(QUERIES & RESPONSES)

Request for Proposals Information System

(Single Stage)

Designing and Developing the Pakistan Regulatory Registry (PRR) and Providing Technical Assistance for Phase-wise Mapping, Streamlining and Cataloguing of RLCOs

Country:	**Pakistan**
Project Name:	**Digital Economy Enhancement Project**
Implementing Agency:	**Board of Investment (BOI)**
Loan No:	**75140-PK**
Project ID No:	**P174402**
RFP/ STEP Ref. No.	**PK-BOI-542104-GO-RFP**

S#	Clarification Question by Firms	Response by DEEP-BOI
1	**For Form EXP 1.4.2, can the qualifying contract value of USD 1.5 million refer to the total project value, or must it be KPMG's own share of the contract if delivered as part of a consortium or sub-consultancy arrangement?**	Per Section III, Sub-Factor 1.4.2 (Specific Experience, RFP p.67–69), the Proposer must demonstrate at least two (2) contracts of similar nature, each with a value of at least USD 1.5 million, successfully and substantially completed within the last five (5) years. The qualifying value is the value attributable to the Proposer: (i) A single entity must meet the full requirement on its own. (ii) For a Joint Venture, the requirement is met by all members combined (qualifying contracts are aggregated across JV members, per the 'All members combined — Must meet requirements' column in Section III 1.4.2). (iii) Where a past contract was delivered as part of a Consortium/JV or in a sub-consultancy role, only the firm's own attributable share counts, supported by the 'Percentage of participation' field in Form EXP 1.4.2. The role 'Sub-consultant' is explicitly recognised in the documentation requirements (Section III, p.69). Mandatory supporting evidence per Section III, p.68–69: signed contract agreement or work order, completion certificate or client reference letter confirming satisfactory performance, and proof of project value and scope (e.g., contract extracts or payment certificates).
2	**Can an ongoing project (substantially completed at more than 80%) be submitted as a qualifying specific experience contract, or must the project be fully and formally closed with a completion certificate?**	Substantially completed project are accepted where all major deliverables have been accepted by the client with the system live and operational. However, a completion certificate or an official client letter confirming satisfactory performance is mandatory as evidence. Formal contract closure is not required, but mere claims or self-declarations will not be accepted.
3	**Are international Key Experts (from KPMG member firms in Portugal, UAE, or KSA) eligible to be proposed as Key Experts, or must all Key Experts be Pakistan-based or have Pakistan work authorization as 'local presence' has been mentioned?**	International Key Experts are eligible and may be proposed. There is no nationality restriction on Key Experts beyond the eligibility provisions of Section V — Eligible Countries (which lists no excluded countries for this RFP, p.133) and the eligibility provisions of ITP Clause 4. Proposed Key Experts must be available and deployable in Pakistan for the engagement durations specified in Section VII Table 2.7-A (Software Development Key Experts KE-06 to KE-12, p.218) and Table 2.7-B (Technical Assistance Key Experts KE-01 to KE-05, p.219–220). Arrangement of work authorisation for international experts, and the cost and logistics of mobilisation and sustained on-the-ground delivery across the six jurisdictions, are the Supplier's responsibility (Section VII Sec.No2.7.1–2.7.3, p.221). The term 'local presence/availability' is interpreted as the Proposer's operational capacity to mobilise and sustain the team for delivery in Pakistan, not the Pakistan nationality of individual experts.
4	**The RFP requires all data to be hosted in Tier-3+ data centres within Pakistan. Will BOI specify the approved data centre provider(s), or is the contractor free to propose any facility that meets the Tier-3 specification?**	Hosting is on GoP-provided infrastructure and bidders neither procure nor select the data-centre facility. Per Section VII Sec.No3.0.2 (p.222) and Sec.No1.1.1.7 (p.149), all active software components and data MUST be hosted on GoP-provided infrastructure (a national government data centre or a GoP-approved public cloud environment) meeting Tier-3 or higher standards, physically located within Pakistan and configured for multi-zone availability across at least two independent availability zones within Pakistan. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) state, verbatim: 'Not Applicable — No hardware is procured under this Contract.' Bidders therefore do not quote for compute, storage, networking, security or ancillary hardware. The Supplier's obligation is limited to documenting the required infrastructure sizing, network and storage specifications, and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2. The solution MUST be cloud-agnostic with

		no dependency on a vendor-operated cloud not approved by the GoP (Sec.No1.1.1.7). The specific designated environment will be confirmed to the selected Supplier.
5	**The RFP mentions 100 economic activities across 5 ISIC Rev.4 sectors. Has BOI pre-defined which 100 economic activities and which 5 sectors are in scope, or is the identification of priority economic activities part of the contractor's deliverable in Phase 1?**	The 100 priority economic activities across five (5) ISIC Rev.4 sectors are the binding scope of the AS-IS/TO-BE mapping engagement per Section VII Sec.No1.2.11.4 (p.178). The SPECIFIC 100 activities are NOT pre-defined in the RFP — they are identified, agreed and notified through a TA deliverable produced by the Supplier in consultation with BOI/AKTU during the early TA phase: the 'ISIC Rev.4 Activity Selection Note' (Table 1.2.11-A row TA-D6 / SIT-1 row TA-02 — see p.179–180, p.247). The selection is informed by: (i) the existing regulatory inventory and prior mapping work; (ii) the PRMI Strategy and the Asaan Karobar Act 2025 priorities; (iii) stakeholder consultations with federal and provincial regulators across the six jurisdictions; (iv) ISIC Rev.4 sector groupings. The Activity Selection Note is approved by BOI/AKTU and forms part of the scope baseline (see S#143 / row 146). Subsequent changes to the activity set are managed under Section VIII GCC Clause 39 (p.362) read with SCC GCC 39.2.1 (p.393). The platform MUST remain scalable to accommodate additional activities and RLCOs in the future without architectural modification (Section VII Sec.No1.1.5, p.151).
6	**The RFP mentions integration with the Pakistan Business Portal (PBP). Is API documentation for PBP currently available, and will it be shared with shortlisted bidders before the proposal submission deadline?**	PBP (Pakistan Business Portal) is a priority integration target per Section VII Sec.No1.3.6.2 (p.194). The clause requires: 'An open, read-only API layer for published RLCO data MUST be provided for future integration with additional government portals including the Pakistan Business Portal (PBP).' PRR is a pre-requisite for PBP and PBP RFP is yet to be published. For proposal pricing and methodology purposes, Proposers should plan for: • Building a documented OpenAPI-compliant integration interface per Sec.No1.3.6.1 (p.194). • Standard integration patterns (REST/JSON; OAuth 2.0 where applicable) per Sec.No1.3.6.3 (p.194). • A dedicated sandbox environment for integration partners (Sec.No1.3.6.1). • Mock services for PRR-side testing pending PBP availability. See also S#43/row 46 (PBP API state), S#100/row 103 (priority integration list), S#108/row 111, S#115/row 118 (third-party API cost allocation).
7	**Do we need CVs for Key Experts only or non-key experts/field staff as well?**	CVs are mandatory only for Key Experts. The Key Expert positions are listed in Section VII Tables 2.7-A (Software Development — seven positions KE-06 to KE-12, p.218) and 2.7-B (Technical Assistance — five positions KE-01 to KE-05, p.219–220). CVs are to be submitted on the Personnel Capabilities form in Section IV. Six (6) Key Expert positions are individually scored under Annex Tech-I (Section X, p.451–456) for a combined total of fifteen (15) marks, applying the Standard Scoring Basis per expert: Excellent 2.5 / Good 1.5 / Marginal 1 / Non-Compliant 0. Non-Key Experts (Table 2.7-C — Indicative Non-Key Expert Staffing, p.220) are indicative only; CVs for non-key or field staff are not required at proposal stage. The Supplier proposes the non-key staffing structure as part of its delivery methodology.

