

PROCUREMENT OF NON-CONSULTING SERVICES

Request for Quotations For

Hiring of a Firm for Vulnerability Assessment & Penetration Testing (VAPT) and ISO 27001 Controls Assessment of the Student Attendance Monitoring & Redress System (SAMRS)

September 2026

PROCUREMENT OF NON-CONSULTING SERVICES

Request for Quotations

For

Hiring of a Firm for Vulnerability Assessment & Penetration Testing (VAPT) and ISO 27001 Controls Assessment of the Student Attendance Monitoring & Redress System (SAMRS)

Ref No: PK-RSU-SINDH-570306-NC-RFQ

Project: Sindh Early Learning Enhancement through Classroom Transformation SELECT

Purchaser: Sindh Early Learning Enhancement through Classroom Transformation (SELECT), School Education & Literacy Department Govt of Sindh.

Country: Pakistan

Issued on: Sep 15th, 2026

Table of Contents

Request for Quotations.....	4
ANNEX A: Purchaser's Requirements	9
ANNEX B: Quotation Forms.....	25
ANNEX C: Contract Forms	28

Request for Quotations

Procurement of Firm for Vulnerability Assessment & Penetration Testing (VAPT) and ISO 27001 Controls Assessment of the Student Attendance Monitoring & Redress System (SAMRS)

RFQ Ref No: PK-RSU-SINDH-570306-NC-RFQ

RFQ Date: September 15th, 2026

To: _____[insert Supplier's name]

Dear [insert name of Supplier's representative]:

Request for Quotation (RFQ)

This RFQ is for the procurement of non-consulting services for the **Vulnerability Assessment and Penetration Testing (VAPT) and ISO/IEC 27001:2022 ISMS Readiness Assessment of the Student Attendance Monitoring and Redress System (SAMRS)**, developed under Component-III of the SELECT Project and operational across all districts of Sindh.

The School Education & Literacy Department (SE&LD), Government of Sindh (hereinafter called "Borrower") has received financing from the World Bank toward the cost of the SELECT Project and intends to apply part of the proceeds toward payments under the contract for the procurement of these non-consulting services.

The Procuring Agency now invites quotations from eligible and qualified information-security firms meeting the eligibility and qualification requirements of this RFQ. The assignment shall be awarded as a single lot; partial quotations shall not be accepted

Requisite Documents

The service provider who opts to offer the services shall submit a quotation in the form included in this RFQ, together with the documentary evidence listed against evaluation criteria E-01 to E-08. The firm must be registered with SECP or the Registrar of Firms, hold a valid NTN, and be a registered taxpayer with the Federal Board of Revenue and the Sindh Revenue Board.

Validity of offers

The offers shall be valid for next **(90) days** from the date of submission

Quoted Price

Prices shall be quoted in the following manner:

- (a) For Non-Consulting Services:
- (b) If known, any Purchaser's Country sales tax and other taxes which will be payable on the Services if the Contract is awarded to the Service Provider; and For Related Services (according to RFQ Document), **whenever such Related Services are specified in the Schedule of Requirements**, the price of each segment comprising the Related Services (inclusive of any applicable taxes).

The contractual unit prices shall be fixed during the Service Provider's performance of the Contract and not subject to adjustment.

Clarifications

Any clarification request regarding this RFQ may be sent in writing to Mr. Junaid Hameed Samo, Chief Program Manager (CPM) RSU at junaidcpmsu@gmail.com or at Procurement Section, pmiuselect.seld@gmail.com before 28th September, 2026, 16:00 PST. The Purchaser will forward copies of its response to all Suppliers including a description of the inquiry but without identifying its source.

Submission of Quotations

- a. Quotations are to be submitted in the form attached at Annex-B **by courier or by hand to the address given below.**
- b. The deadline for submission of Quotations is 02nd October, 2026, 16:00 PST.
- c. The address for submission of Quotations is:

Attention: **Mr. Junaid Hameed Samo, Chief Program Manager (CPM)**

Address: Sindh Early Learning Enhancement through Classroom Transformation (SELECT) RSU, 47-E/1, 48th Street, Block # 06, PECHS, Near Nursery, Shahrah-e-Faisal, Karachi, Pakistan. pmiuselect.seld@gmail.com

Note: Bid submission by email will not be accepted

Opening of Quotations

Quotations will be opened by the Purchaser's representatives immediately after the deadline for the submission of Quotations.

Evaluation of Quotations

Quotations will be evaluated to ensure compliance with the requirements of the RFQ as per Schedule.

The lowest evaluated price & scored advantage will be determined after correcting any arithmetic errors and other specified adjustments, if any.

Quotation will be evaluated for the whole lot/package under this RFQ. If a Price Schedule shows items listed but not priced, their prices shall be assumed to be included in the prices of other items. An item not listed in the Price Schedule shall be assumed not included in the Quotation, and provided that the Quotation is substantially responsive, the average of the item price as Quoted by substantially responsive Suppliers will be added to the Quoted Price and the equivalent total price of the Quotation so determined will be used for price comparison.

Contract Award

The Contract will be awarded to the Supplier/s who:

- a. Offers the lowest evaluated price/s,
- b. Technically compliant quotation.
- c. Scored-advantage methodology

In accordance with the Evaluation of Quotations above.

The Purchaser shall invite by the quickest means the successful Supplier for any discussion/ negotiation that may be needed to conclude the contract or otherwise for contract signature.

The Purchaser shall communicate by the quickest means with the other Suppliers on its contract award decision. An unsuccessful supplier may request clarifications as to why its quotation was not determined to be successful. The Purchaser will address this request within a reasonable time.

The Purchaser shall publish a contract award notice on its website with free access, if available or in a newspaper of national circulation or UNDB online as soon as practicable thereafter. The information shall include the name of the successful Supplier, the Contract Price, the Contract duration, summary of its scope and the names of the Suppliers and their quoted and evaluated prices.

Fraud and Corruption

The Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in the attachment to the Contract Conditions to Fraud and Corruption (Attachment A).

In further pursuance of this policy, the supplier shall permit and shall cause their agents (where declared or not), subcontractors, sub consultants, service providers, suppliers, and personnel, to permit the Bank to inspect all accounts, records and other documents relating to the RFQ and contract performance (in the case of award), and to have them audited by auditors appointed by the Bank.

On behalf of the Purchaser:

Signature:

Name: Mr. Junaid Hameed Samo

Title/position: Chief Program Manager (RSU)

Attachments:

Annex A: Purchaser's Requirements

Annex B: Quotation Form

Annex C: Contract Forms

Evaluation of Quotations

Evaluation Criteria:

Firms must satisfy the following mandatory eligibility criteria. Bids or technical proposals from firms not meeting these requirements shall be rejected at the technical evaluation stage.

