Expression of Interest
(EOI)

Title of Consulting Services
System (IT/IS) Audit of RBBL

Method of Consulting Service
National

Project Name : ***System (IT/IS) Audit of RBBL***
EOI Number : ***RBBL/GSD/EOI/Audit – System/2/077/78***
Office Name : Rastriya Banijya Bank Ltd, Central Office, General Service Department
Address : Singhadurbarplaza, Kathmandu
Issued on : Jestha 18, 2078 (June 01, 2021)

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

REQUEST FOR SUBMISSION OF EXPRESSION OF INTEREST (EOI)

For System (IT/IS) of Rastriya Banijya Bank Ltd.(RBBL)

(First date of publication 2078/02/18)

1. The Rastriya Banijya Bank Ltd now invites Expression of Interest (EOI) from eligible consulting firms ("consultant") to provide the following consulting services: **Procurement of Consultancy Service for System (IT/IS) Audit of RBBL,2078.** Interested firm should submit an **Expression of Interest** (**EOI)** in their own format that shall include:
   - A Covering letter (with expression of interest and declaration to submit detailed proposal)
   - The Profile and applicable organizational certificates
   - An Area coverage with details breakdown and the concept note on how for this proposal
   - The Details of similar experience with evidence and
   - A Proposed team composition, designation and CVs of key team members.
   - The Documents to meet our desired minimum qualification
2. Interested eligible consultants may obtain further information and EOI document free of cost at the address Rastriya Banijya Bank Ltd, Central Office, General Service Department, Kathmandu, Nepal during office hours on or before **Asar 01, 2078 (June 15, 2021)**. A complete set of EOI Document is available online and can be downloaded from RBBL website **www.rbb.com.np.**
3. Consultants may associate with other consultants to enhance their qualifications.
4. Expression of interest shall be delivered *manually* to the ***Rastriya Banijya Bank Ltd, Central Office, General Service Department, Singhadurbarplaza, Kathmandu, Nepal*** during office hour on or before **Asar 02, 2078 (June 16, 2021)**
5. 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.
6. EOI will be assessed based on Qualification 50.0 %, Experience 40.0 %, and Capacity 10.0 % 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 (RFP). Minimum score to pass the EOI is: 60
7. Required Experience & Qualification criterion for system audit of RBBL are as follows:
   - The audit firm or company should have in depth knowledge of the working of the Financial Institutions,
     Information Technology and Information Technology Risk involved in the Financial Industry.
   - The audit firm or company should have proven experience of conducting system (IT/IS) audit of at least 3 (**three) A class commercial banks**.
   - The Audit firm or company should have at least 3 (three) full time certified system audit professionals having CISA, CISSP, OSCP, CPTE,LPT,CEH,CGEIT,CISM,Security+ or equivalent as a permanent member or employee of the firm or company.
   - There should be at least **1 (one)** CISSP or OSCP in the audit team to lead VAPT who has conducted Vulnerability Assessment and Penetration Testing of at least **3 (three)** A class commercial banks.
   - The team leader must be **CISA** Certified with **at least 3 (three)** years of proven post qualification experience of auditing financial institutions. He/she should have successfully led the audit of at least **3 (Three)** A class commercial banks. The team leader should be a full time member or employee of the firm or company, as the case may be, and should be available during the whole audit process.
   - The audit firm or company should have permanent operational office in Nepal and should be available to respond to post audit queries, guidance, support and verification post audit
8. The RBBL reserves all the right to accept or reject one or all EOI proposals without assigning any reason whatsoever with its sole discretion.