8	**What exactly is included within the definition of RLCOs for this assignment—only legally binding instruments, or also SOPs, guidelines, circulars, and operational practices used by departments?**	RLCO definition as per Asaan Karobar Act, 2025 at clause 2(l). AK Act can be accessed at https://pakistancode.gov.pk/pdffiles/administratora25a4ffdfb999bb331f12dd2d8ce37ae.pdf#viewer.action=download The Registrations, Licences, Certificates, and Other Permits (RLCO) concept is the unit of scope for this assignment. RLCOs include legally binding regulatory instruments — rules, licences, registrations, certifications, permits, approvals, no-objection certificates, orders, regulations, SROs, by-laws, notifications, and similar instruments — applicable to businesses, together with the conditions and obligations they impose. Authoritative scope definition: the mandatory minimum dataset in ANNEX VII-A Table 1 (Section VII BIM-3, p.323) governs the structured record format for each RLCO, and Table 2 covers extended fields. Mandatory metadata per Sec.No1.3.3.4 (p.192) includes: jurisdiction, issuing authority, legal instrument type, legal basis reference, economic activity mapping (ISIC Rev.4), validity dates, fee structure, inspection authority, and appeal mechanism. SOPs, guidelines, circulars and operational practices ARE captured to the extent they constitute regulatory conditions or obligations applicable to the mapped economic activity — typically through linkage from the parent legal instrument's RLCO record and as part of the AS-IS workflow capture under Sec.No1.2.5.1 (process steps, decision points, required documents, fees, service channels, inter-agency handoffs). The detailed inventory and the boundary between binding instruments and supporting operational documents is finalised with BOI/AKTU during the mapping waves (Sec.No1.2.11.2 closure SOP).
9	**Are AS-IS BPMN workflows expected to reflect actual practices on the ground, including informal or unwritten steps followed by agencies?**	AS-IS BPMN workflows MUST reflect actual administrative practice on the ground, including informal and undocumented steps observed during stakeholder engagement, in order for the TO-BE redesign to address real bottlenecks. Per Section VII Sec.No1.2.5.1 (p.163), the structured workflow model MUST capture: process steps and tasks; actors and swimlanes; decision points; inputs and outputs; required documents and data objects; applicable fees and time bands; service channels; and inter-agency handoffs. Per Section VII Sec.No1.2.11.4 (p.178), AS-IS workflow documentation MUST be produced for the 100 priority economic activities, 'capturing process steps, actors and lanes, decision points, required documents, fees and time bands, service channels, and inter-agency handoffs' — i.e., the model is comprehensive enough to capture practice variations. Per Sec.No1.2.5.4, the System MUST allow BOI/AKTU to tag workflow steps with configurable bottleneck categories — including manual verification, queue delays, redundant approvals, duplicate documents, physical visits — which are exactly the categories that surface from observed practice rather than documented process alone. Per Sec.No1.2.5.2, both system-assisted draft generation and manual authoring via the BPMN editor are supported; informal steps identified during stakeholder workshops can therefore be authored into the AS-IS workflow before approval.

10	**For federal regulations applicable nationwide, should mapping be done once centrally or re-validated separately with each province during jurisdictional rollout?**	Federal regulations applicable nationwide are mapped CENTRALLY ONCE and then validated jurisdiction-by-jurisdiction during rollout to capture provincial application and any variation. Per Section VII Sec.No1.2.11.1 (p.177), the Supplier supports BOI/AKTU to implement a jurisdiction-wise onboarding plan covering Federal, ICT, and the four provinces (Punjab, Sindh, Khyber Pakhtunkhwa, and Balochistan), in tranche sequencing by readiness and priority. Per Sec.No1.2.11.2 (p.178), each participating agency executes a formal validation and closure SOP — including running data quality and completeness checks, supporting resolution of gaps and discrepancies until records are publishable, and securing formal departmental sign-off from each agency. This applies separately for each jurisdiction the federal regulation is implemented in, even where the underlying instrument is central. Per Sec.No1.1.5 (p.151), the Information System MUST be capable of accommodating jurisdictional requirements arising from equivalent provincial enactments and subordinate legislation without architectural modification — i.e., jurisdiction-specific variations are first-class data fields in the PRR record.
11	**What level of BPMN 2.0 detail is expected—high-level task flows only, or detailed models including gateways, events, exceptions, and rework loops?**	BPMN 2.0 workflow detail MUST be substantive — capturing tasks, gateways, events, exceptions, and rework loops sufficient to support process reengineering, IT readiness assessment, cost-impact calculation, and system configuration. Per Section VII Sec.No1.2.5.1 (p.163), the structured workflow model MUST capture, at minimum:• Process steps and tasks (user tasks, service tasks, manual tasks)• Actors and swimlanes• Decision points (exclusive/inclusive/parallel gateways)• Inputs and outputs• Required documents and data objects• Applicable fees and time bands• Service channels• Inter-agency handoffsPer Sec.No1.2.5.4 (p.163), bottleneck tagging captures categories such as redundant approvals, duplicate documents, physical visits, manual verification, and queue delays — which by their nature require detailed workflow modelling, not high-level flows. TO-BE workflows additionally capture structured redesign rationale and digitisation interventions (Sec.No1.2.5.4).Per Sec.No1.2.5.1, every approved workflow version MUST be stored in three synchronised representations: BPMN 2.0 XML (authoritative machine-readable), structured workflow data model (for analytics and rule-based checks), human-readable PDF rendering. AI-assisted draft generation provides a starting point (see S#237/row 240); full fidelity is achieved through human review and refinement under the approval workflow (Sec.No1.2.5.3).