S. No.	Criterion	Requirement
E-01	Legal Registration	Registered as a company/firm in Pakistan (SECP or Registrar of Firms) with a valid NTN and Sales Tax/GST registration (FBR/SRB).
E-02	Line Business of	Core business must include information/cybersecurity services, including VAPT, penetration testing, security auditing, or ISO/IEC 27001 consultancy, evidenced by registration documents or company profile.
E-03	Years in Operation	Minimum five (5) years of continuous operation in cybersecurity/VAPT services as of the bid or technical proposal submission date.
E-04	Relevant Experience	Minimum three (3) successfully completed VAPT engagements and at least one (1) successfully completed ISO/IEC 27001 ISMS gap assessment, readiness assessment, or implementation-support engagement during the preceding five (5) years. At least one engagement shall have been undertaken for a public-sector, education-sector, or similarly regulated organization. Completion certificates, contracts, purchase orders, or client reference letters shall be submitted as evidence.
E-05	Certifications (Organizational & Personnel)	ISO/IEC 27001 certification of the bidder's own Information Security Management System (ISMS) shall not be a mandatory eligibility requirement and shall not constitute a basis for rejection of the quotation. Where available, the bidder may submit evidence of its organizational ISO/IEC 27001 certification as supporting information demonstrating its internal information-security governance arrangements. Such organizational certification shall not substitute for the mandatory personnel certification requirements specified below. The bidder shall nominate: (a) an ISO/IEC 27001 Assessment Lead holding a valid and independently verifiable ISO/IEC 27001 Lead Auditor certification; and (b) a Penetration Testing Lead holding a valid OSCP, CREST Registered Tester, CREST Certified Tester, GPEN, PNPT, or equivalent relevant certification. The nominated personnel shall personally lead the respective workstreams. Any substitution after award shall require prior written approval of PMIU, and the proposed replacement shall possess qualifications and experience equal to or greater than those of the originally nominated personnel.

S. No.	Criterion	Requirement
E-06	Legal Standing	Not currently blacklisted or debarred by PPRA, any Government of Sindh/Pakistan department, or any donor-funded project. An affidavit/declaration to this effect must be submitted with the bid or technical proposal.
E-07	Local Presence	Firm must have an operational office within Pakistan capable of supporting on-site activities in Sindh (Karachi) for the duration of the engagement.
E-08	Conflict of Interest	The firm (or its personnel) must not have been involved in the design, development, or maintenance of SAMRS or any related SELECT Project system, to preserve independence of the assessment.

The firm shall submit documentary evidence, including registration and tax certificates, client completion evidence or reference letters, personnel certifications, and declarations, against each eligibility criterion with the bid or technical proposal. D-01 is a post-award inception deliverable and shall not be treated as part of the bid or technical proposal submission.

ANNEX A: Purchaser's Requirement

TERMS OF REFERENCE (TORs)

Firm for Vulnerability Assessment & Penetration Testing (VAPT) and ISO 27001 Controls Assessment of the Student Attendance Monitoring & Redress System (SAMRS)

1. Background

The Student Attendance Monitoring and Redress System (SAMRS) is a digital platform developed under Component-III of the SELECT Project, operational across all districts of Sindh. It is used by school staff, District Education Officers, Taluka Education Officers, and provincial users to monitor student attendance, identify at-risk students, and trigger redressal workflows. SAMRS processes sensitive student data including B-Form numbers, parent CNICs, attendance records, and risk profiles.

The SAMRS platform comprises:

- An Android mobile application (v3.0) for offline-first attendance marking, student enrolment, and redressal actions.
- Two web applications: the core SAMRS administrative portal and a separate CPD web dashboard hosted on a dedicated SAMRS subdomain. The CPD dashboard includes the C1 Dashboard, Classroom Observation (CRO), Item Bank, and Formative Assessment (FA) modules.
- A central SAMRS REST API service with thirty-nine (39) currently identified API endpoints, including twenty-one (21) endpoints used by the SAMRS Mobile Application and controlled API interfaces used for authorized external data exchange.
- A central MySQL 8.0 database server accessible only over an internal LAN, with no direct public internet exposure.
- API-based integration points with external systems. External systems exchange data with SAMRS only through controlled API interfaces; no direct database access to those external systems is included in the integration scope.

PMIU SELECT RSU is seeking a qualified and independent information-security firm to conduct a combined engagement comprising: (a) a comprehensive Vulnerability Assessment and Penetration Testing exercise; and (b) an ISO/IEC 27001:2022 Information Security Management System readiness and controls gap assessment for the defined SAMRS scope. The engagement is not an ISO/IEC 27001 certification audit. Any subsequent formal certification shall be undertaken separately by an accredited Certification Body independent of this engagement.

2. Objectives

VAPT Objectives

- Identify, evaluate, and document security vulnerabilities across the SAMRS web application, CPD web dashboard, Android mobile application, REST API service and endpoints, database layer, external API integrations, and server infrastructure.
- Conduct active penetration testing to determine exploitability and real-world impact, using CVSS v4.0 scoring throughout.
- Issue a signed clearance letter confirming all Critical and High severity findings have been fully remediated.
- Establish a repeatable VAPT baseline for future periodic review cycles.

ISO/IEC 27001:2022 ISMS Readiness Assessment Objectives

- Assess the defined SAMRS ISMS scope against the applicable requirements of ISO/IEC 27001:2022 Clauses 4-10 and determine the applicability and implementation status of Annex A controls through review of the SAMRS risk assessment, risk treatment plan, and Statement of Applicability. The 23 control areas listed in Section 3.3 shall constitute minimum mandatory focus areas and shall not limit assessment of other requirements or controls applicable to the defined scope.
- Identify control gaps, classify them by priority level, and develop actionable remediation recommendations tailored to SAMRS's operational environment.
- Produce a detailed controls assessment report for the technical team, documenting the baseline, identified gaps, and recommended remediation actions.
- After the SAMRS technical team implements the recommended actions, conduct a re-evaluation to verify the implementation status of corrective actions, document residual gaps and risks, and assess readiness to proceed to an accredited certification audit.
- Issue a firm-signed ISO/IEC 27001 Readiness Assessment Opinion stating the assessment scope, criteria, evidence reviewed, exclusions, unresolved gaps, and the firm's conclusion regarding readiness to proceed to an accredited certification audit. The opinion shall not be represented as formal ISO/IEC 27001 certification and shall not use certification marks or logos.

3. Scope of Work

3.1 VAPT In-Scope Systems

The following systems and components are in scope for penetration testing:

Component	Testing Focus
SAMRS Web Application	Authentication, session management, input validation, XSS, SQL injection, CSRF, security headers, role-based access controls, and OWASP Top 10, latest stable release at contract signing
CPD Web Application / Dashboard	Security assessment of the separate CPD web dashboard and its C1 Dashboard, Classroom Observation (CRO), Item Bank, and Formative Assessment (FA) modules, including authentication, authorization, session management, input validation, access controls, application security, and module-specific data handling.
SAMRS Mobile Application	API communication, offline data storage, sync security, certificate handling, authentication mechanisms (PIN/OTP/biometric); root detection, emulator detection, certificate pinning bypass, reverse engineering resistance, APK hardening, local SQLite encryption, Android KeyStore validation, secure clipboard handling, screenshot protection, intent hijacking, deep-link security, exported activity review
SAMRS REST API Service & Endpoints	Assessment of the central SAMRS REST API service and its currently identified thirty-nine (39) endpoints, including twenty-one (21) endpoints used by the SAMRS Mobile Application; OWASP API Security Top 10, rate limiting, token validation, object-level authorization, JWT validation, OAuth misuse, Broken Object Level Authorization (BOLA), Broken Function Level Authorization (BFLA), mass assignment, and integration endpoint security.