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 ***consulting firm/company/ organization***.
4. The assignment has been scheduled for a period as mentioned in TOR**.** Expected date of commencement of the assignment is August,2021**.**
5. A Consultant will be selected in accordance with the ***QCBS*** method.
6. 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).*
7. 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.
8. 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 ***System (IT/IS) Audit of RBBL*** .The Envelope should also clearly indicate the ***name and address of the Applicant***..
9. 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 / TOR

Terms of References for the System (IT/IS) Audit

1.0 Background

Rastriya Banijya Bank (RBB) has a history of serving its customers far and wide across the nation for more than half a century. The bank then fully owned by Government of Nepal, was established on 10 Magh 2022 (23 January 1966) under the special statute "Rastriya Banijya Bank Act, 2021" and had operated under the "Commercial Bank Act,2031" until it was re-registered as public limited company on 6 Baishak 2063 (19 May 2006). At present, the Bank operates as "A" class financial institution licensed by Nepal Rastra Bank and carries out commercial banking activities as per the provisions of the "Bank and Financial Institutions Act 2073," (2017).

The bank stands as one of the most preferred bank with the highest number of customers in all 77 districts and 7 provinces of the country. The Bank has been able to imprint its presence in the national economy through efficient allocation of resources in all sectors of the economy thereby enhancing production and generating employment opportunities within the country. The unflinching faith and goodwill bestowed by our customers, continued support from the Government, well-wishers and the general public has been the reason for us to stand as the most trusted bank in the country.

RBB intends to engage a competent consultant for carrying out system (IS/IT) audit. The system audit will entail conducting a risk assessment of the IT systems at the bank; identification and evaluation of the risks. In the light of the risk assessment exercise, the selected consultant should recommend and assist in implementing a set of best practices governing the management of the Information System at the bank. The consultant should deliver at the end of the audit exercise; a complete audit report comprising an executive summary, findings, and recommendations, which shall include but not limited to all areas as specified in the scope of services.

2. Scope of Services

2.1 Objective

RBB intends to carryout system (IT/IS) audit including Vulnerability Assessment and Penetration Testing (VAPT). The system (IT/IS) audit should cover the bank's Information System Infrastructure including Data Center (DC), Disaster Recovery (DR) Site, Backup Disaster Recovery (BDR) Site, Network System, Security Devices, Servers, Databases, and Applications accessible through LAN, WAN as well as public IPs. The selected consultant shall carry out an assessment of threats and vulnerability in the bank's IT infrastructure. This will include identifying existing threats if any and suggest remedial solutions and recommendations to mitigate all identified risks and to enhance the security of IT systems.

The system (IT/IS) audit should cover the following IT Infrastructure but not limited to the following IT Infrastructures:

- Data Center(DC), Disaster Recovery (DR), and Backup Disaster Recovery (BDR) sites.
- Servers, databases, and applications (both web-based and desktop-based applications) in the bank.
- Firewalls and other security devices in DC, DR, and BDR sites.
- Routers at DC, DR, BDR Sites, Central Office, Provincial Offices, and Branches.
- Demilitarized Zone (DMZ), Virtual Private Network (VPN)
- Wi-Fi Network and VoIP Communication Network
- All the L3 and L2 network switches in DC, DR, and BDR Sites.
- Desktop PCs and Laptops (on a sample basis).

2.2 Areas to be Covered

The areas to be covered in IT/IS Audit but not limited to the followings:

2.2.1 IT Governance

a) Review the lapses in existing IT Policy and Guideline.
b) Procurement Policy for IT equipment
c) Review IT governance structure and its effectiveness
d) Standard Operating Procedure / Operation Manual
e) Implementation of Directives
f) Identify the status of overall IT security
g) Verify the utilization of IT-resources and suggestion on enhancing efficiency
h) Check the compliance of IT Security Policy, Guidelines, Procedures and Manuals defined by the Bank and Nepal Rastra Bank Information Technology Guidelines