12	**What minimum level of quantitative analysis is expected under RIA Lite (e.g., steps, time, cost), and will a standard template be issued by BOI/AKTU?**	RIA-lite (the regulatory impact assessment-lite methodology referenced in the Cost Impact Assessment Module, Section VII Sec.No1.2.7, p.166–168) supports quantitative analysis of regulatory burden. Per Sec.No1.2.7, Module 7 MUST enable BOI/AKTU to quantify and compare the administrative and compliance cost of RLCO processes before reform (AS-IS) and after reform (TO-BE). The Module requirements include: • Structured capture of cost drivers — process steps; time bands per step; fee and charge components; document and form requirements; channel mode; agency contact frequency; rework rates. • Built-in calculations supporting Standard Cost Model (SCM) and RIA-lite methodologies with configurable formulas, parameter libraries, and multi-currency support. • AS-IS versus TO-BE comparison reports with quantified impact (time-saving, cost-saving, document-elimination, fee-rationalisation). • Exports of cost impact assessments as structured records linked to the RLCO Record ID and workflow artefact. The Supplier MUST propose the cost methodology, assumption library and parameter values consistent with the PRMI Strategy and the Asaan Karobar Act, 2025 mandates; the standard template, assumption library and methodology pack are developed in consultation with BOI/AKTU during Inception (see Table 1.2.11-A TA Minimum Deliverables, p.179–180, especially TA Capacity Building Toolkit). The Module is configurable by BOI/AKTU without code changes (Sec.No1.2.7).
13	**The RFP specifies that any post-go-live maintenance or support services constitute recurrent costs and must be governed by separate, enforceable contracts. Could the Purchaser please confirm whether including maintenance or support services within the main financial proposal without such separate contractual instruments would render the pricing non-compliant or subject to rejection? Additionally, please clarify the expected contractual structure for post-go-live support to avoid any ambiguity at award or implementation stage.**	Confirmed. Post-go-live maintenance and support services constitute Recurrent Costs and MUST be priced under the Recurrent Cost sub-tables in Section IV (Forms 3.3 Recurrent Cost Summary and 3.5 Recurrent Cost Sub-Tables, including Table 3.5-A AMC, p.117 onwards). The contractual framework is: • Warranty / Defect Liability Period — TWO (2) YEARS from issuance of the Final Acceptance Certificate (Section IX SCC GCC 29.1, p.394); defect repair, security patches, AI module maintenance and software/licence renewals are included in the Supply and Installation Price (Section VII SIT-2 rows 1.1–1.4, p.252) and MUST NOT be separately quoted. • Post-Warranty Annual Maintenance Contract (AMC) — Years 1, 2 and 3 (Y1–Y3) MANDATORY line items; proposals failing to quote Y1–Y3 are non-responsive (Section VII SIT-2 Notes, p.251–252). Years 4–5 are at Purchaser's discretion (Section VII Sec.No5.2.3, p.238). • Service Level Agreements — Section VII Table 5.1-A (p.237). Embedding maintenance/support into the Supply and Installation price as a single bundle (instead of pricing Recurrent Costs separately in Forms 3.3/3.5 and as required SIT-2 line items) would render the Proposal non-compliant in respect of Section IV pricing structure.
14	**Could the Purchaser please clarify whether technical resources may be shared or overlap across jurisdictions when mapping waves are staged, or whether resources are expected to be exclusively dedicated to a single jurisdiction throughout its active mapping window? Additionally, please confirm whether senior subject-matter experts and quality-assurance roles may be shared across jurisdictions,**	Resource sharing across jurisdictions is permitted, subject to mandatory on-the-ground capacity for each active jurisdiction. Per Section VII Sec.No1.2.11.3 (p.178), the Supplier MUST design and deliver structured stakeholder engagement sessions across all jurisdictions — physically and virtually — with a minimum of one stakeholder session per jurisdiction per mapping wave. Per Section VII Sec.No2.7.1 — Field Deployment Capacity, the Supplier MUST demonstrate adequate field staffing to execute activities in parallel across all six jurisdictions (Federal, ICT, Punjab, Sindh, Khyber Pakhtunkhwa, and Balochistan) and to meet the milestone schedule. The team MUST remain mobilised throughout the Contract Period. Senior subject-matter experts (Key Experts per Table 2.7-B, p.219–220) and quality-assurance roles may be shared across jurisdictions where

	provided the minimum on-ground field staffing requirements per active jurisdiction are fully met.	mapping waves are staged, provided the on-ground field staffing in each active jurisdiction is sufficient to deliver the wave's mapping, workshops and validation activities to the milestone schedule. Engagement weeks and mobilisation expectations for each Key Expert are specified in Table 2.7-B.
15	**Hosting infrastructure: The Request for Proposals seems to contradicts itself on this fundamental point. Need clarification. The Proposal Data Sheet at ITP 18.1 states:"Work, services, facilities, etc., to be provided by the Purchaser: No."But Section VII, Section 3.0.2 of the Technical Requirements states:"All active software components and data MUST be hosted on GoP-provided infrastructure meeting the following minimum standards: Tier-3 or higher data centres physically located within Pakistan…multi-zone high availability across at least two independent availability zones within Pakistan."Could the Purchaser confirm explicitly: Is the data centre space, compute, storage, networking, Graphics Processing Unit hardware, and Hardware Security Module infrastructure provided by the Government of Pakistan at no cost to the Supplier? Or must the Supplier procure, supply, and price all of this within the Supply and Installation cost?**	There is no contradiction. The reference to 'Work, services, facilities, etc., to be provided by the Purchaser: No' in Section II PDS appears under entry ITP 36.1(f), p.52 — within sub-section 'I. Evaluation of Financial Part of Proposals'. This entry is a PRICE-EVALUATION ADJUSTMENT setting under the World Bank Standard Procurement Document framework: it specifies that NO price-adjustment will be applied to Proposers' bid prices in respect of 'Work, services, facilities etc. to be provided by the Purchaser' for the purpose of comparing financial proposals. It is NOT a substantive statement that the Purchaser will provide no facilities to the Supplier.The substantive provisions on hosting infrastructure are in Section VII Sec.No3.0.2 (p.222): all active software components and data MUST be hosted on GoP-provided infrastructure meeting Tier-3 or higher standards within Pakistan, multi-zone across at least two independent availability zones. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) each state verbatim: 'Not Applicable — No hardware is procured under this Contract.'Accordingly: data centre space, compute, storage, networking, GPU and HSM infrastructure are GoP-provided. The Supplier does NOT procure or price these items. The Supplier documents the required infrastructure sizing, network and storage specifications and auto-scaling thresholds in the Deployment Architecture document under Sec.No2.6.2.
16	**Section 1.6.9 prohibits transmitting Pakistan Regulatory Registry data to external Artificial Intelligence Application Programming Interfaces "unless explicitly approved in writing by the Purchaser." What is the approval process, and have any external models been pre-approved?**	Section VII Sec.No1.6.9 (p.203) and Sec.No1.2.10.1 (p.175) require that the AI Assist Module operate exclusively within government-controlled hosting and MUST NOT transmit PRR data to external AI platforms, model APIs, or cloud-based AI services unless explicitly approved in writing by the Purchaser. The prohibition extends to cloud-based embedding/inference APIs. Where a Proposer wishes to use an external AI service for a specific function, written Purchaser approval is sought through the project governance/issue-resolution mechanism on a case-by-case basis, supported by documented data-protection safeguards. No external models have been pre-approved at this RFP stage. The default expectation is self-hosted AI within government-controlled hosting; required GPU infrastructure forms part of GoP-provided infrastructure, with the Supplier documenting the GPU sizing/architecture in the Deployment Architecture document (Section VII Sec.No2.6.2 / Sec.No3.0.2).