Component	Testing Focus
Database Security	Access controls, privilege management, audit logging, encryption at rest, secure configuration, database hardening, and vulnerability validation for the shared SAMRS/CPD MySQL database environment, including logical separation of module-specific tables through table prefixes.
Network & Infrastructure	Open ports, service exposure, TLS configuration, server hardening, and configuration review for all approved in-scope server hosts. The indicative server count is three (3): Primary, Secondary, and Disaster Recovery (DR). The authoritative host and service inventory shall be validated and confirmed in D-01.
External API Integrations	Security assessment of the SAMRS-controlled API interfaces used for external data exchange: Frames (bi-directional), Sindh School Management Information System (SSMIS) (uni-directional/inbound to SAMRS), and Sindh Education Management Information System (SEMIS) (uni-directional/inbound to SAMRS). Testing covers authentication, authorization, input/output validation, token handling, rate limiting, error handling, logging, and data-exposure controls on the SAMRS-controlled side.
Authentication & Session Management (Web, API, Mobile)	Password reset workflow, account enumeration, account lockout, MFA bypass, session fixation, refresh-token handling, JWT manipulation, token replay, concurrent session management

3.1.1 Indicative Asset Schedule

For bid sizing and proposal preparation, the following indicative asset counts are provided based on the current SAMRS/CPD environment. These counts represent the presently identified scope and shall be validated by the selected firm during D-01. Any material variance shall be documented and agreed with PMIU through the approved scope-control process.

Item	Estimated Count	Indicative Scope / Notes
Web applications / dashboards	2	1. Core SAMRS web application and a separate CPD web dashboard hosted on a dedicated SAMRS subdomain. 2. The CPD dashboard includes four internal functional modules: C1 Dashboard, Classroom Observation (CRO), Item Bank, and Formative Assessment (FA).
Mobile application	1	SAMRS Android Mobile Application supporting attendance, enrolment, synchronization, and related field operations. The mobile application communicates with the SAMRS backend through authenticated API endpoints.
REST API service	1	Central SAMRS REST API service supporting the SAMRS Mobile Application and authorized data exchange with external systems.
API endpoints	39	Total currently identified SAMRS API endpoints, including twenty-one (21) endpoints used by the SAMRS Mobile Application. Final route/endpoint enumeration shall be validated during D-01.
External API integrations	3	Bi-directional: a. Frames Uni-directional/inbound to SAMRS: a. Sindh School Management Information System (SSMIS) b. Sindh Education Management Information System (SEMIS) External systems communicate with SAMRS through controlled API interfaces.
Servers	3	Primary, Secondary, and Disaster Recovery (DR). Final host, service, database placement, and role mapping shall be validated during D-01.

Note: The above schedule is indicative for procurement sizing and pricing purposes. CRO and Formative Assessment (FA) are internal components of the CPD application and are not counted as external integrations. The SAMRS Mobile Application is likewise treated as an in-scope application component rather than an external integration. D-01 shall confirm the authoritative asset inventory, API endpoint enumeration, external integration directionality, server/service mapping, database placement, and any approved scope adjustments before active testing commences.

Note: Testing of external integrations shall be limited to the SAMRS-controlled side of the API interfaces, including authentication, authorization, request/response validation, token handling, rate limiting, error handling, logging, and data-exposure controls. External systems currently in scope are Frames (bi-directional), SSMIS (uni-directional/inbound to SAMRS), and SEMIS (uni-directional/inbound to SAMRS). No active testing shall be conducted against the databases, servers, file systems, administrative interfaces, or other infrastructure of an external system unless PMIU provides written authorization from the relevant system owner. In the absence of such authorization, the firm shall document the external-system limitation in its reports.

The engagement shall use a predominantly grey-box testing approach, supplemented by white-box review where source-code or configuration review is required. PMIU shall provide, subject to applicable confidentiality controls:

- staging URLs, approved IP addresses, and an authoritative in-scope asset inventory;
- role-based test accounts covering relevant SAMRS and CPD user roles, including school, Taluka, district, provincial, administrative, and other applicable roles;
- API specifications, integration documentation, and test credentials;
- Android APK/AAB files and relevant build information;
- supervised read-only source-code or repository access for agreed SAST and secure-code review activities;
- architecture diagrams, data-flow diagrams, and trust-boundary information;
- synthetic or anonymized test data; and
- designated technical and emergency contacts.

All scope changes shall require written approval through a documented change-control process. The indicative asset schedule in Section 3.1.1 shall be used for bid sizing and proposal preparation. During D-01, the firm shall validate the two web applications, mobile application, REST API service, endpoint enumeration, external API integration directionality, host/service mapping, and shared database placement, and shall document any material variance from the indicative counts for PMIU review and approval before testing.

3.2 VAPT - Out-of-Scope Items

Any system/item not listed in Section 3.1 is explicitly excluded unless written approval is obtained from the PMIU.

3.3 ISO/IEC 27001:2022 ISMS Readiness and Controls Assessment Scope

The firm shall conduct an ISMS readiness and controls gap assessment against the applicable requirements of ISO/IEC 27001:2022 Clauses 4-10 and Annex A. The following 23 SDL/operational control areas are minimum mandatory focus areas. The assessment shall determine the current implementation state, identify evidence-based gaps, evaluate associated risks, and provide prioritized corrective-action recommendations. The firm shall also review the SAMRS ISMS scope, risk assessment, risk treatment plan, and Statement of Applicability.

Category	ISO/IEC 27001:2022 Reference	Checklist Item	Assessment Tasks for Firm
Secure Design	A.8.25, A.8.26, A.8.27	Threat modelling & architecture review	Review system architecture diagram (VMs, app servers, DB, APIs, network zones); verify trust boundary documentation; assess threat model completeness.
Secure Design	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.5, A.8.26	Auth & access model review	Verify authentication framework (hashed passwords, MFA, secure sessions); assess RBAC and least privilege enforcement; test for privilege escalation paths.
Secure Design	A.5.12, A.5.13, A.5.34, A.8.10, A.8.11, A.8.12, A.8.24, A.8.26	Data flow & sensitive data classification	Review data flow diagram (user→app→DB); verify PII classification; confirm encryption in transit and at rest; assess B-Form/CNIC data handling controls. Assess PII exposure across the system; evaluate data minimisation practices; review data retention schedules; verify secure deletion procedures; assess export controls on sensitive data extracts; confirm logging of personal data access.
Secure Design	A.8.26, A.8.28, A.8.29	Input validation & API security design	Verify input-validation controls; assess XSS and SQL-injection prevention; review parameterized-query enforcement; evaluate file-upload restrictions; and assess security testing coverage for internet-facing interfaces and APIs.
Secure Coding	A.8.15, A.8.16	Logging, monitoring & traceability	Assess centralized logging implementation; verify audit-log completeness for security-relevant events; evaluate monitoring, alerting, access controls, retention, and log tamper protection.
Secure Coding	A.5.17, A.8.9, A.8.24, A.8.25, A.8.28	Secrets management	Confirm that credentials, keys, tokens, and other secrets are not hard-coded; verify approved environment- or vault-based secret storage; assess access controls, rotation, revocation, and cryptographic key-management practices.
Secure Coding	A.8.15, A.8.26, A.8.28	Error handling & debug configuration	Verify generic error messages in production; confirm debug mode is disabled; assess stack-trace and sensitive-information exposure; and review logging of security-relevant application errors.