2.2.2 Core Banking System

a) Interest calculation mechanism for both deposits and loan products.
b) Non-performing loan and loan loss provision calculation
c) User access and control mechanisms.
d) Uses of Network bandwidth for Core Banking System and its efficient use.
e) Review of automated scheduled tasks present in the system and analysis of their effectiveness.
f) Polices, practices, time duration analysis of End-of-Day, Month End, Quarter End, and Year End operations in Core Banking System.
g) Policies and practices of testing and implementation of patches in the core banking system.
h) Review the existing report and its format.
i) Review of reports generated from the core banking system including distribution and access control system of these reports.
j) Data Violation, Database restore & Reuse, Password Protection, hacking & Cracking
k) Review of Technical Documentation, Standard Operating Procedure (SOP)/ Operation Manual, User Manuals, etc.
l) Review security risk in Core Banking System with Card Switch, ATM, Mobile Banking and Internet Banking System.
m) Risk analysis and control mechanisms in Core Banking System.
n) Review third-party system/middleware (including of PSP/PSO) integration risk with CBS.
o) Review security risk from middleware between Core Banking System and third-party systems.
p) Review of Migration Procedure.
q) Application/data backup and restoration policies and procedures of the Core Banking System.
r) Review consultant access and consultant risk.
s) A contingency plan to continue the core banking system in event of disruptions to normal operations.
t) AMC (Annual Maintenance Contract)
u) Whether the licensing policy is favorable for an organization or not
v) Review the overall performance of the Core Banking System and recommend if any.

2.2.3 In house Developed System

a) Review of in-house developed applications
b) Review in-house development lifecycle.
c) Technical Documentation

d) Administration of User Profile, Control
e) Security Measures
f) Platform Dependence
g) Flexibility
h) User Interface Design
i) User Manuals / Help Files

2.2.4 Email System

a) Review of Email system's framework.
b) Review of security policies and practices of the system.
c) Administration of user accounts and presence of security measures in user accounts.
d) Security measures to prevent unwanted email traffic (spam, infected emails, etc.) originating from/coming into the email system.
e) Application plus data backup and restoration process.
f) Filtration of outgoing email.
g) Servers Compatibility and optimum use
h) Security measures to prevent unwanted email traffic (spam, infected emails, exe files, scripts)
i) Firewall management for e-mail system
j) Password Encryption

2.2.5 Internet Banking

a) Review of Internet Banking system's framework.
b) Functionality of Internet Banking.
c) Review of security policies and practices of the system.
d) Administration of user accounts.
e) Security features of user accounts such as protective measures taken by the system to prevent unauthorized access in the system.
f) Transaction process, application and its performance.
g) Un-successful transaction rates and reversal authorizations
h) Application plus data backup and restoration process.
i) Certificate Authority (CA)
j) An unauthorized Access Control mechanism
k) Password Policy
l) Security of Users profile, password & Secret Question
m) Review security threats in Core Banking System from Internet Banking.
n) Internet Banking System platform
o) Review consultant access and consultant risk

2.2.6 Mobile Banking

a) Review of Mobile Banking system's framework.
b) Functionality of Mobile Banking.
c) Review of security policies and practices of the system.
d) Administration of user accounts.
e) Security measures of user accounts such as protective measures taken by the system to prevent unauthorized access in the system.
f) Transaction module, application and its performance.
g) Certificate Authority (CA)
h) Unauthorized Access Control mechanism

i) Password Policy
j) Security of Users profile, password & Secret Question
k) Un-successful transactions rates and reversal authorizations
l) Application plus data backup and restoration process.
m) Review security threats in Core Banking System from Mobile Banking.
n) Review consultant access and consultant risk

2.2.7 Anti-Virus System

a) Review of Anti-Virus system's framework.
b) Review of security policies and practices of the system.
c) Review of system's monitoring tool and virus intrusion detection tool.
d) Review of the functionality of the system.
e) Application plus data backup and restoration policies and practices.
f) Review Virus Intrusion Detection Log.
g) Effectiveness, use of the server, and functioning.