17	**You've asked for system administrator and deployment and operations team members name. Do we need to submit their CVs as well? In addition, you've asked for BPMN workflow and AI governenace team member also and their names. Is this different from KE and non-KE experts already mentioned in rfp and do we need to give their CV as well or just names?**	CVs are mandatory only for the Key Expert positions specified in Section VII Tables 2.7-A (Software Development KE-06 to KE-12, p.218) and 2.7-B (Technical Assistance KE-01 to KE-05, p.219–220) — twelve (12) Key Expert positions in total. Six (6) of these are individually scored under Annex Tech-I (Section X, p.451–456) for fifteen (15) marks combined. For the indicative Non-Key Expert staffing per Table 2.7-C (p.220) — including system administrators, deployment and operations engineers, BPMN workflow analysts, AI governance team members, content moderators and other field/support roles — names and CVs are NOT required at proposal stage. The Supplier proposes the non-key staffing structure and capability as part of its delivery methodology; named individuals are nominated during inception/mobilisation, subject to Purchaser no-objection (Section VIII GCC 20 — Subcontracting and Personnel arrangements). Note: Per Section VIII GCC 39.8 (Key Personnel Lock-In) referenced in the Section IX SCC, named Key Personnel cannot be substituted without Purchaser consent during the Contract Period.
18	**Will formal sign-off of the AS-IS assessment and TO-BE design documents constituting scope baseline approval for subsequent development and acceptance activities?**	YES. Formal sign-off of the AS-IS assessment and TO-BE design documents establishes the approved scope baseline for subsequent development and acceptance activities. The framework is: • Approval workflow per Section VII Sec.No1.2.5.3 (p.163): Draft → Under Review → Returned for Revision → Verified/Approved → Archived/Superseded. Approval records verifier identity, timestamp, and comments. Approved workflow versions are locked; edits create a new version. • Departmental validation and closure SOP per Sec.No1.2.11.2 (p.178): formal sign-off from each participating agency confirming the RLCO inventory is accurate, official, and complete. • BPR methodology approval per Sec.No1.2.11.4 (p.178): the Supplier supports BOI/AKTU to develop and approve the BPR methodology, diagramming standards and analysis toolkit. • Module 9 RIS/AKTU Gating workflow (Sec.No1.2.9): central gating mechanism for AKTU Final Approval. Post-baseline scope additions: • Section VIII GCC Clause 39 — Changes to the System (p.362) read with Section IX SCC GCC 39.2.1 (p.393): Minor or Major classification; documented Change Order procedure with Change Order Forms in Section X (p.425–432). • GCC 39.6 turnaround: Supplier impact assessment within 5 business days; BOI decision within 10 business days; approved CRs into next available sprint. • SCC GCC 39.4 (p.393): Value Engineering Proposals will NOT be considered. • 15% Change Request budget ceiling under SCC GCC 39.5 (p.364). See S#143/row 146 for the full baseline + change-control + final approving authority treatment.
19	**After TO-BE approval, how will additional functional or regulatory requirements be governed under change-control mechanisms?**	After formal sign-off of the TO-BE design (which establishes the scope baseline per S#143/row 146 and S#18/row 20), additional functional or regulatory requirements are governed by Section VIII GCC Clause 39 — Changes to the System (p.362), read with Section IX SCC GCC 39 (p.393):• Change classification (SCC GCC 39.2.1): Minor (no cost/schedule impact) or Major (subject to detailed review/approval where applicable). All changes follow a documented Change Order procedure with Change Order Forms in Section X (p.425–432).• Turnaround (GCC 39.6, p.363–364): Supplier impact assessment within five (5) business days of CR submission;

		BOI approval/rejection within ten (10) business days; approved CRs incorporated into the next available sprint; rejected CRs recorded in the Change Log.• Budget ceiling (SCC GCC 39.5, p.364): Up to fifteen percent (15%) of total contract value may be allocated for Change Requests raised after MVP go-live — subject to BOI written approval for each change AND World Bank no-objection for cumulative changes exceeding 10% of contract value. Changes beyond 15% require a contract amendment.• Value Engineering proposals: NOT considered (SCC GCC 39.4, p.393).• MVP feedback under GCC 39.7 (p.364): Priority 1 within 30 days and Priority 2 within 60 days at NO additional cost — provided they do not constitute new features beyond the agreed MVP scope (see S#66/row 69).
20	**Who will be the final approving authority for AS-IS and TO-BE deliverables across Federal and Provincial stakeholders?**	Final approval of AS-IS and TO-BE workflow deliverables rests with the Purchaser (Board of Investment / AKTU) through the project governance structure, in coordination with the relevant federal and provincial line departments. Per Section VII Sec.No1.2.5.3 (p.163), all workflow artifacts pass through defined states — Draft, Under Review, Returned for Revision, Verified/Approved, and Archived/Superseded — with approval recording the verifier identity, timestamp and comments; approved workflow versions are locked and edits create a new version.
21	**These questions are strategically important because there are several key stakeholders involved from including but not limited to: Multiple ministries/departments RLCO harmonization Regulatory process reengineering Cross-provincial coordination Evolving integration And without formal TO-BE baseline approval, vendors can later face issues like: Unlimited requirement expansion Rework cycles Delayed milestone acceptance Uncontrolled stakeholder feedback Based on the above scenario and as per our past experience working with government departments, certain delays are very common from the purchaser side (due to HR unavailability majorly) and heavily impacting the suppliers from time & cost point. Is there any mechanism to re-schedule the activities and implementation of any LD or compensation?**	The Contract addresses delays caused by Purchaser-side factors (including delays attributable to stakeholder unavailability) through the following mechanisms: • Extension of Time for Achieving Operational Acceptance — Section VIII GCC Clause 40 (p.364): the Supplier may seek schedule relief for delay beyond its control, by notification under GCC 18.2 and GCC 19 with documentary evidence and impact analysis on the Implementation Schedule. A granted EoT adjusts the scheduled Operational Acceptance date correspondingly; Liquidated Damages do not accrue for the granted relief period. BOI/AKTU facilitates stakeholder engagement across the federal and provincial jurisdictions through the project governance and AKTU institutional mechanisms (Section VII Sec.No1.2.11.3, p.178).

22	**As per our understanding of the RFP, the project appears to consist of two major components:** *** development and management of departmental/public information for citizens and businesses; and** *** digitization, mapping, and management of regulatory processes, approvals, and compliance requirements of the respective departments.** **Kindly confirm whether our understanding is correct in accordance with the scope defined in the RFP.**	The understanding is broadly correct, with refinement. The engagement is structured as two parallel Activities under a single Contract, each priced and milestone-tracked separately (Section IV Price Schedules; Section IX SCC GCC 12.1 Payment Release Schedule, p.385–388): • Activity 1 — PRR System Development (Weeks 2–40 + post-go-live): the digital platform comprising the ten (10) mandatory modules — PRR Registry Core, Workflow Engine, MIS Dashboards, Mapping Enablement, BPR/AS-IS/TO-BE (Module 5), IT Readiness Assessment (Module 6), Cost Impact Assessment SCM/RIA-lite (Module 7), Public Portal & CMS (Module 8), RIS/AKTU Gating (Module 9), AI Assist (Module 10) — for the publishing and management of regulatory information for citizens and businesses, with departmental/public access. 12 milestones M1–M12. • Activity 2 — PRR RLCO Mapping & Workflow Reform Programme (Weeks 4–100): the Technical Assistance workstream covering RLCO mapping, AS-IS workflow documentation, TO-BE reengineering, IT readiness assessment and cost-impact analysis across one hundred (100) priority economic activities × five ISIC Rev.4 sectors × six jurisdictions (Federal, ICT, Punjab, Sindh, KP, Balochistan), per Section VII Sec.No1.2.11 (p.177–179). 10 milestones PM-1 to PM-10. The Supplier's responsibility under Activity 2 is to provide the platform, mapping methodology and TA capacity-building. Substantive validation of legal correctness of departmental content is exercised by BOI/AKTU and the line departments (see S#270).
23	**Will the selected firm be responsible for collecting and consolidating regulatory information from all relevant ministries/Provincial and Federal departments? Please share the list of departments.**	The Supplier is responsible for assistance in collecting, consolidating, structuring and standardising regulatory (RLCO) information from the relevant federal and provincial departments under the TA workstream, with BOI/AKTU facilitation. Per Section VII Sec.No1.2.11.1 (p.177–178), the Supplier supports BOI/AKTU to implement a jurisdiction-wise onboarding plan covering Federal, ICT, and the four provinces (Punjab, Sindh, Khyber Pakhtunkhwa, and Balochistan), including: regulator outreach support; focal person nomination facilitation; tranche sequencing by readiness and priority; structured RLCO data capture using PRR workflows; in-person and remote mapping assistance to DFPs. The specific list of participating departments per jurisdiction is operationally determined through the agency onboarding process under Module 4 (Mapping Enablement, Sec.No1.2.4) and recorded in the Agency Registry; this list is built up across the mapping waves rather than fixed at RFP stage. An indicative scope list is the set of departments and regulators with jurisdiction over the 100 priority economic activities across the five ISIC Rev.4 sectors (per Sec.No1.2.11.4, p.178), confirmed during Inception. BOI/AKTU provides formal engagement letters and DFP-nomination facilitation per Sec.No1.2.11.1; escalation for non-cooperation is through GCC 40 EoT (Section VIII, p.364).