Category	ISO/IEC 27001:2022 Reference	Checklist Item	Assessment Tasks for Firm
Dependencies	A.8.8	SCA & dependency management	Run SCA tool scan (e.g., Snyk, npm audit, or equivalent); identify vulnerable/deprecated libraries; verify lock files and official registry usage.
Environment	A.8.31	Dev/Test/Prod separation	Confirm environment isolation; verify no production data reuse in lower environments; review environment-specific configuration management.
Environment	A.8.4, A.8.9, A.8.25, A.8.31, A.8.32	CI/CD pipeline security	Assess CI/CD access controls (RBAC); verify vault-based secret storage; review pipeline approval gates; assess audit logging for build/deployment activities.
Code Review	A.8.25, A.8.28, A.8.32	Peer review & change management	Verify mandatory peer-review enforcement; assess direct-commit prevention; review secure-coding standards and change-approval procedures for production deployments.
Code Review / Testing	A.8.8, A.8.25, A.8.29	SAST & DAST scan results	Review SAST scan results (SonarQube, Semgrep, or equivalent); run DAST scan (OWASP ZAP, Burp, or equivalent) on staging; verify quality gates are blocking high/critical findings.
Testing	A.8.5, A.8.29	Auth & access control test results	Validate login flows, session handling, MFA, RBAC; conduct privilege escalation testing; verify test coverage documentation.
Deployment	A.8.31, A.8.32	Rollback & change control	Verify formal change request approval process; review rollback plan documentation; confirm rollback tested in staging.
Post-Deployment	A.5.24-A.5.28, A.8.15, A.8.16	Logging, monitoring & incident response	Assess centralized logging/monitoring setup (ELK, Datadog, Prometheus, or equivalent); review incident response documentation (lifecycle, roles, escalation paths, runbooks).
Organizational Controls	A.5.9, A.5.10, A.5.11	Asset management	Verify asset inventory (hardware, software, data, VMs) is maintained and current; confirm asset ownership assignment; review acceptable-use and return-of-assets procedures.

Category	ISO/IEC 27001:2022 Reference	Checklist Item	Assessment Tasks for Firm
Organizational Controls	A.6.1, A.6.2, A.6.3, A.6.4, A.6.5	HR security	Review screening/background-check procedures for personnel with system access; verify information-security responsibilities are included in terms and conditions of employment; assess awareness and disciplinary processes; and verify access revocation upon termination or change of role.
Organizational Controls	A.5.29, A.5.30	Business continuity	Review business continuity and disaster recovery plans for SAMRS; verify ICT readiness for business continuity; assess testing frequency and documented recovery time/point objectives.
Organizational Controls	A.8.13	Backup management	Verify backup schedule, retention, and encryption; confirm backup restoration testing is performed and documented; assess offline/offsite backup storage.
Organizational Controls	A.7.1, A.7.2, A.7.3, A.7.4	Physical security	Review physical access controls at the hosting/data center (badges, biometrics, visitor logs, CCTV); verify secure areas and equipment siting; assess monitoring of physical access events.
Organizational Controls	A.5.3, A.5.15, A.5.16, A.5.18, A.8.2, A.8.5	Access governance (provisioning, de-provisioning, periodic review, privileged access review, segregation of duties, shared accounts)	Verify formal user provisioning/de-provisioning workflow; confirm periodic (monthly) access reviews; assess privileged/admin access reviews; verify segregation of duties across roles; identify and review any shared/generic accounts.
Organizational Controls	ISO/IEC 27001:2022 Clauses 6.1.2 and 6.1.3; A.5.7	Risk management process	Review the documented information-security risk assessment and treatment methodology; verify that a risk register and risk treatment plan are maintained and updated; review the Statement of Applicability; and assess threat-intelligence sources feeding the risk process.

Category	ISO/IEC 27001:2022 Reference	Checklist Item	Assessment Tasks for Firm
Organizational Controls	A.5.31, A.5.32, A.5.34	Compliance & legal obligations	Verify identification of applicable legal, regulatory, and contractual requirements (data protection, government policy); review IP rights management; assess privacy/PII protection compliance for student and parent data.

The ISO/IEC 27001 readiness assessment shall be conducted through document review, interviews, sampling of records, observation of relevant processes, and supervised read-only review of applicable system configurations. Intrusive security testing shall be restricted to the approved staging environment. Where evidence relates to production operations, including backup records, access reviews, monitoring records, change records, incident records, and data-centre controls, the firm may review such evidence through supervised, read-only access without conducting exploitation or disruptive testing on production systems.

3.4 Gap Priority Classification

ISO/IEC 27001:2022 ISMS Readiness Gaps

All ISO/IEC 27001 readiness and control gaps shall be classified using the following priority framework:

Priority	Classification	Definition	Required Treatment
Priority 1	Critical readiness blocker	Absence or systemic failure of an applicable ISMS requirement or control that creates material security exposure or prevents a defensible readiness conclusion.	Immediate corrective action. Must be resolved, formally risk-treated, or explicitly identified in a qualified readiness opinion.
Priority 2	Major gap	Significant or widespread partial implementation that materially weakens the ISMS or control environment.	Corrective action should be completed before certification readiness, with progress and evidence tracked.
Priority 3	Minor gap	Isolated procedural, implementation, or documentation deficiency that does not represent a systemic control failure.	Address through the corrective-action plan and continual-improvement process.
Advisory	Improvement opportunity	Good-practice recommendation beyond the minimum readiness criteria.	Optional enhancement to be prioritized according to risk and available resources.

VAPT Severity Classification

Severity	CVSS v4.0 Base Score	Treatment Expectation	Target Timeline
Critical	9.0-10.0	Immediate containment and prioritized remediation.	Target closure within 7 calendar days.
High	7.0-8.9	Priority remediation based on exploitability and business impact.	Target closure within 15 calendar days.
Medium	4.0-6.9	Corrective action within the agreed remediation plan.	Normally within 30-60 calendar days.
Low	0.1-3.9	Planned hardening or routine corrective action.	Address through scheduled improvement activities.
Informational	Not scored	Record as an observation or best-practice recommendation.	Implement where justified by risk and available resources.

Each confirmed vulnerability shall include a CVSS v4.0 Base Score and complete CVSS:4.0 vector string. Where sufficient threat and environmental information is available, the firm shall also document the applicable Threat and Environmental metrics. CVSS severity and PMIU remediation priority shall be recorded separately where business context requires adjustment.

3.5 Testing Environment

All intrusive VAPT activities shall be conducted on the designated staging environment, which shall be a functional replica of production and shall use synthetic, anonymized, or appropriately masked test data. Production student or parent PII shall not be copied into staging solely for this engagement. No intrusive testing shall be conducted on the production environment without prior written approval from the SAMRS MIS Team. Any approved production-scope activity shall be scheduled outside operational hours and governed by the approved Rules of Engagement.

Testing methodology shall be aligned with:

- OWASP Top 10, latest stable release at contract signing, currently OWASP Top 10:2025
- OWASP API Security Top 10, latest stable release at contract signing, currently the 2023 edition
- OWASP Mobile Application Security Verification Standard (MASVS) and Mobile Application Security Testing Guide (MASTG) for Android testing
- NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)
- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- CVSS v4.0 for vulnerability scoring, including the complete vector string
- ISO/IEC 27001:2022 and ISO/IEC 27002:2022 for the ISMS readiness and controls assessment methodology

3.6 VAPT Rules of Engagement

Before active testing begins, the firm and the SAMRS MIS Team shall approve written Rules of Engagement covering:

- the final in-scope and excluded assets;

- authorized source IP addresses;
- testing dates and time windows;
- permitted and prohibited techniques;
- rate limits and denial-of-service restrictions;
- emergency contacts and escalation procedures;
- stop-testing conditions;
- backup and recovery confirmation;
- incident-reporting procedures; and
- evidence-handling and secure communication channels.