2.2.8 Network (LAN/MAN/WAN) and Securities

a) Review of network infrastructure, which includes the infrastructures at the data center, disaster recovery site, backup disaster recovery site, provincial offices, branches, and the connectivity between these locations.
b) Review of the functionality of network and security devices (firewalls, routers, switches, and other network & security devices.) and whether they fulfill all of the bank's requirements.
c) Review of network monitoring tools and their effectiveness.
d) A contingency plan to continue network services from the main data center/disaster recovery site to all branches.
e) Firewall policies, backup, and restoration mechanisms.
f) Review of network firewall device policies and practices.
g) Management of Routers logs for unauthorized Access
h) Trust Zones
i) Operating System Security
j) VPN
k) Anti-malware controls
l) Data Cables and Switch Management
m) Idle workstations, Data cables (Terminals RJ)
n) Review consultant access and consultant risk

2.2.9 System / Infrastructure Securities

a) Review of preventive measures taken by the bank to prohibit the following: installation of unauthorized software, the spread of computer viruses/malware/spam emails, visit blocked websites, unauthorized hardware/software changes to the computers at the bank, etc.
b) Review of security policies and practices including intrusion detection system, avoiding denial of service attacks, blocking unauthorized access to the bank's secured network, etc.
c) User security for individual computer users at the bank.
d) Review of architecture and placement of security devices.
e) Review of security devices and their effectiveness at maintaining securities at the bank.
f) Reporting and escalation mechanism for security issues.
g) Implementation of Active Directory and its functioning.

h) DNS and DHCP configuration.
i) Unauthorized Access in RBB Network.
j) Use and Installation of External Device in RBB Network.
k) Review Operation System and other System/Software Licenses.

2.2.10 Hardware Infrastructure

a) Architecture of hardware at the main data center, disaster recovery site, and backup disaster recovery site.
b) Review of policies and practices of hardware monitoring process at the data center, disaster recovery site, and backup disaster recovery site.
c) A contingency plan to continue operations in event of a hardware problem at the data center and/or at the disaster recovery site.
d) Policies and practices of maintaining the hardware inventory and its effectiveness.
e) Review of periodic hardware servicing process and its effectiveness.
f) Effectiveness of Hardware Inventory
g) Optimum use of Hardware in Existing Resources
h) Misuse of Devices/ Resources
i) Pre and Post Delivery Inspection (PDI) Policy and Conditions

2.2.11 Operating Systems Audit

a) The Information System Audit should cover the following aspects of servers, databases, network equipment, security systems, and storage area network:
b) Set-up and maintenance of system parameters
c) Hardening and configuration of servers and operating systems
d) Updates, Upgrades and Patch management
e) Change management procedures
f) Logical access controls
g) User management and security
h) Fault tolerance, performance, scalability and availability
i) Evaluation of role, responsibility and accountability of IT process owners based on the principle of least privilege and "need to know" commensurate with the job responsibilities

2.2.12 General / Business Continuity Plan

a) Data retention policies and practices of the bank relating to IT services.
b) Data backup policies and practices for individual computer users at the bank.
c) Review of system checklist logs, service downtime logs, hardware maintenance logs, and their effectiveness.
d) Working procedure in Help Desk
e) Maintenance of documentation to comply with bank's policies and audit requirements.
f) Incident Response
g) Review the "Business Continuity Plan" and its effectiveness.
h) Logging and Monitoring
i) Configuration/Change management
j) Physical and Environmental controls at both primary and secondary data centers

2.2.13 Data Centre and Disaster Recovery (DR) site.

a) Backup, Replication, Mirroring
b) Storage & Offside Backup
c) Disaster Recovery Plan & Practice
d) Integrity Check, Database Testing Mechanism
e) Review the Overall infrastructure of the Data Center, Disaster Recovery (DR), and Backup Disaster Recovery Site.

f) Password Protection mechanism for core database
g) Review Physical security of Data Center, Disaster Recovery Site, and Backup Disaster Recovery Site.