24	**AS-IS to TO-BE Process Reengineering, for our understanding that It includes: Current official Processes and workflow, Existing departments and responsibilities, Manual steps, Delays and bottlenecks, Current software/systems being used, Problems and inefficiencies etc. etc. and need to be digitized the processes, do automation, Digital workflows, Faster approvals, Reduced, paperwork, Better transparency, Integration between departments/systems, etc. that include bidder scope of work or not?**	Confirmed — facilitate in AS-IS to TO-BE reengineering covers the elements listed by the bidder and is a substantive Supplier responsibility under the TA workstream. Per Section VII Sec.No1.2.5 (Module 5, p.163), Sec.No1.2.6 (Module 6 IT Readiness, p.165), Sec.No1.2.7 (Module 7 Cost Impact, p.166–168) and Sec.No1.2.11 (TA workstream, p.177–179):AS-IS scope (Sec.No1.2.5.1, Sec.No1.2.11.4):• Current official processes and workflows of the 100 priority economic activities• Current departmental roles, responsibilities, and inter-agency handoffs• Manual steps, delays, bottlenecks (captured via bottleneck tagging per Sec.No1.2.5.4)• Existing systems and portals in use, with their digitisation status (Sec.No1.2.6.2)• Fees, time bands, document requirements, service channels (Sec.No1.2.5.1)TO-BE scope (Sec.No1.2.5.4, Sec.No1.2.6, Sec.No1.2.7):• Redesigned digital workflows aligned with the Asaan Karobar Act 2025 and PRMI Strategy• Process simplification and automation pathway (Quick Win / Medium / Complex per Sec.No1.2.6.3)• Inter-agency integration plan and dependency matrix (Sec.No1.2.6.4)• Reduced paperwork, faster approvals, transparency through publication• Structured redesign rationale, expected impact (time/cost/document elimination), digitisation interventions, and dependencies on legal changes or IT integrations (Sec.No1.2.5.4)• SCM/RIA-lite quantified cost-impact analysis (AS-IS vs TO-BE) per Sec.No1.2.7Deliverables: AS-IS BPMN diagrams, TO-BE BPMN diagrams, sector reform packages (minimum 5 sectors per Sec.No1.2.5.5), IT readiness reports, cost-impact reports, first-cut draft amendment text where legal changes are required.
25	**If yes, then is there any timeframe for collecting the data from the departments? What are the mechanisms of getting the data because we have to hire a team of resources and financial cost involve to get the data from the departments across Pakistan.**	Timelines are addressed in Asaan Karobar Act, 2025. Further timeline management to be addressed by Supplier in inception report by giving a plan on handholding and capacity building of DFPs. Data collection from departments is conducted through the TA workstream over the 100-week programme, with the wave-based jurisdiction onboarding plan per Section VII Sec.No1.2.11.1 (p.177–178). The wave structure per Section IX SCC Activity 2 Payment Release Schedule (p.387–388) is: • PM-1 (Week 4): TA Inception & Governance Pack — rollout framework for the six jurisdictions. • PM-2 (Week 14): TA Capacity Building Toolkit + Methodology Pack. • PM-3 (Week 28): ISIC Rev.4 Activity Selection Note (100 priority activities × 5 sectors finalised). • PM-4 (Week 40): Wave 1 — Federal Government + ICT mapping completion (~Weeks 28–40). • PM-5: Wave 2 (first provincial wave) mapping completion. • PM-6: Wave 3 (second provincial wave) mapping completion. • PM-7 to PM-10 (through Week 100): rolling AS-IS workflow capture, TO-BE design, IT Readiness, Cost Impact, and final RLCO closure with reform pack handover. Mechanisms (Section VII Sec.No1.2.11.1 to Sec.No1.2.11.4): • Dedicated TA resources providing practical mapping assistance to DFPs through remote support and in-person visits across the six jurisdictions. • Structured stakeholder engagement sessions — minimum one session per jurisdiction per mapping wave (Sec.No1.2.11.3, p.178). • BOI/AKTU facilitation through formal engagement letters and DFP nomination support. • Bulk import facility with validation rules (Excel/CSV upload to Table 1 ANNEX VII-A fields) per Sec.No2.5.2 (p.215). • AI-assisted extraction with mandatory Human Verification Queue