Denial-of-service, destructive testing, bulk deletion, uncontrolled password spraying, and social-engineering activities shall remain prohibited unless separately and expressly authorized in writing.

4. Deliverables

The firm shall deliver the following:

#	Deliverable	Description
D-01	Inception Report, Detailed Work Plan, and Rules of Engagement	Validation of the indicative asset schedule in Section 3.1.1 and confirmation of the final authoritative scope and asset inventory, including web applications, the mobile application, REST API service, API endpoint enumeration, external API integration directionality, server/service mapping, and shared database placement; testing approach; methodology; tools and equivalent-tool justification; CVSS v4.0 scoring approach; ISO/IEC 27001 assessment criteria; personnel deployment plan; communications matrix; engagement risk register; approved Rules of Engagement; and detailed activity schedule.
D-02	Draft VAPT Report	Results of automated and manual security testing across all approved in-scope components. Scanner findings shall be manually validated, duplicates consolidated, and false positives removed. Each confirmed finding shall include the affected asset, CVSS v4.0 score and vector, evidence, business impact, safe reproduction information, and recommended remediation.
D-03	ISO/IEC 27001:2022 ISMS Readiness Assessment Report	Assessment against applicable ISO/IEC 27001:2022 Clauses 4-10 and Annex A controls, including the 23 minimum focus areas in Section 3.3; review of the ISMS scope, risk assessment, risk treatment plan, and Statement of Applicability; and evidence-based findings with current state, gap narrative, priority, and corrective-action recommendation
D-04	Findings & Recommendations	Findings, root-cause analysis, and prioritized remediation recommendations for confirmed VAPT findings and ISO/IEC 27001 gaps. Remediation/fixation is the sole responsibility of the SAMRS technical team; the firm's role is limited to findings, recommendations, and retesting/verification.

#	Deliverable	Description
D-05	Re-test & Verification Report	Re-test all VAPT findings and ISO/IEC 27001 gaps submitted by PMIU as ready for verification. Record each item as Remediated, Partially Remediated, Not Remediated, Not Submitted for Re-test, Not Reproducible, or Risk Accepted, with supporting evidence and residual-risk observations. The contract price shall include one complete re-test cycle and one targeted verification cycle for remaining Critical and High findings within the contractual or formally extended period.
D-06	Final VAPT and ISO/IEC 27001 Readiness Report, Applicable Clearance Statement, and Readiness Assessment Opinion	Consolidated final report covering VAPT results, ISO/IEC 27001 readiness findings, remediation evidence, and residual risks. Where clearance criteria are met, issue a VAPT Clearance Letter; otherwise issue a Non-Clearance and Residual-Risk Statement. Issue an unqualified or qualified ISO/IEC 27001 Readiness Assessment Opinion, as supported by the evidence. These documents are not a substitute for formal certification by an accredited Certification Body.

The Final Consolidated Report (D-06) shall include, at minimum:

- Executive Summary covering both VAPT and ISO/IEC 27001:2022 ISMS readiness assessment results.
- VAPT findings register: Vulnerability ID, affected component, CVSS v4.0 score and vector, severity, description, proof-of-concept evidence, business impact, and remediation guidance.
- ISO/IEC 27001 assessment register: requirement or control area, ISO/IEC 27001 reference, current state, evidence reviewed, gap narrative, priority rating, and recommendation.
- Remediation tracker for VAPT findings showing Open, Partially Remediated, Remediated, Not Submitted for Re-test, Not Reproducible, or Risk Accepted status.
- ISO/IEC 27001 gap tracker showing pre- and post-remediation status for Priority 1, Priority 2, and Priority 3 gaps.
- Compliance mapping against the latest stable OWASP Top 10 and OWASP API Security Top 10 releases applicable at contract signing, and ISO/IEC 27001:2022 requirements and Annex A controls.
- Infrastructure and SSL/TLS scan results.
- Where no unresolved Critical or High VAPT findings remain, a signed VAPT Clearance Letter. Medium findings shall either be remediated or covered by a PMIU-approved corrective-action plan or documented risk acceptance. Where the clearance criteria are not met, a signed Non-Clearance and Residual-Risk Statement identifying the outstanding findings.
- An unqualified ISO/IEC 27001 Readiness Assessment Opinion where the readiness criteria are met, or a qualified opinion identifying outstanding Priority 1 and Priority 2 gaps where the criteria are not met. A qualified opinion or Non-Clearance Statement caused by outstanding PMIU-owned remediation shall not constitute non-performance by the firm.
- Intellectual-property declaration confirming that all project-specific reports, findings registers, evidence packages, assessment records, and documentation produced specifically for this engagement are owned by the Government of Sindh / PMIU SELECT RSU. The firm shall retain ownership of its pre-existing tools, methodologies, templates, and intellectual property, while

granting PMIU a perpetual, royalty-free licence to use any such material embedded in accepted deliverables for internal government purposes.

- Risk acceptance may be approved only by an authorized PMIU official identified in the approved governance or escalation matrix. The security firm may recommend risk treatment but shall not approve risk acceptance on behalf of PMIU.

5. Duration

The total duration of the engagement is sixty (60) working days from the date of contract signing (T). The ISO/IEC 27001 ISMS readiness assessment shall run concurrently with the VAPT remediation window to avoid unnecessarily extending the overall timeline. The indicative schedule is as follows:

Phase	Activity	Detail	Period
Phase 1	Inception & Scoping	Scope confirmation; validation of the indicative asset schedule and final asset inventory; API endpoint and external-integration directionality verification; NDA execution; environment setup; host/service and shared-database mapping verification; and personnel list submission	T+5
Phase 2	VAPT VA + Penetration Testing	Information gathering, vulnerability assessment, active penetration testing on staging environment	T+15
Phase 3	ISO/IEC 27001 ISMS Readiness Assessment	Assessment against applicable Clauses 4-10 and Annex A controls, including the 23 minimum focus areas; interviews with system owners, developers, MIS personnel, and relevant control owners	T+30
Phase 4	Draft Reports & PMIU Remediation	Draft VAPT and ISO/IEC 27001 readiness reports delivered; PMIU remediates Critical and High VAPT findings and Priority 1 and Priority 2 ISO gaps.	T+40
Phase 5	Re-test & Verification	Firm re-tests submitted VAPT remediation and re-assesses submitted ISO/IEC 27001 corrective actions with documented evidence	T+50
Phase 6	Final Reports & Debrief	Final VAPT and ISO/IEC 27001 Readiness Report; applicable Clearance or Non-Clearance Statement; management debrief; credential-destruction confirmation; and qualified or unqualified Readiness Assessment Opinion	T+60

Any request for an extension shall be submitted in writing within three (3) working days after the firm becomes aware, or should reasonably have become aware, of the event causing the delay, and before the affected milestone where practicable. The request shall state the cause, affected activities, mitigation actions, and proposed revised dates. Where delay results from the unavailability of PMIU personnel, systems, approvals, test environments, credentials, infrastructure, or completed remediation, the affected milestone and overall schedule shall be extended proportionately. Such extension shall not automatically result in additional payment unless the delay materially increases the firm's approved level of effort and PMIU approves the additional cost in writing.

6. Reporting and Communication

The firm will report directly to the MIS Team of the SELECT Project.

