Expression of Interest
(EOI)

Title of Consulting Services:
SSPP-EOI-083/84-01

Method of Consulting Service: National

Project Name: Update of Information System Security Guidelines and Security Audit of Information Systems of Lumbini Province
EOI: SSPP-EOI-083/84-01
Office Name : Suchana tatha Sanchaar Prawidhi Pratisthan
Office Address: Butwal, Rupandehi, Lumbini Province
Issued on: September 03, 2026
Financing Agency: Government Budget

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

Lumbini Province Government
Suchana tatha Sanchaar Prawidhi Pratisthan
Butwal, Rupandehi

Date: September 03, 2026

Name of Project: Update of Information System Security Guidelines and Security Audit of Information Systems of Lumbini Province

1. Lumbini Province Government has allocated fund ***towards the cost of Information system security audit*** 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 **Suchana tathaa Sanchaar Prawidhi Pratisthan** now invites Expression of Interest (EOI) from eligible consulting firms ("consultant") to provide the following consulting services: **Design of Security Guidelines for Software Systems and Perform Security Audit of Information Systems of Lumbini Province**
3. Interested eligible consultants may obtain further information and EOI document free of cost at the address during office hours on or before 09 September 2026 or visit the website https://ictp.lumbini.gov.np.
4. Consultants may associate with other consultants to enhance their qualifications.
5. Expressions of interest shall be delivered manually to the address **Information and Commu**nication Technology Pratisthan, Butwal, Rupandehi, Lumbini Province on or before 09 Sep 2026 17:00 hours.
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 (40%), Experience (50%), 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 ***consulting firm***.
4. The assignment has been scheduled for a period of ***9 months.*** Expected date of commencement of the assignment is ***15 October 2026.***
5. A Consultant will be selected in accordance with the **Quality Cost Based Selection *(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.

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 **"Update of Information System Security Guidelines and Security Audit of Information Systems of Lumbini Province**
8. **"**. 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 or Brief TOR

Background of the Project:

Section I: Preparation of Information Security Guideline and Security Audit

1. 1. Technology Requirements

The technology requirements section of the existing information systems security guideline shall be assessed and updated to ensure that it remains relevant and conforms to current recognized secure-development standards, including the OWASP Application Security Verification Standard (ASVS) and OWASP secure-coding guidance. This involves reviewing the minimum traits required for a platform to be selected for building a system and updating these traits based on changes in technology and security practices since the guideline was last issued.

The guideline shall require that all technology platforms and programming languages be evaluated for their ability to support secure coding practices, secure data storage, secure communication protocols, and secure access controls. This evaluation shall, at minimum, examine the following dimensions:

- Secure coding practice support: availability of static application security testing (SAST) tooling, linting for common insecure patterns, memory-safety characteristics of the language, and the maturity of the platform's official secure-coding documentation.
- Secure data storage support: native or well-supported libraries for encryption at rest, parameterized query interfaces that prevent injection, and integration paths for secret- and key-management services rather than hard-coded credentials.
- Secure communication protocol support: built-in or well-maintained libraries for current TLS versions (TLS 1.2 or higher, with TLS 1.3 preferred), correct certificate validation by default, and support for mutual TLS where system-to-system communication is required.
- Secure access control support: availability of role-based or attribute-based access control primitives, secure session-management handling, and compatibility with centralized identity and directory services.
- Platform sustainability: vendor or community support lifecycle, patch release cadence, history of disclosed vulnerabilities, and time remaining until end-of-life or end-of-support, so that platforms approaching obsolescence are not newly approved.
- Ecosystem and dependency health: size and activity of the package ecosystem, availability of software composition analysis (SCA) tooling, and prevalence of actively maintained versus abandoned libraries within that ecosystem.
- Deployment and packaging support: availability of secure, minimal base images or runtime packages, and the platform's compatibility with containerized or isolated deployment models that limit the blast radius of a compromise.
- Configuration safety by default: whether the platform ships with secure default settings (e.g., encryption enabled, verbose errors disabled) or requires the developer to actively opt into security, since insecure-by-default platforms are more prone to misconfiguration.