		(Sec.No2.5.2). The Supplier MUST plan and price its TA resources — Key Experts per Table 2.7-B (p.219–220), non-key field staff, travel and logistics — to meet the wave schedule. Field deployment capacity per Sec.No2.7.1 (p.221).
26	**There are 2 types of data for the departments.**	The mandatory minimum RLCO dataset is defined in ANNEX VII-A (Table 1)
27	**Data digitization is the scope of the bidder, or it is the responsibility of all departments. Approximately how much legacy data/documents need digitization? Will scanned documents be provided by BOI? Is OCR/document scanning included in the scope and related to Human Resources?**	Data structuring and standardisation of RLCO records will be handled through development of into the PRR and it's functionality is within the Supplier's TA scope. Per Section VII Sec.No2.5.1 (p.215), the Supplier MUST handhold the DFPs and 'provide services and tools to incorporate all existing regulatory inventory datasets provided by the Purchaser — including prior mapping outputs, departmental RLCO lists, regulatory scans, and legacy database exports — into the PRR.' Volume, type, structure and format will be confirmed during Inception.Per Sec.No2.5.1, the Supplier MUST 'conduct a data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, and records requiring manual validation.'Per Sec.No2.5.2 (p.215), bulk import facility (Excel/CSV) is mandatory; AI-assisted extraction from documents or portals MAY be used to accelerate data structuring, BUT all AI-extracted outputs MUST be placed in a Human Verification Queue and MUST NOT be promoted to Validated status until human review and approval are completed.Source records:• Where existing in structured digital form (databases, structured spreadsheets) — bulk import per Sec.No2.5.2.• Where existing as scanned PDFs or paper records — the Supplier captures and structures through its methodology, which may include OCR, AI-assisted extraction with human verification, or direct data entry through Module 4 (Mapping Enablement).BOI/AKTU provides available source documents and prior mapping outputs (Sec.No2.5.1). The Supplier sizes its team (Key Experts per Table 2.7-B + indicative non-key staffing per Table 2.7-C, p.220) for the wave-based mapping workload across the six jurisdictions. The Supplier prices the TA effort with appropriate contingency for the variable data maturity.
28	**What level of training is expected? How many users/departments will require training? Without knowing the details of how many government officials need to be trained. We will not able to make accurate costing?**	Training requirements are specified in Section VII Sec.No2.4 (p.212–215). Mandatory minima: • Audience coverage (Sec.No2.4.3, p.213): role-based separate training tracks for AKTU Administrators, AKTU Operations and Reviewers, Moderators, Departmental Focal Persons (DFPs), and IT Operations teams. • Train-the-Trainer (Sec.No2.4.3): mandatory for international Suppliers with local technical partnerships; capacity retention strategy must be explained. • Training Plan (Sec.No2.4.1): mandatory deliverable during Inception covering target audiences, schedule, sequencing, delivery mode, environment requirements, materials list and evaluation methodology — includes initial centralised bootcamp, jurisdiction-wise DFP onboarding aligned to mapping tranches, and recurring refresher clinics during waves. • Materials (Sec.No2.4.4): user manuals, quick reference guides, SOP checklists, slide decks, exercise scripts, troubleshooting guides, FAQs, sample datasets — in editable formats, with operational SOPs and user-facing guides in both English and Urdu. • TA capacity building (Sec.No2.4.5–Sec.No2.4.8): distinct standalone programme for regulatory mapping methodology training, BPR/workflow documentation training, and stakeholder engagement / reform facilitation

		training. All training logistics, tools and sandbox environment setup are the Supplier's responsibility.
29	**Does BOI currently maintain any existing database, documentation, or inventory of RLCOs that will be shared with the selected bidder?**	BOI/AKTU has access to prior regulatory mapping outputs, departmental RLCO inventories, and regulatory scans produced under earlier government regulatory reform initiatives, which will be shared with the selected Supplier during the Inception phase per Section VII Sec.No2.5.1 (p.215). Specifically: • 'The Supplier MUST provide services and tools to incorporate all existing regulatory inventory datasets provided by the Purchaser — including prior mapping outputs, departmental RLCO lists, regulatory scans, and legacy database exports — into the PRR.' (Sec.No2.5.1) • Per Sec.No2.5.1: 'Volume, type, structure, and format of existing data available will be confirmed during the Inception phase.' • Per Sec.No2.5.1, the Supplier MUST conduct a data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, and records requiring manual validation. The existing inventory is NOT exhaustive across all 6 jurisdictions and 100 priority activities; the Supplier remains responsible for completing, structuring and standardising the inventory to ANNEX VII-A Table 1 (mandatory minimum dataset, Section VII BIM-3, p.323) and Table 2 (extended fields) through the wave-based mapping programme (Activity 2 milestones PM-1 to PM-10). Departmental sign-off per Sec.No1.2.11.2 (p.178) closes each agency's inventory.
30	**Approximately how many concurrent users are expected to be connected on that platform? and future expectations?**	The mandatory concurrency targets are specified in Section VII Sec.No1.5.3 (p.198) and Table 1.5-A (p.201) and are contractually binding minimum requirements: • Concurrent authenticated DFP/AKTU sessions: 2,000 simultaneous (national mapping campaign scenario) • Concurrent simultaneous public portal users (normal operations): ≥ 5,000 (auto-scaling baseline) • Concurrent simultaneous public portal users (peak consultation): ≥ 25,000 (auto-scaling activated; consultation surge scenario) Mandatory page-load P95 targets per Table 1.5-A: public search/browse ≤ 2 s; RLCO detail retrieval ≤ 3 s; workflow state transition ≤ 5 s; record save/create ≤ 3 s; bulk-import validation of 1,000 records ≤ 30 s. System availability ≥ 99.9% monthly (target 99.95%). RTO ≤ 4 hours and RPO ≤ 1 hour (Section VII Sec.No1.3.5.3, p.193). Horizontal auto-scaling for the public portal and search tier MUST activate automatically under load (Sec.No1.5.3). Targets are validated during Pre-commissioning Tests (Sec.No4.2) and Operational Acceptance Tests (Sec.No4.3). The platform must remain scalable for future growth.

31	**Is document management included in the scope?**	YES. Document management of RLCO records, evidence documents, statutory forms, formal closure documents and audit artefacts is within the scope of this engagement. Specifically:• **RLCO records and evidence documents**: Module 1 Registry Core (Sec.No1.2.1) — Table 1 (ANNEX VII-A) data plus document attachments referenced in the legal basis and supporting evidence fields.• **Document version control and time-aware design** per Sec.No1.3.3.5 (p.192): effective date tracking, historical snapshot retrieval, future-dated changes, automatic deactivation upon expiry. Regulatory time-state machine-readable and queryable via API.• **Formal closure documents** signed under ETO 2002 per Sec.No1.1.3 (p.151) and Sec.No1.3.6.2 e-Sign integration (p.194): each signed document stored with certificate metadata, document hash, timestamp.• **Immutable audit trail** per Sec.No1.1.4 (p.151): seven (7) years minimum retention; protected against alteration or deletion; exportable in machine-readable formats.• **Object storage architecture** for binary documents and attachments — separate datastore per Table 1.3.2-A architectural NFRs.• **Data classification enforcement** per Sec.No1.3.3.4 (p.192) — four tiers: (1) Public; (2) Government Restricted; (3) Internal; (4) Confidential (encrypted at rest, HSM-protected).• **Content Management System (CMS) for public portal** per Module 8 (Sec.No1.2.8).• **PII redaction** for consultation comments before publication (Sec.No1.6.10, p.205).See also S#226/row 229 (data classification enforcement), S#225/row 228 (tamper-evident audit), S#196/row 199 (digital signatures).
32	**Will each department have separate dashboards/workflows? And each department is to see its own dashboard?**	Dashboards will be role based. Per Section VII Sec.No1.1.1.9 (Multi-Jurisdictional Regulatory Framework, p.149), the System MUST give equal operational weight to the regulatory frameworks of all jurisdictions (Federal, ICT, Punjab, Sindh, Khyber Pakhtunkhwa, Balochistan) and 'accommodate jurisdiction-specific configuration, content, templates, workflows, dashboards, escalation rules, and user role assignments without code modification.' Per Sec.No1.6.2 (p.203) and Sec.No1.3.6.2, RBAC with least-privilege enforcement governs user access. Each department/agency works with its own jurisdiction-scoped workflows, work queues, dashboards and reports, subject to the multi-tenant data isolation model (see S#206 / row 209). Specifically: • Module 1 (Registry Core) — agency-scoped RLCO submission, return, validate, publish workflows. • Module 2 (Workflow Engine & Work Queues) — agency-scoped work queues with SLA timers and escalation per Sec.No1.2.3.3. • Module 3 (MIS Dashboards) — agency dashboards plus aggregated views for BOI/AKTU oversight and PMO-level dashboards. • Module 4 (Mapping Enablement) — agency onboarding, focal person nomination, tranche management per agency. • Module 9 (RIS/AKTU Gating) — central or distributed AKTU review queues per Sec.No1.2.9 (see S#48 / row 51). Cross-agency aggregated views are available to BOI/AKTU oversight roles per RBAC; departments see their own scope by default.