Confidentiality and Data Handling

- The firm shall execute a Non-Disclosure Agreement (NDA) with PMIU SELECT RSU prior to commencement. The NDA shall remain in force for three (3) years post-contract.
- No student records, PII, or production database content shall be extracted, copied, or retained by the firm except where PMIU provides specific written authorization for a defined purpose and duration. Any authorized evidence shall be minimized and redacted wherever practicable.
- All testing credentials, API keys, and system documentation must be securely destroyed upon contract completion. Written confirmation of destruction must be provided within five (5) working days of contract closure.
- The firm shall maintain a log of all personnel who accessed SAMRS test systems and provide it to PMIU upon request.
- Prior to commencement, the firm must submit a personnel information list for all individuals performing activities under this TOR: Full Name, Photograph, CNIC, Mobile Number, and Role. No personnel outside this approved list shall perform any activities.
- All reports, screenshots, logs, packet captures, source-code extracts, and other assessment evidence shall be treated as Confidential Information. Evidence shall be encrypted in transit and at rest, accessible only to approved personnel, and stored only in locations approved by PMIU.
- Screenshots and report evidence shall be redacted to remove unnecessary CNIC, B-Form, student, parent, credential, and other sensitive information.
- Cloud-hosted or SaaS-based scanning platforms shall not be used to upload SAMRS source code, credentials, database content, or PII without prior written approval from PMIU and documented confirmation of the tool's data-residency, retention, access, and deletion arrangements.
- Any suspected exposure, loss, or unauthorized access involving SAMRS information shall be reported immediately to the designated PMIU contact, together with initial containment information, and followed by a written incident report.
- All temporary working files and evidence copies shall be securely deleted after acceptance of D-06, subject only to any retention specifically required by PMIU in writing.

ANNEX B: Quotation Forms

Service provider Quotation Form

From:	[Service provider's name]
Supplier's Representative:	[Insert name of Service provider's Representative]
Title/Position:	[Insert Representatives title or position]
Address:	[Insert Service provider's address]
Email:	[Insert Service provider's email address]

To:	Sindh Early Learning Enhancement through Classroom Transformation (SELECT)
Purchaser's Representative:	Mr. Junaid Hameed Samo
Title/Position:	Chief Program Manager (CPM)
Address :	Sindh Early Learning Enhancement through Classroom Transformation (SELECT) RSU 47-E/1, 48th Street, Block # 06, PECHS, Near Nursery, Shahrah-e-Faisal, Karachi, Pakistan.
RFQ Ref No.:	PK-RSU-SINDH-570306-NC-RFQ
Date of Quotation:	02 nd October 2026

Dear [insert name of Purchaser's Representative]:

SUBMISSION OF QUOTATION

1. Conformity and no reservations

In response to the above-named RFQ we offer to perform the Non-Consulting Services as per this Quotation and in conformity with the RFQ, the Terms of Reference, the Completion Schedule and the Deliverable Review and Acceptance mechanism set out in Annex A. We confirm that we have examined and have no reservations to the RFQ, including the Contract.

2. Eligibility

If awarded the Contract, the Non-Consulting Services that we perform shall originate from an eligible country. We confirm that we meet the eligibility and qualification requirements E-01 to E-08, and the firm (or its personnel) must not have been involved in the design, development, or maintenance of SAMRS or any related SELECT Project system, to preserve independence of the assessment.

We, along with any of our subcontractors, suppliers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the World Bank Group or a debarment imposed by the World Bank Group in accordance with the

Agreement for Mutual Enforcement of Debarment Decisions between the World Bank and other development banks. Further, we are not ineligible under the Purchaser's Country laws or official regulations or pursuant to a decision of the United Nations Security Council.

3. Quotation Price

The total price of our offer is *[insert the total price of the offer in words and figures, indicating the various amounts and the respective currencies]*.

4. Quotation Validity

Our Quotation shall be valid until the date specified in the RFQ, and it shall remain binding upon us and may be accepted at any time before it expires.

5. Not Bound to Accept

We understand that you reserve the right to:

- a. accept or reject any Quotation and are not bound to accept the lowest evaluated cost Quotation, or any other Quotation that you may receive.
- b. Annul the RFQ process at any time prior to the award of the Contract without incurring any liability to Suppliers.

6. Fraud and Corruption

We hereby certify that we have taken steps to ensure that no person acting for us, or on our behalf, engages in any type of Fraud and Corruption.

On behalf of the Supplier:

Name of the person duly authorized to sign the Quotation on behalf of the Supplier: *[insert complete name of person duly authorized to sign the Quotation]*

Title of the person signing the Quotation: *[insert complete title of the person signing the Quotation]*

Signature of the person named above: *[insert signature of person whose name and capacity are shown above]*

Date signed *[insert date of signing]* day of *[insert month]*, *[insert year]*

Price Schedule

[The following forms may be used by the Service provider for submitting its quotation. The forms may also be used for the contract subsequent to any negotiations.]

S. No.	Description	Amount in Figures (PKR)	Amount in Words
A.	Quotation Price		
B.	Applicable Taxes		
C.	TOTAL (A+B)		

Deliverable Wise Break Down of the Quotation:

Deliverable	Description	Weightage	Cost of Each Deliverable (PKR)
1	Inception Report, Detailed Work Plan and Rules of Engagement	(D-1+D-2) 20%	
2	Draft VAPT Report		
3	ISO/IEC 27001:2022 ISMS Readiness Assessment Report	20%	
4	Findings and Recommendations Report	10%	
5	Re-test and Verification Report (one complete re-test cycle and one targeted verification cycle)	25%	
6	Final Consolidated Report, Clearance / Non-Clearance Statement and Readiness Assessment Opinion	25%	

Signature: _____

Name of Authorized representative: _____

Date: _____

ANNEX C: Contract Forms

Contract Agreement

THIS AGREEMENT made the [*insert: number*] day of [*insert: month*], [*insert: year*].

BETWEEN

- (1) Sindh Early Learning Enhancement through Classroom Transformation (SELECT), School Education & Literacy Department, Govt Of Sindh, having its principal place of business at Reform Support Unit 47-E/1, Street No. 48, PECHS Block-6, Near Nursery Furniture Market, Shahrah-e-Faisal, Karachi. (hereinafter called “the Purchaser”), of the one part, *and*
- (2) [*insert name of service provider*], a corporation incorporated under the laws of [*insert: country of service provider*] and having its principal place of business at [*insert: address of service provider*] (hereinafter called “the *service provider*”), of the other part :

WHEREAS the Purchaser invited quotations for certain Non-Consulting Services and related services [*insert brief description of Goods / Services*] and has accepted a quotation by the *service provider* for the certain Non-Consulting Services.

The Purchaser and the *service provider* agree as follows:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Contract documents referred to.
2. The following documents shall be deemed to form and be read and construed as part of this Agreement. This Agreement shall prevail over all other Contract documents.
 - (a) the Letter of Award of Contract
 - (b) the Supplier’s quotation
 - (c) Conditions of Contract
 - (d) the Purchaser’s Requirements (including Schedule of Requirements and Technical Specifications)
 - (e) the completed Schedules (including Price Schedules)
 - (f) any other document listed as forming part of the Contract
3. In consideration of the payments to be made by the Purchaser to the Supplier as specified in this Agreement, the Supplier hereby covenants with the Purchaser to provide the Goods / Services and Related Services if applicable and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the Goods / Services and Related Services if applicable and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of *[the Purchaser's country, unless agreed otherwise]* on the day, month and year indicated above.

[To facilitate this emergency procurement, if acceptable to the Purchaser and the service provider, electronic signature of the Contract Agreement such as using DocuSign is recommended.]

