version control.

f. Network Audit:

The audit would provide assurance on overall network management, network architecture/design review, structuring of cable, traffic analysis and base lining. The auditor would evaluate procedures adopted for.

- Secured transmission of data through dial-up/ leased line/ VPN/ VSATs, Wireless
- Bandwidth management
- Uptime of network – it's monitoring as per SLA
- Fault Management
- Capacity Planning
- Performance Management.
- Monitoring for logs.

Information system auditor would further provide assurance on network devices for any security threats, privileges available to system integrator and outsourced vendor, configuration and access control audit for all networking devices, viz. routers, switches, IDN/IPS, Firewalls, etc. The auditor would conduct audit of antivirus protection at host and at desktop levels, procedure of antivirus updated at DC, servers and desktops, gateway level antivirus protection. It would cover the aspects of domain controllers, its configurations, security and administration of active directory.

g. Security Management Review

It would provide assurance on security equipment configuration and policies, Vulnerability Assessment and Penetration Testing (VAPT) of various security zones/networks/delivery channels and maintenance of necessary logs. Vulnerability Assessment and Penetration Testing execution and contingency plan as well as commitment letter for business continuity during the test should be submitted before execution of the test.

h. Review of IT Processes and IT Management Tools

It would provide assurance on IT asset management, enterprise management system; help desk, change, incident, network, back–up, media, anti-virus, vendor & SLA management, etc.

i. Review of Policies and Procedures

The auditor should provide assurance on IT Policy/ Manual, IS security policy, disaster recovery policy, data purging policy, Email policy and any other policies which are in force. The auditor should review the documentation electronic attacks and suspected electronic attacks in the system.

j. Payment Gateway Audit

The auditor should provide assurance on verification of controls for SWIFT, Reuters etc. at payment gateway, as per the Bank’s policies and guidelines.

k. Business Continuity and Disaster Recovery Planning

The auditor should analyze and provide assurance on:

- Business Continuity Plan (BCP) considering impact analysis, recovery strategies, business continuity plan as well as testing, training, awareness, communication and crisis management program.
- Recovery Point Objective (RPO) and Recovery Time Objective (RTO) as specified in the BCP.
- The configuration of the data centre, disaster recovery solution, enterprise network and security and branch or delivery channels.

- The overall executive ownership, Charter, Policy (ies), Risk Assessment, and Preventive Actions.

l. Risk Management (System Risk) Process

The auditor should evaluate the adequacy of system risk management process of the Bank and provide complete coverage of system risk management concepts and applications for safe design and operation of process facilities. Also provide better alternative for different software/ programs used by the Bank.

m. Follow-up of previous IS audit findings

The auditor should evaluate the adequacy and timeliness of management's response and the corrective action taken on significant audit recommendations from previous IS audit.

In line with the above, IS Auditor is required to perform gap analysis of the business requirements and current function available in MIS and FIS application. Validation of business system controls in the MIS and FIS applications covering documentation, transaction origination, input and output controls, processing controls, and most importantly the accuracy of system generated reports is also required to done. In addition the IS auditor must analyze business process risks and controls based on an understanding of planned or implemented controls and identified controls gaps.

The IS auditor is required to review role of Internal audit in relation to IS audit. This may involve evaluating audit plans and reporting to audit committee and senior management on controls, specific resources required for performing IS audit function.

The Priority of Domains for IS Audit

Current Audit Cycle

i. Application System Audit
ii. Database Audit
iii. Network Audit
iv. Security Management Review
v. Operating System Audit
vi. Payment Gateway Audit
vii. Review of IT Process and IT Management tools
viii. IT Department Audit

Next Audit Cycle

ix. Review of Policies and Procedures
x. Data Center Facilities Audit
xi. Business Continuity and Disaster Recovery Planning
xii. Follow-up of previous IS audit findings
xiii. Cost effectiveness of existing system

CONFIDENTIALITY

It shall be the duty of IS auditor and all members involved in the IS Audit to maintain the confidentiality of the information obtained during the course of audit. The IS auditor and its staff, during the course of audit or afterward, shall not disclose any information to other person except otherwise required by prevailing laws if any.

SKILLS REQUIRED

The Bank seeks service of Chartered Accountant firm, either singly or in joint venture with other specialized firm/company in information system audit. The firm (together with joint venture, if applicable) should meet the following skills/criteria.