33	**Are APIs for such integrations already available, or will they need to be developed as part of the project scope? If there is any middleware server required, who will bear that cost?**	Where the priority integration APIs of Section VII Sec.No1.3.6.2 (p.194) already exist and are available, the Supplier integrates with them. Where they do not exist, are not API-ready, or lack sandbox/credentials, the Supplier is responsible for designing and implementing the integration to recognised standards (REST/JSON, OAuth 2.0/OpenID Connect, SAML 2.0 where applicable), consistent with the integration modes of Sec.No1.3.6.3 (p.194): secure REST APIs for real-time synchronous queries; scheduled ETL pipelines for batch data exchange; CSV/Excel import staging with validation; webhooks and event triggers for asynchronous notifications. Per Sec.No1.3.6.1 (p.194), all PRR services MUST be exposed through a centralised API Gateway with OpenAPI-compliant documentation, canonical data exchange formats, versioned and backward-compatible APIs, and a dedicated sandbox testing environment for integration partners. Middleware: any middleware or integration adapter required to integrate with priority government systems forms part of the software solution and is the Supplier's responsibility. The middleware runs on GoP-provided infrastructure (Sec.No3.0.2; Sec.No3.1–Sec.No3.3 — 'No hardware is procured under this Contract'). The Supplier documents middleware sizing in the Deployment Architecture document under Sec.No2.6.2 for Purchaser provisioning. BOI/AKTU facilitates access to the counterparty agency. Where the counterparty agency is not technically ready and delays the Supplier, see S#259/row 259 for the EoT/compliance treatment.
34	**Could the Purchaser kindly provide further details regarding the expected implementation timeline, milestones, and phase-wise deliverables?**	The implementation timeline and milestones are defined in the Section IX SCC Payment Release Schedule (SCC GCC 12.1, p.385–388), structured as two parallel Activities within the 100-week programme:Activity 1 — PRR System Development Contract (Weeks 2 to 40 + post-go-live):• M1 (Week 2): Project Inception — Project Plan, Architecture, Standards Finalization — 10%• M2 (Week 10): Subsystem 1 — PRR MVP Core operational — 15% (cumulative 25%)• M3 (Week 16): Subsystem 2 — Workflow Engine & Compliance Controls — 10%• M4 (Week 18): Subsystem 3 — MIS Dashboards + Reminders/Escalations — 5%• M5 (Week 20): Subsystem 4 — Public Portal & Consultation System — 10%• M6 (Week 22): Subsystem 5 — BPMN/BPR Workflow Library + Reform Packs — 5%• M7 (Week 24): Subsystem 6 — IT Readiness Assessment — 10%• M8 (Week 26): Subsystem 7 — Cost Impact Assessment (SCM/RIA-lite) — 10%• M9 (Week 28): Subsystem 8 — RIS/AKTU Gatekeeping — 5%• M10 (Week 28): Subsystem 9 — AI Assist modules operational — 5%• M11 (Week 40): Subsystem 10 — Integrated System Acceptance & Operational Go-Live — 10% (cumulative 95%)• M12 (Post Go-Live): Final Documentation, Handover & Stabilization Completion — 5% (cumulative 100%)Activity 2 — PRR RLCO Mapping & Workflow Reform Programme (Weeks 4 to 100): ten milestones PM-1 to PM-10. The full TA workstream Implementation Schedule (Table B) is set out in Section VII.The successful Supplier will submit a detailed Sprint Plan and Agreed Project Plan during inception (Section VII Sec.No1.3.5.5, Sec.No2.6.2) elaborating the phase-wise activities and deliverables consistent with these milestones.

35	**What is the expected duration and scope of post-deployment support, maintenance, and warranty services**	Post-deployment support comprises three components: 1. Warranty / Defect Liability Period: TWO (2) YEARS commencing from issuance of the Final Acceptance Certificate (FAC) following Platform Operational Acceptance (Section IX SCC GCC 29.1, p.394). During the Warranty Period, defect repair, security patches, AI module maintenance and recalibration, and software/licence renewals are included in the Supply and Installation Price (Section VII SIT-2 rows 1.1–1.4, p.252) and MUST NOT be separately priced. 2. Hypercare Support Period (mandatory): minimum three (3) to six (6) months immediately following go-live (Section VII Sec.No5.1.4, p.236), with on-call technical assistance under the warranty SLAs (Table 5.1-A). An extended transition support period of 6–12 months beyond minimum hypercare is strongly recommended for full institutional independence. 3. Post-Warranty Annual Maintenance Contract (AMC): Years 1, 2 and 3 (Y1–Y3) are MANDATORY line items in the Recurrent Cost Sub-Table; proposals failing to quote Y1–Y3 AMC are non-responsive (Section VII SIT-2 Notes, p.251). The Purchaser reserves the right to extend the AMC for up to two (2) additional years (Y4–Y5) at the agreed annual rate (Section VII Sec.No5.2.3, p.238). Post-Warranty Services Period is defined as TWENTY-FOUR (24) MONTHS in SCC GCC 1.1(e)(xiii), p.384. Defect Repair SLAs (Table 5.1-A, p.237): Critical 2 h response / 24 h resolution; High 4 h / 72 h; Medium 1 business day / 10 business days; Low 2 business days / 30 business days.
36	**There are 3 JV allowed, and unlimited Sub-contractors. Sub-contractors will be part of the Consortium. Do its documents have any weightage, and can we allow the subcontractor representative to be authorized to deal with POC from the Consortium?**	Joint Ventures: per Section II PDS ITP 4.1 (p.46), the maximum number of members in a JV is THREE (3). JV members are jointly and severally liable for performance of the Contract. Subcontractors: subcontracting is permitted subject to the ITP and GCC provisions. There is no fixed cap on the number of subcontractors; however, the Supplier is fully responsible for all subcontracted work, must identify subcontractors in the Proposal, and is subject to the Purchaser's no-objection process (including the pre-mobilisation notice requirement under GCC Clause 20). Subcontractor documents are considered for compliance and eligibility evidence as expressly required by the Evaluation and Qualification Criteria (Section III). However, subcontractor experience is NOT credited towards the Proposer's (Lead Bidder/JV's) qualifying experience under Section III Sub-Factor 1.4 unless the criteria expressly provide for it (see also S#83). The authorised representative dealing with the Purchaser MUST be the Proposer (Lead Bidder/JV) as authorised under ITP Clause 21 (Format and Signing of Proposal); a subcontractor cannot substitute for that authorisation.
37	**Ernest's money required or not?**	No.
38	**declaration form will be submitted instead of EM in the Bid ?**	Yes, proposer must submit a signed Proposal-Securing Declaration instead.
39	**IT Readiness Assessment Completion — 100 activities and linked RLCOs (see TA08 in Table B)? Please elaborate on the 100 activities.**	IT Readiness Assessment Completion — 100 activities and linked RLCOs' (referenced as TA-08 in Table B / Implementation Schedule) refers to the IT Readiness Assessments for the 100 priority economic activities across five (5) ISIC Rev.4 sectors and their linked RLCOs, scoped per Section VII Sec.No1.2.11.4 (p.178).The IT Readiness Assessment is governed by Section VII Sec.No1.2.6 Module 6 (p.165). Each readiness record:• MUST be bidirectionally linked to the PRR RLCO Record ID and version, the associated AS-IS and TO-BE workflow artifact IDs and versions, and the agency/jurisdiction/sector (Sec.No1.2.6.1).• Captures structured readiness