The evaluation shall be documented for each candidate platform, framework, or language using a simple scoring approach so that approval decisions are consistent and repeatable.

Any technology requirement found to be outdated relative to current practice shall be revised, and any platform, framework, or language that no longer satisfies the minimum traits above shall be flagged as non-approved, with a documented migration path or compensating controls for systems still running on

it, so that the guideline remains current and effective.

2. 2. Test Requirements and Reporting Formats

The test requirements and reporting formats section of the existing guideline shall be assessed and updated to ensure that the types of tests conducted, and the frequency of testing, remain effective at identifying and mitigating security risks. The guideline shall specify the types of tests that must be conducted, including but not limited to penetration testing, vulnerability assessments, code reviews, and security configuration reviews, together with the minimum frequency of each. Testing shall follow recognized methodologies, including NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) and, for web applications, the OWASP Web Security Testing Guide (WSTG):

Test Type	Purpose	Minimum Frequency
Penetration Testing	Simulate real-world attacks against running systems to identify exploitable vulnerabilities.	Annually, and before major releases
Vulnerability Assessment	Systematically scan infrastructure and applications for known vulnerabilities and misconfigurations.	Quarterly
Code Review	Identify insecure coding patterns, logic flaws, and injection points before deployment.	Every release
Security Configuration Review	Verify server, network, and platform configurations against recognized hardening baselines such as the CIS Benchmarks.	Semi-annually

For each test type, the guideline shall specify the data that needs to be captured and reported. At minimum, every test report shall record:

- The scope tested and the methodology and tools used to conduct the test.
- Each finding classified by severity, together with the evidence supporting it and its likelihood of exploitation.
- Recommended remediation for each finding and the party responsible for implementing it.
- A remediation deadline proportional to severity, and the current status of any previously reported finding.

Severity shall be assigned consistently using the Common Vulnerability Scoring System (CVSS v3.1 or later); the qualitative scale below maps to CVSS base-score bands and anchors the expected remediation timeframe:

Severity	Typical Criteria
Critical	Directly exploitable; results in full system or data compromise.
High	Exploitable with some effort; significant data or access exposure.
Medium	Exploitable under specific conditions; limited impact.
Low	Minor weakness; requires additional factors to exploit.

The guideline shall also define the frequency of reporting to project stakeholders, distinguishing between per-test reports issued immediately after each test and periodic consolidated summaries that track outstanding findings over time in a central register maintained by ICTP. Any test type, testing frequency, or reporting format found to be outdated or ineffective at identifying and mitigating security risk shall be updated or replaced with a more effective method.

3. 3. Metrics, Criteria, and Models for Software System Testing

The metrics, criteria, and models section of the existing guideline shall be assessed and updated to

ensure that the metrics and models used to evaluate the security preparedness of an application remain effective. This involves reviewing the metrics and models currently in use and updating them based on changes in technology and security practices.

The guideline shall specify criteria and models such as:

- Severity- and risk-based scoring criteria that classify each finding by exploitability and potential impact, so that remediation effort can be prioritized consistently across systems.
- Quantitative readiness metrics, for example the proportion of high-severity findings remediated before go-live, the number of outstanding findings by age, and the coverage of automated security testing across the codebase.
- A security maturity model — aligned with an established framework such as OWASP SAMM or BSIMM — that classifies each system's overall preparedness level, so that systems below the minimum acceptable level are held back from production release until remediated.
- A structured threat-modeling exercise, using an established methodology such as STRIDE, conducted at design time for systems handling sensitive data, used to identify likely attack paths before testing begins rather than relying solely on post-build testing.

The security maturity levels used to classify systems, and the minimum level required before production go-live, shall be defined explicitly.

Any metric, criterion, or model found to be outdated or ineffective at identifying and mitigating security risks shall be updated or replaced with a more effective method, so that the guideline remains a reliable basis for go/no-go deployment decisions.