- Have been registered in Nepal and have conducted IS Audit during last three consecutive fiscal years,
- Have conducted IS Audit of at least three banks,
- Average annual turnover of last three fiscal years should not be less than Rs. 1.476 million,
- Should be associated with company/firm/ international auditor with CISA qualification; and
- Shall have staff base of at least 10 on payroll. At least 2 of the staff or partners should be ISA or CISA certified and one of them should be IT Security Specialist.

DELIVERABLE

At the end of consultancy the IS Auditor is required to submit a report containing detailed observations on aforementioned areas as well as suggested areas during preliminary meeting with the management, In addition, a detailed roadmap/recommendations for improvements in risk areas identified are also required. The auditor would submit a draft report within 90 days of the start of work .The final report shall be submitted within 30 days after response from Nepal Rastra Bank, if any, on the draft. Furthermore, the follow up report for previous audit should be submitted. The auditor is also required to submit the monthly work plan before the start of the work and progress report every 30 days to the Nepal Rastra Bank, Internal Audit Department.

TIMEFRAME

The audit assignment should be completed in all its forms within 4 months from the date of commencement of the work.

INTELLECTUAL PROPERTY RIGHT

D. Evaluation of Consultant's EOI Application

Consultant's EOI application which meets the eligibility criteria will be ranked on the basis of the Ranking Criteria.

i) Eligibility & Completeness Test	**Compliance**
Copy of Registration of the company/firm	
VAT/PAN Registration	
Tax Clearance/Tax Return Submission/Letter of Time Extension for Tax Return Submission FY***2075/76***	
In case of a natural person or firm/institution/company which is already declared blacklisted and ineligible by the GoN, any other new or existing firm/institution/company owned partially or fully by such Natural person or Owner or Board of director of blacklisted firm/institution/company; shall not be eligible consultant.	
EOI Form 1: Letter of Application	
EOI Form 2: Applicant's Information Form	
EOI Form 3: Experience (3(A) and 3(B))	
EOI Form 4: Capacity	
EOI Form 5: Qualification of Key Experts	

ii) EOI Evaluation Criteria	**Insert Minimum Requirement if Applicable**	**Score [Out of 100%]**
A. Qualification		
System Audit Expert	*Atleast 2 of the staff or partners should be ISA or CISA certified and one of them should be IT Security Specialist. Should have staff base of atleast 10 on payroll.*	***Score 50.0***
B. Experience		
General of consulting firm	*Chartered Accountant Firm either singly or in Joint Venture with other specialized firm/company in information system audit.*	***Score 40.0***
Specific experience of consulting firm within last 7 years.	*Have been registered in Nepal and have conducted IS Audit during last three consecutive fiscal years. Have conducted IS Audit of at least three banks*	
C. Capacity		
Financial Capacity		***Score 10.0***
Average annual turnover of last three fiscal years	*Should not be less than 1.476 million*	

Note : In Case, a corruption case is being filed to Court against the Natural Person or Board of Director of the firm/institution /company or any partner of JV, such Natural Person or Board of Director of the firm/institution /company or any partner of JV such firm's or JV EoI shall be excluded from the evaluation, if public entity receives instruction from Government of Nepal.

E. EOI Forms & Formats

Form 1. Letter of Application

Form 2. Applicant’s information

Form 3.Experience *(General, Specific and Geographical)*

Form 4. Capacity

Form 5. Qualification of Key Experts

1. Letter of Application

(Letterhead paper of the Applicant or partner responsible for a joint venture, including full postal address, telephone no., fax and email address)

Date: .....

To,

Full Name of Client: _____

Full Address of Client: _____

Telephone No.: _____

Fax No.: _____

Email Address: _____

Sir/Madam,

1. Being duly authorized to represent and act on behalf of (hereinafter "the Applicant"), and having reviewed and fully understood all the short-listing information provided, the undersigned hereby apply to be short-listed by ***[Insert name** of Client)* as Consultant for ***{Insert brief description** of Work/Services}.*

2. Attached to this letter are photocopies of original documents defining:

    a) the Applicant's legal status;

    b) the principal place of business;

3. ***[Insert name of Client]*** and its authorized representatives are hereby authorized to verify the statements, documents, and information submitted in connection with this application. This Letter of Application will also serve as authorization to any individual or authorized representative of any institution referred to in the supporting information, to provide such information deemed necessary and requested by yourselves to verify statements and information provided in this application, or with regard to the resources, experience, and competence of the Applicant.