2.2.14 ATM/Card

a) Review existing practice
b) Security measures in generating Card
c) PIN Embossing and its Control
d) User Management
e) Control Mechanism
f) Database Management
g) Security measures in ATM
h) Technical Relationship with NIBL
i) Review the security measures of NARADA System and its Administration
j) Un-successful transactions rates and reversal authorizations
k) AMC with NARADA
l) Backup of Technical Expertise in its operation.
m) Segregation of Duty in operations.
n) Review consultant access and consultant risk

2.2.15 IT Department Audit

The Audit should cover the IT organizational structure and human resources management of the bank with a specific focus on the IT Department

a) Review of organizational structure for IT, employee strength whether it is commensurate with the size, scale, and nature of business activities carried out by the bank
b) Review of Development, Technology, IT Operation and Information Assurance team within the department
c) Assessment of periodic IT training requirement for IT personnel and performance monitoring and measuring system according to the IT functions of the bank
d) Segregation of Duty in all IT operations

2.2.16 Review of Policies and Procedures

Covering the following aspects:

a) IT Policy, IT Guidelines, Standard Operating Procedure/Operation Manual
b) Information Security Policy
c) Business Continuity and Disaster Recovery Policy
d) Data and Media Disposal Policy and Procedures
e) ATM/Card Policy covering the following:
    i. Controls over procurement and issuance of cards
    ii. Controls on printing of covering letter, terms & conditions etc
    iii. Controls on physical usage of kits & insertions and treatment of waste
    iv. Control on cards hands off to delivery cell
    v. Ensuring acknowledged delivery in each case
    vi. Controls over the cancellation of undelivered cards
    vii. Controls on the process of PIN generation and delivery.
    viii. Control on Authorization Process
    ix. Controls on the transaction Authorization process
    x. Control on Statements
    xi. Controls on data flow for statement generation
    xii. Controls relating to Card Cancellation/Re-issuance/Renewal Process

f) Internet Banking Policy, Mobile Banking Policy, Branchless Banking Policy
g) Email Policy involving the mail server administrator, network administrator, and the email user with the objective
   i. To protect the confidentiality of identified information by preventing leakage of information to those without the need – to - know.
   ii. To ensure an appropriate level of sender authentication and non - repudiation.
   iii. To ensure an appropriate level of email integrity.
   iv. To protect the availability of the system by controlling access to critical system functions and preventing malicious code based denial of service attacks
h) Outsourcing Policy
i) Review the documentation of electronic attacks and suspected electronic attacks in the system
j) Any other policies which are not listed above and are in force

3. Vulnerability Assessment and Penetration Test (VAPT)

The consultant shall perform VAPT of servers, databases, Core Banking System, applications in RBB (Internet Banking, Mobile Banking, RBB Remit and other systems/applications in the bank), wallet and other ISO middlewares, Network (LAN, WAN), Network and Security devices, and the overall IT infrastructure without disturbing operations. The consultant shall perform Black Box Testing, Grey Box Testing, and White Box Testing.

3.1 Network and Infrastructure

VAPT should be comprehensive but not limited to the following activities:

- **Network Scanning**
  - Review server response and information leaks.
- **Network Architecture**
  - Review existing network Architecture and recommend for improvement if any.
- **Network and Security Device Assessment**
  - Review existing network and security devices and recommend for the improvement if any
- **Port Scanning**
  - Detect unnecessary open ports and services running on the servers.
- **Vulnerability Scanning**
  - Scan for vulnerabilities or weaknesses in a system and all other IT assets.
- **Access Control**
  - Review access Control List and recommend for improvement if any.
- **IDS/IPS**
  - Review existing placement of IDS/IPS and recommend for the improvement if any
  - Review the existing configuration of IDS/IPS and recommend for improvement if any.
  - Review IDS logs and alerts.
- **Man in the Middle Attack**
  - examine the possibilities of eavesdropping the MIMA has to be occurred out
- **Malware Scanning**
  - The consultant shall do the scanning for hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