For and on behalf of the Purchaser:

Signed: *[insert signature]*

In the capacity of *[insert title or other appropriate designation]*

In the presence of *[insert identification of official witness]*

For and on behalf of the service provide:

Signed: *[insert signature of authorized representative(s) of the service provider]*

In the capacity of *[insert title or other appropriate designation]*

In the presence of *[insert identification of official witness]*

Conditions of Contract

1. Definitions	1.1 The following words and expressions shall have the meanings hereby assigned to them: (a) “Bank” means the World Bank and refers to the International Bank for Reconstruction and Development (IBRD) or the International Development Association (IDA). (b) “CC” means the Conditions of Contract. (c) “Contract” means the Contract Agreement entered into between the Purchaser and the Supplier, together with the Contract Documents referred to therein, including all attachments, appendices, and all documents incorporated by reference therein. (d) “Contract Documents” means the documents listed in the Contract Agreement, including any amendments thereto. (e) “Contract Price” means the price payable to the Supplier as specified in CC 8.1, subject to such additions and adjustments thereto or deductions there from, as may be made pursuant to the Contract. (f) “Day” means calendar day. (g) “Completion” means the fulfillment of the Related Services, as applicable, by the Supplier in accordance with the terms and conditions set forth in the Contract. (h) “CC” means the Conditions of Contract. (i) “Goods” means all of the commodities, raw material, machinery and equipment, and/or other materials that the Supplier is required to supply to the Purchaser under the Contract. (j) “Party” means the Purchaser or the Contractor, as the context requires, and “Parties” means both of them. (k) “Purchaser” means the entity purchasing the Goods / Services and Related Services as applicable, as specified in CC 2. (l) “Purchaser’s Country” is the country specified in the CC 2. (m) “Related Services” means the services incidental to the supply of the goods / services, such as insurance, installation,
-----------------------	---

	Training and initial maintenance and other such obligations of the Supplier under the Contract, as applicable. (n) “Subcontractor” means any person, private or government entity, or a combination of the above, to which any part of the Goods / Services to be supplied or execution of any part of the Related Services is subcontracted by the Supplier. (o) “Service provider” means the person, private or government entity, or a combination of the above, whose Quotation to perform the Contract has been accepted by the Purchaser and is named as such in the Contract Agreement. (p) “The Project Site,” where applicable, means the place named in the CC.
2. Purchaser, Purchaser’s Country, Project Site/Final Destination	2.1 The Purchaser is: Sindh Early Learning Enhancement through Classroom Transformation (SELECT), Reform Support Unit (RSU), Sindh Education & Literacy Department (SE& LD), Government of Sindh 2.2 The Purchaser’s Country is: Pakistan. 2.3 The Assignment sites of execution is : Karachi
3. Inco terms	3.1 Not Applicable
4. Notices and Addresses for notices	4.1 Any notice given by one Party to the other pursuant to the Contract shall be in writing to the address hereafter using the quickest available method such as electronic mail with proof of receipt. <u>Address for notices to the Purchaser:</u> <i>Mr. Junaid Hameed Samo, Chief Program Manager (CPM)</i> Address: Sindh Early Learning Enhancement through Classroom Transformation (SELECT) RSU <i>47-E/1, 48th Street, Block # 06, PECHS, Near Nursery, Shahrah-e-Faisal, Karachi, Pakistan. Email: junaidecpmrsu@gmail.com</i> <u>Address for notices to the Supplier:</u> <i>[insert the name of officer authorized to receive notices]</i> <i>[title/position]</i> <i>[department/work unit]</i> <i>[address]</i> <i>[Electronic mail address]</i>
5. Governing Law	5.1 The Contract shall be governed by and interpreted in accordance with the laws of Islamic Republic of Pakistan.
6. Settlement of Disputes	(a) Contract with foreign Supplier: Not Applicable (b) Contracts with Supplier national of the Purchaser’s Country:

		In the case of a dispute between the Purchaser and a Supplier who is a national of the Purchaser’s Country, the dispute shall be referred to adjudication or arbitration in accordance with the laws of the Purchaser’s Country.																												
7. Execution	7.1	The execution of services and delivery of the related goods / services shall be in accordance with the Delivery and Completion Schedule specified in the Schedule of Requirements.																												
8. Contract Price	8.1	The Contract Price is specified in Price Schedule.																												
	8.2	The unit prices charged by the Service provider for subject services and supply of related goods / services under the Contract shall not vary from the prices quoted by the Supplier and accepted by the Purchaser.																												
9. Terms of payment	9.1	The method and conditions of payment to be made to the Service provider under this Contract shall be as follows: <table><tr><th>#</th><th>Milestone</th><th>Condition</th><th>Payment %</th></tr><tr><td>P-01</td><td>Acceptance of D-01 + D-02</td><td>SAMRS MIS Team written acceptance of the Inception Report, Detailed Work Plan, and Rules of Engagement (D-01) and the Draft VAPT Report (D-02)</td><td>20%</td></tr><tr><td>P-02</td><td>Acceptance of D-03</td><td>SAMRS MIS Team written acceptance of ISO/IEC 27001:2022 ISMS Readiness Assessment Report (D-03)</td><td>20%</td></tr><tr><td>P-03</td><td>Acceptance of D-04</td><td>SAMRS MIS Team written acceptance of Findings & Recommendations Report (D-04); remediation/fixation remains the responsibility of the SAMRS technical team.</td><td>10%</td></tr><tr><td>P-04</td><td>Acceptance of D-05</td><td>SAMRS MIS Team written acceptance of D-05 after the firm has completed the agreed re-testing and verification activities and documented the status of all items submitted by PMIU for re-test. Payment shall not be conditional upon successful remediation of matters that are the responsibility of PMIU or the SAMRS technical team.</td><td>25%</td></tr><tr><td>P-05</td><td>Acceptance of D-06</td><td>PMIU written acceptance of D-06, including the applicable VAPT Clearance Letter or Non-Clearance and Residual-Risk Statement, and the applicable unqualified or qualified ISO/IEC 27001 Readiness Assessment Opinion</td><td>25%</td></tr><tr><td colspan="3">Total</td><td>100%</td></tr></table>	#	Milestone	Condition	Payment %	P-01	Acceptance of D-01 + D-02	SAMRS MIS Team written acceptance of the Inception Report, Detailed Work Plan, and Rules of Engagement (D-01) and the Draft VAPT Report (D-02)	20%	P-02	Acceptance of D-03	SAMRS MIS Team written acceptance of ISO/IEC 27001:2022 ISMS Readiness Assessment Report (D-03)	20%	P-03	Acceptance of D-04	SAMRS MIS Team written acceptance of Findings & Recommendations Report (D-04); remediation/fixation remains the responsibility of the SAMRS technical team.	10%	P-04	Acceptance of D-05	SAMRS MIS Team written acceptance of D-05 after the firm has completed the agreed re-testing and verification activities and documented the status of all items submitted by PMIU for re-test. Payment shall not be conditional upon successful remediation of matters that are the responsibility of PMIU or the SAMRS technical team.	25%	P-05	Acceptance of D-06	PMIU written acceptance of D-06, including the applicable VAPT Clearance Letter or Non-Clearance and Residual-Risk Statement, and the applicable unqualified or qualified ISO/IEC 27001 Readiness Assessment Opinion	25%	Total			100%
#	Milestone	Condition	Payment %																											
P-01	Acceptance of D-01 + D-02	SAMRS MIS Team written acceptance of the Inception Report, Detailed Work Plan, and Rules of Engagement (D-01) and the Draft VAPT Report (D-02)	20%																											
P-02	Acceptance of D-03	SAMRS MIS Team written acceptance of ISO/IEC 27001:2022 ISMS Readiness Assessment Report (D-03)	20%																											
P-03	Acceptance of D-04	SAMRS MIS Team written acceptance of Findings & Recommendations Report (D-04); remediation/fixation remains the responsibility of the SAMRS technical team.	10%																											
P-04	Acceptance of D-05	SAMRS MIS Team written acceptance of D-05 after the firm has completed the agreed re-testing and verification activities and documented the status of all items submitted by PMIU for re-test. Payment shall not be conditional upon successful remediation of matters that are the responsibility of PMIU or the SAMRS technical team.	25%																											
P-05	Acceptance of D-06	PMIU written acceptance of D-06, including the applicable VAPT Clearance Letter or Non-Clearance and Residual-Risk Statement, and the applicable unqualified or qualified ISO/IEC 27001 Readiness Assessment Opinion	25%																											
Total			100%																											
	9.2.	NOTE: • All invoices must reference the relevant deliverable number: D-01+ D-02, D-03, D-04, D-05, or D-06. • Payment shall be processed upon written acceptance of the corresponding deliverable.																												