4. 4. Authentication and Authorization Protocols Recommendation

The authentication and authorization protocols section of the existing guideline shall be assessed and updated to ensure that the protocols used in any system remain effective at protecting against unauthorized access. The guideline shall recognize the criticality of the system in question and recommend standards to be followed for authentication and authorization accordingly, with stronger controls required as system criticality increases. At minimum, the guideline shall recommend:

- Federated, token-based authentication protocols based on open standards such as OAuth 2.0, OpenID Connect (OIDC), and SAML 2.0, for user-facing and API authentication, in preference to custom-built authentication logic.
- Mandatory multi-factor authentication for any administrative, privileged, or system-administrator-level access, regardless of the system's overall criticality tier.
- A minimum password policy aligned with NIST SP 800-63B (sufficient minimum length, screening of new passwords against known-breached password lists, and rotation-on-compromise rather than arbitrary periodic rotation) for any system relying on password-based authentication.
- Defined session and token lifetimes, with shorter lifetimes and mandatory re-authentication for higher-privilege sessions, and automatic session termination after a period of inactivity.

The authorization protocols shall be defined in the guideline for multiple general access tiers, so that access rights are granted according to role rather than by default.

The guideline shall also recognize the nature of the information being accessed and the corresponding authorization requirements, such that access to personal, financial, or otherwise sensitive information is subject to stricter authentication, approval, and logging requirements than access to purely public information. Any authentication or authorization protocol found to be outdated or ineffective against current attack techniques shall be updated or replaced with a more effective method.

5. 5. Production Deployment Security

The production deployment security section of the existing guideline shall be assessed and updated to ensure that the set of standard allowed protocols and recommended security measures remain effective. The guideline shall provide standard requirements across the following areas:

Public-facing component security: internet-facing components shall be restricted to a minimal, explicitly allowed set of protocols and ports, unnecessary services and default accounts shall be disabled, and administrative interfaces shall not be directly exposed to the public internet.

- Only protocols required for the service's function shall be permitted at the network boundary, with all other inbound traffic denied by default.
- Default credentials, sample content, and diagnostic or debug endpoints shall be removed before go-live.

Web application firewall: public-facing web applications shall sit behind a web application firewall configured to detect and block common attack patterns (using, for example, the OWASP Core Rule Set as a baseline), with rule sets kept current and periodically reviewed.

- Web application firewall rule sets shall be tuned to the specific application rather than left at generic defaults, and shall be reviewed whenever the application changes significantly.

Software-based networking component security: load balancers, reverse proxies, virtual networks, and API gateways shall be configured according to documented hardening baselines derived from recognized standards such as the CIS Benchmarks, with network segmentation separating public-facing components from internal application and data components.

- Management interfaces for networking components shall be reachable only from a restricted, internal administrative network, never directly from the public internet.
- Traffic between network segments shall be restricted by explicit rules rather than broad allow-all rules, so that a compromise of one segment does not automatically grant access to others.

High-availability assurance architecture: systems shall be deployed with a level of redundancy and failover capability appropriate to their criticality, together with documented backup and restore procedures and a defined recovery objective, so that a single component failure does not result in extended service outage or data loss.

- Backup and restore procedures shall be tested periodically, not only documented, so that recovery is proven to work rather than assumed.
- Critical systems shall have a documented failover procedure specifying how traffic is redirected if a primary component becomes unavailable.

Any allowed protocol or recommended security measure found to be outdated or ineffective against current threats shall be updated or replaced with a more effective method, so that the guideline continues to protect systems during and after production deployment.

6. 6. Data Security

The data security section of the existing guideline shall be assessed and updated to ensure that the different nature of data aggregated and stored by provincial systems continues to be protected effectively. Based on the sensitivity of the information stored, and consistent with a recognized information-classification framework such as ISO/IEC 27001 and any applicable data-protection legislation, the guideline shall specify different data protection, encryption, and storage requirements, as summarized below:

Data Sensitivity	Illustrative Examples	Protection / Encryption / Storage Requirement
Public	Published notices, open datasets.	Integrity protection only; no confidentiality

Data Sensitivity	Illustrative Examples	Protection / Encryption / Storage Requirement
		requirement.
Internal	Internal reports, non-sensitive operational data.	Restricted to authenticated staff; encrypted in transit.
Confidential	Citizen personal data, employee records.	Encrypted at rest and in transit; access logging required.
Highly Sensitive	National identity data, financial or legal records.	Encrypted at rest and in transit, with restricted key access, strict access approval, and full audit trail retention.