- **Key loggers/ Rootkit/ Botnet**
  - Assess the systems to see the presence or probability of the presence of key loggers, rootkit, and botnet
- **System and OS Fingerprinting**
  - Detect OS, version, etc.
- **System and OS Configurations**
  - review the existing configuration of critical server OS and recommend for the improvement if required
- **OS Hardening**
  - Review the existing OS Hardening and recommend the gap in hardening, patch management, etc.
- **DOS and DDOS Attacks**
  - Examine possibilities of DOS and DDOS attacks on the system and recommend for the improvement if any
- **Authentication and Authorization**
  - Review authorization and authentication of the system including AD.
- **Virtualization**
  - Review security risk on virtual servers/systems.
- **Database Assessment**
  - Review existing databases and recommend for improvement if any.
- **Social Engineering**
  - Consultant shall carry put social engineering for users at Central Office, IT Staff, Provincial Staff, and Branch Staff.
- **Security Risk associated with OS**
  - Review security risk associated with systems running on the different OS platforms.
- **Remote Access**
  - Review remote access practice and recommendations for improvement.

3.2 Applications

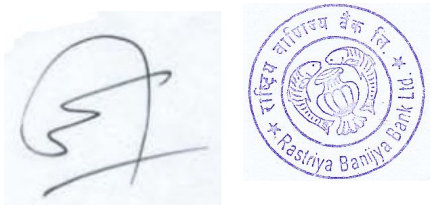
RBB intends to carry out Vulnerability Assessment and Penetration Testing (VAPT) of the bank's applications including the Core Banking System of the bank with the underlying infrastructure. Some applications in the bank are desktop-based and the rest are web-based applications. The core banking system of the bank is Pumori and it is a desktop/windows application.

The consultant shall perform the assessment for the web application as per the OWASP guidelines including but not limited to the following:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring
- Any other attacks, which are vulnerable to websites and web applications.

To exploit vulnerabilities or defects in the security features in the system, the consultant may use a manual process, or vulnerability scanning, or other authorized automated tools. The consultant should perform their VAPT activities carefully without disturbing the running system.
The consultant should perform the following activities but not limited to the following:

- **Infrastructure**
  - Review the current infrastructure and recommendations for improvement if any.
  - Review OS Security Configuration.
  - Review server configuration, and security measures. Provide possible security threats and recommendations for improvement if any.
- **Authentication**
  - Verify the password policy of RBB and other common standards in the applications.
  - Identify possible brute force attacks, cryptographic attacks, password cracking in applications.
  - Bypass authentication in applications - spoofed tokens, replay authentication information, Injection attacks, etc.
  - Verify authentication sessions - the number of failure login allowed, login timeout, etc.
  - Review access control in application - access permissions, login duration, idle duration.
  - Verify transmission of authentication - authentication credentials in clear text/ encrypted / hash.
  - Review Certificate Authority (CA) and other security measures.
- **Session Management**
  - Session information - number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, the session ID in URL encoding string, the session ID in hidden HTML field variables, etc.
  - Session ID sequence and format
  - Check if the same session information can be retried and reused in another machine.
  - Session management limitations - bandwidth usages, file upload/download limitations, transaction limitations, etc.
  - Gather sensitive information with Man-In-the-Middle attacks.
  - Inject excess/bogus information with Session-Hijacking techniques.
  - Replay gathered information to fool the applications.
- **Cookie Security**
  - Review cookie setting & bugs and recommend the best practice for a secure environment.
- **DOS and DDOS Attacks**
  - Verify user accounts, system files, and other resources are secured and all access follows the Principle of Least Privilege (POLP).
  - Verify what procedures are in place to respond to irregular activity.
  - Verify the response to propaganda attacks.
  - Verify server loads.
- **Application Bug Analysis**
  - Review the application bugs and recommend the best practice.
- **Input Manipulation**
  - Verify that input validation at the client and server end.
  - Find the limitations variables and protocol payload - data length, data type, etc.
  - Buffer overflows vulnerability in the applications.



- Inject SQL in the input strings.
- Cross-Site Scripting in the applications.
- Directory Traversal: verify unauthorized directory/file access.
- Bypass input validation mechanisms of the applications - Use specific URL-encoded strings and/or Unicode-encoded strings.
- Execute remote commands through "Server Side Include".
- Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
- Manipulate the (hidden) field variable in the HTML forms to fool or modify the logic in the server-side web applications.
- Use illogical/illegal input to test the application error-handling routines and to find useful debug/error messages from the applications.