10. Taxes and Duties	10.1 The Service provider shall be entirely responsible for all taxes, duties etc., incurred until the completion of contract. 10.2 If any tax exemptions, reductions, allowances or privileges may be available to the Service provider in the Purchaser's Country, the Purchaser shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.
11. Performance Security	11.1. Not Applicable
12. Subcontractors	12.1 The Service provider shall notify the Purchaser in writing of all subcontracts awarded under the Contract if not already specified in the Quotation. Such notification, in the original Quotation or later shall not relieve the Service provider from any of its obligations, duties, responsibilities, or liability under the Contract.
13. Insurance cover	Not Applicable
14. Transportation	14.1 Service provider shall entirely be responsible for transportation.
15. Site of inspections	15.1 PMIU SELECT RSU, Karachi; the designated SMARS staging environment and, where required for ISO/IEC 27001 evidence verification, the applicable hosting/data-center location or other PMIU-approved location. No district-level training-point inspections are envisaged under this assignment
16. Completion Date	16.1 Sixty (60) Working Days from Date of Signing Contract.
17. Copyright	17.1 The copyright in project-specific reports, findings registers, evidence packages and assessment records, and documentation produced specifically for this engagement shall be owned by the Government of Sindh / PMIU SELECT RSU. The Service Provider shall retain ownership of its pre-existing tools, methodologies, templates, and intellectual property; however, PMIU shall receive a perpetual, royalty-free license to use any such material embedded in acceptance of D-06, subject to the Contract terms.
18. Fraud and Corruption	18.1 The Bank requires compliance with the Bank's Anti- Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in Attachment A to the Conditions of Contract. 18.2 The Purchaser requires the Supplier to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the request for quotations or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

19. Inspections and Audit by the Bank	19.1 Pursuant to paragraph 2.2 e. of the attachment to the Conditions of Contract, the Service Provider shall permit and shall cause its agents (where declared or not), subcontractors, sub consultants, service providers, suppliers, and personnel, to permit, the Bank and/or persons appointed by the Bank to inspect the site and/or the accounts, records and other documents relating to the request for quotations process and/or execution of Contract. The Supplier's and its subcontractors attention is drawn to CC 22.1 (Fraud and Corruption) which provides, inter alia, that acts intended to materially impede the exercise of the Bank's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to the Bank's prevailing sanctions procedures).
20. Limitation of Liability	20.1 Except in cases of criminal negligence or willful misconduct, (a) the Service provider shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser and (b) the aggregate liability of the Service provider to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, Provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the supplier to indemnify the Purchaser with respect to patent infringement.
21. Force Majeure	21.1 The Service provider shall not be liable for forfeiture of its Performance Security (if required), liquidated damages, or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure. 21.2 For purposes of this Clause, "Force Majeure" means an event or situation beyond the control of the Supplier that is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of the Supplier. Such events may include, but not be limited to, acts of the Purchaser in its sovereign capacity, wars or revolutions, fires, floods, and freight embargoes. 21.3 If a Force Majeure situation arises, the Supplier shall promptly notify the Purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the Purchaser in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

22. Termination	22.1 Termination for Default The Purchaser, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the Service provider may terminate the Contract completely or in part: (i) If the Service provider fails to deliver any or all of the services or related goods within the period specified in the Contract, or within any extension thereof granted by the Purchaser; (ii) If the Supplier fails to perform any other obligation under the Contract; or (iii) if the Supplier, in the judgment of the Purchaser has engaged in Fraud and Corruption, in competing for or in executing the Contract. In the event the Purchaser terminates the Contract in whole or in part, the Purchaser may procure, upon such terms and in such manner as it deems appropriate, Services or Related Goods if applicable similar to those undelivered or not performed, and the service provider shall be liable to the Purchaser for any additional costs for such similar Goods / Services or Related Services if applicable. However, the Service Provider shall continue performance of the Contract to the extent not terminated. 22.2 Termination for Convenience (a) The Purchaser, by notice sent to the Service provider, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Purchaser's convenience, the extent to which performance of the Supplier under the Contract is terminated, and the date upon which such termination becomes effective.
------------------------	--

Attachment A to the Conditions of Contract

Fraud and Corruption

(Text in this Appendix shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders (applicants/proposers), consultants, contractors and suppliers; any sub-contractors, sub-consultants, service providers or suppliers; any agents (whether declared or not); and any of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

- a. Defines, for the purposes of this provision, the terms set forth below as follows:
 - i. "corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;
 - ii. "fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation;
 - iii. "collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;
 - iv. "coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;
 - v. "obstructive practice" is:
 - (a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or
 - (b) Acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

- b. Rejects a proposal for award if the Bank determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, suppliers and/ or their employees, has, directly or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question;
- c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;
- d. Pursuant to the Bank's Anti- Corruption Guidelines and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;¹ (ii) to be a nominated² sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;
- e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders (applicants/proposers), consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents personnel, permit the Bank to inspect³ all accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have them audited by auditors appointed by the Bank.

¹ For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, either directly or as a nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider, in respect of such contract, and (ii) entering into an addendum or amendment introducing a material modification to any existing contract.

² A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

³ Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank to address specific matters related to investigations/audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies thereof as relevant; accessing and examining any other documents, data and information (whether in hard copy or electronic format) deemed relevant for the investigation/audit, and making copies thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

Sample Letter of Award of Contract

[modify as appropriate]

[use letterhead paper of the Purchaser]

[date]

To: *[name and address of the Supplier]*

Subject: **Notification of Award of Contract No.**

In reference to the RFQ *[insert reference number and date]*, your Quotation *[insert reference number and date]* has been accepted.

Please find inclosed herewith the Contract. You are requested to sign the contract within *[insert no of days]*.

[Insert the following only if Performance Security is required:] “You are also requested to furnish a Performance Security within *[insert no of days]* in accordance with the Conditions of the Contract, using for that purpose one of the Performance Security Forms attached to the Contract.

Authorized Signature: _____

Name and Title of Signatory: _____

Name of Agency: _____

Attachment: Contract