In addition to the classification tiers above, the guideline shall specify the following baseline requirements applicable across all Confidential and Highly Sensitive data, with encryption implemented using current recognized algorithms (for example, AES-256 for data at rest and TLS 1.2 or higher for data in transit):

- A documented key-management procedure, aligned with NIST SP 800-57, covering how encryption keys are generated, rotated, and revoked, so that keys are not left unmanaged indefinitely.
- Defined data-retention periods and a secure-disposal procedure for data that has passed its retention period, rather than indefinite retention by default.
- Backups of Confidential and Highly Sensitive data shall themselves be encrypted and access-controlled, so that a backup copy does not become a weaker point of exposure than the live system.

Any data protection, encryption, or storage measure found to be outdated or ineffective at protecting sensitive data, given the classification above, shall be updated or replaced with a more effective method, so that the guideline remains effective at protecting sensitive information throughout its lifecycle, from collection through storage, processing, and eventual disposal.

Section II: Security Audit of Existing Systems

7. Penetration Testing

1. Dependency Vulnerability Testing

This testing approach assumes that at least one third-party module, framework, library, or piece of code has been used in the production build of the system, which requires a security audit of those modules. The security engineer must verify and report on the following:

- Whether modules that provide security services, such as firewalls or authentication servers, fail during automated testing.
- Whether there are known security vulnerabilities — for example, CVEs recorded in the National Vulnerability Database (NVD) — in the registries corresponding to the modules in use, consistent with OWASP Top 10 A06 (Vulnerable and Outdated Components).
- Whether all modules are properly updated to the latest security patch available for that module.
- Whether the specific version of each module in use is pinned and documented, so that the exact set of in-use dependencies is known rather than inferred.
- Whether vulnerable modules are direct dependencies of the system or are pulled in indirectly through another dependency, since indirect (transitive) dependencies are often overlooked.

- Whether a software bill of materials in a standard format such as SPDX or CycloneDX, or an equivalent dependency inventory, exists and matches what is actually deployed in production.

2. Client Facing Components Security Testing

During this type of testing, a security engineer works only with the user interface and checks to produce unwanted results. This test involves entering incorrect input sequences or performing malformed POST requests. This testing shall follow the OWASP Web Security Testing Guide (WSTG) and verify the application against the OWASP Application Security Verification Standard (ASVS), covering the OWASP Top 10 web application risks. Examples of testing activity include, but are not limited to:

- Using escape characters to observe how the application handles unexpected special characters within input fields.
- Using long strings to test for buffer-handling issues and input-length validation failures.
- Experimenting with remote code injection and/or remote code execution against inputs processed by the system.
- Performing SQL injection against forms, query parameters, and any interface that interacts with a database.
- Attempting user-controlled cache bypassing to determine whether cached responses can be manipulated to expose data.
- Testing for cross-site scripting by attempting to inject scriptable content that executes in another user's browser.
- Attempting cross-site request forgery to determine whether state-changing actions can be triggered without the user's consent.
- Testing file-upload functionality with disguised or mismatched file types to determine whether the system correctly validates uploaded content rather than trusting the declared file extension.
- Testing for excessive request rates and repeated failed login attempts, to determine whether rate-limiting or account lock-out protections are in place against brute-force attempts.
- Manipulating or tampering with authentication tokens and session identifiers to determine whether the system correctly detects and rejects altered or forged tokens.
- Testing for open redirects and unvalidated URL parameters that could be used to redirect users to an unintended destination.