4. ***[Insert name** of Client)* and its authorized representatives are authorized to contact any of the signatories to this letter for any further information.[2]

5. All further communication concerning this Application should be addressed to the following person,

    [Person]

    [Company]

    [Address]

    [Phone, Fax, Email]

6. We declare that, we have no conflict of interest in the proposed procurement proceedings and we have not been punished for an offense relating to the concerned profession or

[2] Applications by joint ventures should provide on a separate sheet, relevant information for each party to the Application.

business and our Company/firm has not been declared ineligible.

7. We further confirm that, if any of our experts is engaged to prepare the TOR for any ensuing assignment resulting from our work product under this assignment, our firm, JV member or sub-consultant, and the expert(s) will be disqualified from short-listing and participation in the assignment.

8. The undersigned declares that the statements made and the information provided in the duly completed application are complete, true and correct in every detail.

Signed **:**

Name **:**

For and on behalf of (name of Applicant or partner of a joint venture):

2. Applicant's Information Form

(In case of joint venture of two or more firms to be filled separately for each constituent member)

1. Name of Firm/Company:

2. Type of Constitution (*Partnership/ Pvt. Ltd/Public Ltd/ Public Sector/ NGO)*

3. Date of Registration / Commencement of Business *(Please specify):*

4. Country of Registration:

5. Registered Office/Place of Business:

6. Telephone No; Fax No; E-Mail Address

7. Name of Authorized Contact Person / Designation/ Address/Telephone:

8. Name of Authorized Local Agent /Address/Telephone:

9. Consultant's Organization:

10. Total number of staff:

11. Number of regular professional staff:

(Provide Company Profile with description of the background and organization of the Consultant and, if applicable, for each joint venture partner for this assignment.)

3. Experience

3(A). General Work Experience

(Details of assignments undertaken. Each consultant or member of a JV must fill in this form.)

S. N.	Name of assignment	Location	Value of Contract	Year Completed	Client	Description of work carried *out*
1.						
2.						
3.						
4.						
5.						
6.						
7.						

3(B). Specific Experience

Details of similar assignments undertaken in the previous seven years
(In case of joint venture of two or more firms to be filled separately for each constituent member)

Assignment name:	Approx. value of the contract (in current NRs; US$ or Euro)[3]:
Country: Location within country:	Duration of assignment (months):
Name of Client:	Total No. of person-months of the assignment:
Address:	Approx. value of the services provided by your firm under the contract (in current NRs; US$ or Euro):
Start date (month/year): Completion date (month/year):	No. of professional person-months provided by the joint venture partners or the Sub-Consultants:
Name of joint venture partner or sub-Consultants, if any:	Narrative description of Project:
Description of actual services provided in the assignment: **Note: Provide highlight on similar services provided by the consultant as required by the EOI assignment.**	

Firm's Name: _____

[3] Consultant should state value in the currency as mentioned in the contract

3(C). Geographic Experience

Experience of working in similar geographic region or country

(In case of joint venture of two or more firms to be filled separately for each constituent member)

No	***Name of the Project***	***Location (Country/ Region)***	***Execution Year and Duration***
1.			
2.			
3.			
4.			
5.			
6.			
7.			

4. Capacity

4(A). Financial Capacity

(In case of joint venture of two or more firms to be filled separately for each constituent member)

Annual Turnover	
Year	**Amount Currency**

- **Average Annual Turnover of Best of 3 Fiscal Year Of Last 7 Fiscal Years**

(Note: Supporting documents for Average Turnover should be submitted for the above.)

4(B). Infrastructure/equipment related to the proposed assignment[4]

No	Infrastructure/equipment Required	Requirements Description
1.		
2.		
3.		
4.		
5.		

[4] *Delete this table if infrastructure/equipment for the proposed assignment is not required.*

5. Key Experts *(Include details of Key Experts only)*

(In case of joint venture of two or more firms to be filled separately for each constituent member)

SN	Name	Position	Highest Qualification	Work Experience (in year)	Specific Work Experience (in year)	Nationality
1						
2						
3						
4						
5						

(Please insert more rows as necessary)