- **Output Manipulation**
  - Retrieve valuable information stored in the cookies
  - Retrieve valuable information stored in the client application cache.
  - Retrieve valuable information stored in the temporary files and objects.
  - Retrieve bulk information/multiple rows from the database.
- **Information Leakage**
  - Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
  - Find valuable information stored in the HTML source code on the browser.
  - Examine the information contained in the application banners, usage instructions, welcome messages, application help messages, debug/error messages, etc.

4. Deliverable

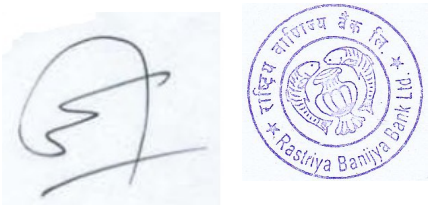
The consultant required to deliver the following:

- Interim System Audit Report with findings and recommendations.
  - The consultant should help to analyze the request report. Moreover, the consultant should provide guidance to fix the gaps indicated.
  - Give alternate recommendations in case the primary recommendation is not feasible to implement.
- Final System Audit Report with Executive Summary.
  - The consultant is required to retest or verify improvements if any and should provide the final report.
  - The final report should include an executive summary, statement of scope, review of past threats & vulnerabilities, methodologies, limitations, a summary of test results, recommendations, tools used, etc.

5. Experience and Qualification of the Consultant/Audit Firm

1. The consultant organization/audit firm should have in-depth knowledge of the working of the Financial Institutions, Information Technology, and Information Technology Risk involved in the Financial Industry.
2. The consultant organization/audit firm should have proven experience of conducting system audit (IS/IT Audit) of at least three (3) A class commercial banks.
3. The consultant organization/audit firm should have at least three (3) full-time certified system audit professionals having CISA, CISSP, OSCP, CPTE, LPT, CEH, CGEIT, CISM, Security+ or equivalent as a permanent member or employee of the consultant organization or firm.

4. There should be at least one CISSP or OSCP in the audit team to lead VAPT who has conducted Vulnerability Assessment and Penetration Testing of at least three (3) A class commercial banks.
5. The team leader must be CISA Certified with at least three (3) years of proven post qualification experience of auditing financial institutions. He/she should have successfully led the audit of at least three (3) A class commercial banks. The team leader should be a full-time member or employee of the firm or company, as the case may be, and should be available during the whole audit process.
6. The consultant organization/audit firm should have a permanent operational office in Nepal and should be available to respond to post audit queries, guidance, support and verification post audit.



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**
Updated Copy of Registration of the company/firm	
VAT/PAN Registration	
Tax Clearance Certificate of FY 2076/77	
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.	
If the 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 shall not be eligible to participate in procurement process till the concerned Court has not issued the decision of clearance against the Corruption Charges.	
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	**Minimum Requirement**	**Score [Out of 100%]**
A. Qualification		
Qualification of Key Experts	*As Mentioned in TOR*	***50%***
Experience of Key Experts	*As Mentioned in TOR*	
B. Experience		
General of consulting firm	Should have at least **3** years of general experience in **System (IT/IS) Audit**.	***40%***
Specific experience of consulting firm within last 7 years.	Consulting company/firm must have specific experience in **System (IT/IS) Audit** within last seven years. The consultant is required to furnish at least **3 client** (**A class commercial banks**) testimonials for the same.	
C. Capacity		
Financial Capacity (Average Turnover)	Average annual turnover of best three years out of last seven years should be at least NRs. **4 Million**	***10 %***

Minimum score to pass the EOI is: **60**

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.[1]
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 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):

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

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.)

2. 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)[2]:
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(C). Geographic Experience – Not Applicable

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

3. 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

Not Applicable

4. 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)