3. Design and Implementation Vulnerability Testing

This testing is carried out manually to evaluate whether any unintentional loose ends were left behind from the software development process. This involves looking for the following:

- Demo user accounts that were never removed or disabled after development or testing concluded.
- Privilege leaks, where a user or process retains more access than its role requires.
- Open and unsecured ports that are exposed but not required for the system to function.
- Gaps in SSL coverage, where some endpoints or connections fall outside encrypted communication.
- Intertwined debug logic left active within the production build, including verbose error messages that reveal internal file paths, stack traces, or configuration details.

- Time-of-check to time-of-use (TOCTOU) issues, where a condition checked at one point may no longer hold true by the time it is acted upon.
- Hard-coded credentials, API keys, or secrets embedded directly in source code or configuration files rather than stored in a secrets manager.
- Version-control or configuration artifacts inadvertently left accessible on the production server, which can reveal source code history or environment configuration.
- Insecure direct object references, where a user can access another user's data simply by altering an identifier in a request, without a proper authorization check on the server side.

Section III: Governance and Reporting

This section establishes the governance structure for the engagement described in Sections I and II. It defines the roles of the parties, the reporting lines the Consultant shall follow, and the allocation of responsibilities between the Consultant, ICTP, and the owners of the systems under audit.

8. 1. Definitions and Roles

The following terms and roles apply throughout this document:

ICTP: the [Information and Communication Technology authority — full legal name to be confirmed] that owns this engagement, maintains the central findings register referred to in Section I.2, and approves the updated guideline and the outcomes of the security audit.

The Consultant: the firm or individual engaged to assess and update the information security guideline under Section I and to perform the security audit of existing systems under Section II.

Security Engineer: the Consultant's personnel who carry out the penetration-testing and audit activities described in Section II.

System Owner: the provincial entity accountable for a given system under audit, responsible for providing access to that system and for implementing approved remediation.

9. 2. Reporting Lines

The Consultant shall report to ICTP throughout the engagement in accordance with the following:

Point of contact: the Consultant shall report to [ICTP engagement lead / named point of contact — to be confirmed], who serves as the single point of contact for the engagement and the recipient of all deliverables and reports.

Routine reporting: per-test reports shall be issued to ICTP immediately after each test, and periodic consolidated summaries shall be provided [monthly / at an interval to be confirmed], consistent with the central findings register described in Section I.2.

Critical-finding escalation: any finding rated Critical under CVSS that affects a live system processing Confidential or Highly Sensitive data shall be escalated to ICTP immediately on discovery, and in any event within [X hours], ahead of the routine reporting cycle.

Governance checkpoints: ICTP shall convene a governance checkpoint at [each milestone / interval to be confirmed] to review progress, outstanding findings, and go/no-go decisions on production release as described in Section I.3.

10.

11.3. Responsibilities

Responsibilities are allocated between the parties as follows:

Party	Responsibilities
ICTP	Owns the engagement; authorizes testing and approves access; maintains the central findings register; reviews and approves the updated guideline; and makes final go/no-go and sign-off decisions on production release.
The Consultant	Applies the methodologies and standards set out in Sections I and II; conducts testing and produces reports; classifies and prioritizes findings using CVSS; recommends remediation; and safeguards all data accessed during the engagement.
System Owner	Provides timely access to systems and environments; supplies required documentation such as software bills of materials and architecture diagrams; and implements approved remediation within the deadlines set by severity.

Any governance or reporting arrangement found to be ineffective in practice shall be updated during the engagement so that oversight of the guideline update and the security audit remains clear and accountable.

Key Manpower, Qualification and Experiences required for Personnel:

Specialist	Qualifications and Experience required	Person-Days (incl. Field Work)
Team Leader	Masters in Computer Science (or equivalent) or higher. Thorough understanding of the Software Development Lifecycle. At least 5 years of professional experience in implementation/evaluation or management of large scale systems.	2 months
Deputy Team Leader	Masters in Computer Science or in similar discipline . Thorough understanding of the Software Development Lifecycle. At least 3 years of experience in implementation, evaluation of large scale websystems.	2 months
Cloud Engineer (Security)	Bachelors in Computer Engineering or Information Systems or in similar discipline. Experienced in Designing Highly Available Cloud Architecture with proven track record. Experience in implementation of latest security measures for safe keeping of infrastructure resources.	9 months
Software Engineer (Security)	Bachelors in Computer Engineering or Information Systems or in similar discipline. Experience in implementation of system testing and security measures for safe keeping of website from malicious attacks. 1+ years of experience in design and development of enterprise scale applications.	9 months
Software Engineer	Bachelors in Computer Engineering or Information Systems or in similar discipline. Has Experience building back-end Development of the website and its systems. Strong command in web security application concepts is a plus.	2 months
Technical Documentation Writer	Bachelors in Computer Science/Engineering or Equivalent . Strong command over English Language. At Least 2 years of experience in technical documentation.	2 month

Delivery Requirement

1. **Deliverables for Section I:**

The consultant should deliver:
An assessment and updated version of the information systems security guideline for software development in Lumbini Province.

2. **Deliverable for Section II:**

2.1 The Security Test Report highlighting the following :

a) Scope of Tests
b) Assumption for Test Execution
c) Test Completion/Success Criteria
d) Testing Strategy/Tools
e) Measurement and Metrics Used
f) Threat tree
g) Static/Dynamic Testing Model
h) Penetration Testing for (Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), SQL injection, Code Injection attack, Cookies poisoning, Row Hammer possibilities, Session management vulnerabilities, Dirty CoW possibilities on implementation platform, Buffer Overflows, RCE, etc.)
i) Result of the vulnerabilities found and measures recommended to mitigate them classified according to the titles stated above

2.2 Recommendations

- A list of recommendations (if any) to mitigate/reduce the impact of discovered vulnerabilities/threats.
- At least 25 Software applications/websites must be audited, and report should be submitted accordingly.
- All the requests for audit issued by ICTP must be fulfilled and report should be submitted accordingly

Developer Company/Firm Qualification

The consulting firm to be selected through the procurement procedure should meet following criteria:

1. The developer company/firm must be a legal entity registered in Nepal.
2. The developer company/firm must have tax clearance up to the fiscal year, according to Government of Nepal.
3. The developer company/firm must not be blacklisted by any agencies of Government of Nepal.
4. Consulting firm must have at least 1 year of experience in relevant field.

Time Schedule

The consultant shall commence the work from the date of signing of the agreement and should complete within the period mentioned in the agreement. The duration of the assignment shall be till end of fiscal year from work order date.

Mode of Payment

The payment for the amounts claimed upon submission of the reports mentioned above based on the prevailing laws and rules/regulation of the Government of Nepal. As per agreement, the developer can claim the payment in a single installment after submission and acceptance of the Final Report(s) or in installment as follows:

- First installment, 20% of the total amount (excluding reimbursable costs and taxes).
- Second installment, 50% of the total amount (excluding reimbursable costs and taxes) upon submission and acceptance of the updated information system security guideline.
- Final and remaining 30% of the total amount upon final submission of the project.

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 ***(for National consulting firm only)***	
Tax Clearance/Tax Return Submission/Letter of Time Extension for Tax Return Submission ***2082/83 (for National consulting firm only)***	
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		
Qualification of Key Experts	*As per ToR*	***40%***
Experience of Key Experts	*As per ToR*	
B. Experience		

General Experience of consulting firm	*Should have at least 3 years of experience in the field of software development/support and/or IT consulting*	***50%***
Specific experience of consulting firm within last 7 years.	*Should have at least 3 years of experience in Information Security System Audit of Large scale systems*	
Similar Geographical experience of consulting firm	*In order to show geographical competence, provide the details required as per the attached format*	
C. Capacity		
Financial Capacity[1]	*Average annual turnover of best three years out of last seven years should be at least NRs. 2.5 Million*	***10%***

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.

[1] *Average turnover required shall not exceed 150% of cost estimate*

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]

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

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):

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)
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

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.)

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)