		indicators — current digitisation status; service channel mode; existing systems/portals; data availability and ownership; integration readiness (targets, API availability, data standards); authentication and payments readiness; structured constraints and blockers (Sec.No1.2.6.2).• Yields a readiness rating: Quick Win / Medium Complexity / Complex, with optional sub-scores (Sec.No1.2.6.3).• Passes through a draft → approved workflow with versioning and immutable approval records (Sec.No1.2.6.3).• Drives prioritisation for the Pakistan Business Portal (PBP) and phased automation planning under the PRMI Strategy.The specific 100 activities are notified through the 'ISIC Rev.4 Activity Selection Note' (Table 1.2.11-A row TA-D6 / SIT-1 row TA-02, p.179–180, p.247) during the early TA phase.
40	**Who will be responsible for the Cyber security of the provincial /Federal Departments**	Cybersecurity responsibility under this Contract: • PRR Platform and its hosted components: the Supplier is responsible for delivering and securing the PRR System in compliance with the mandatory security regime — Section VII Sec.No1.3.4 (Security Architecture, p.190–192) and Sec.No1.6 (Cyber Security Requirements, p.202–205) — including PSS compliance (Sec.No1.3.4.3); OWASP Top 10 (Sec.No1.6.1); ISO/IEC 27001-aligned controls (Sec.No1.6.8); HSM-based KMS hosted within Pakistan (Sec.No1.3.4.4); mandatory MFA (Sec.No1.6.2); TLS 1.2+/1.3 in transit and at-rest encryption (Sec.No1.6.3); SIEM/centralised logging (Sec.No1.3.4.6); annual third-party VAPT (Sec.No1.6.6); security incident notification within four (4) hours of confirmed detection (Sec.No1.6.7). • PRR integration interfaces with departments: the Supplier secures the PRR side of the interface — including authentication, authorisation, rate limiting, request validation, transport security and audit logging — per Sec.No1.3.6.x and Sec.No1.6.x. • Departments' own internal/legacy systems, networks and endpoints (Federal and Provincial): cybersecurity of these systems remains with the respective department/agency — they are not within the Supplier's scope of supply or contractual responsibility. The Supplier supports cybersecurity capacity-building of BOI/AKTU and DFP users through the training programme (Section VII Sec.No2.4.3, p.213) — including security controls and log interpretation training.
41	**What is the current state of the Pakistan Business Portal (PBP) API is it documented, available for integration testing, and who manages access to it?**	PBP development RFP is yet to be published
42	**How many total RLCOs are estimated to exist across all 6 jurisdictions; federal and provincial combined; based on any preliminary assessment already done?**	There is no fixed aggregate RLCO count across the six jurisdictions.

43	**Will the government provide a dedicated data migration team to assist with bulk import of existing regulations, or is the vendor solely responsible for data collection and digitization?**	Data collection, cleansing, structuring, validation and migration into the PRR are within the Supplier's TA scope per Section VII Sec.No2.5.1 (p.215). The Purchaser/BOI-AKTU provides facilitation (formal engagement letters, DFP nomination support, access to available source data) but does NOT provide a dedicated data migration team to execute the work. Supplier responsibilities (Sec.No2.5.1, Sec.No2.5.2): • Provide services and tools to incorporate all existing regulatory inventory datasets — prior mapping outputs, departmental RLCO lists, regulatory scans, legacy database exports — into the PRR. • Conduct data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, records requiring manual validation. • Bulk import facility (Excel/CSV) with validation rules, error reports, staging area review. • AI-assisted extraction with mandatory Human Verification Queue (Sec.No2.5.2). • Migration runbooks with rollback procedures and cutover plans (Sec.No2.5.3). BOI/AKTU facilitates content validation through DFPs and departmental sign-off (Sec.No1.2.11.2, p.178). Substantive legal correctness of RLCO content remains with the owning regulator (see S#271/row 271, S#161/row 164).
44	**Are there regulations that exist only in physical paper form with no digital version? If so, what is the estimated volume and who is responsible for digitization?**	Some Regulations across the six jurisdictions may exist only in physical/paper form with no readily available digital version. Capture and digitisation of such records is within the Supplier's TA scope per Section VII Sec.No2.5.1–Sec.No2.5.2 (p.215). While digitization of RLCOs will be part of PBP RFP
45	**It is requested to kindly confirm if a standardized classification system for RLCOs is already in use across departments. If available, please share the RLCO classification taxonomy along with any related documentation.**	A standardised classification framework for RLCOs is to be established by the Supplier as per RFP: • ANNEX VII-A Table 1 — Base Template: Minimum Dataset for RLCO Data Collection (Section VII BIM-3, p.323): the authoritative standardised data template minimum dataset that all RLCO records MUST conform to. • ANNEX VII-A Table 2 — Extended Fields: AS-IS governance, statutory forms, lifecycle gaps (Section VII BIM-3). • ISIC Rev.4 sector classification — applied to economic activities (Section VII Sec.No1.2.11.4, p.178). • PRR template versioning — Section VII Sec.No1.2.1.2 (template Draft → Pilot → Approved transitions with versioning and historical retention).
46	**Will there be one central AKTU team reviewing all RLCOs from all 6 jurisdictions, or will each province have its own AKTU counterpart?**	Every Jurisdiction will have it's own AKTU in-line with the enshrined rule-making autonomy given in the constitution of Pakistan. However, the system is envisioned to be a unitary system at the backend and extended to each jurisdiction from the front end to have a clear analysis of mapped RLCOs across jurisdictions at the end of exercise.
47	**Who has the authority to archive or revoke a regulation's Registry ID, and what process is handled through the platform or through a separate legal process?**	Authority to archive or revoke an RLCO Registry ID rests with BOI/AKTU

48	**What is the escalation path when AKTU rejects a regulation? Does it return to the originating department, to a minister, or to a legal review committee?**	The escalation/rejection path is configured within the Module 9 RIS/AKTU Gating Module (Section VII Sec.No1.2.9). When AKTU rejects an RLCO submission, the System returns the record to the originating department/role for remediation. The detailed escalation matrix — including whether further escalation goes to a minister, a legal review committee, an inter-jurisdictional coordination body, or back to the originating department's leadership — is configurable in the platform and will be agreed during Inception based on AKTU's governance arrangements. The Module 9 workflow provides: • Configurable review states (Draft, Under Review, Returned for Revision, Verified/Approved, Archived/Superseded per Sec.No1.2.5.3) with rejection categorisation, comments, and recommended remediation. • Automatic escalation ladder for overdue SLA states per Sec.No1.2.3.3 (p.156–157): Level 1 (DFP) → Level 2 (Agency Head/Authorised Signatory) → Level 3 (BOI/AKTU oversight). • Full audit trail of all rejection and re-submission events stored in the Immutable Audit Store (Sec.No1.1.4, p.151 — 7-year retention). • Multi-channel notifications (email, SMS, in-app) to involved parties. Where AKTU rejection raises substantive legal or policy questions outside the platform workflow, the issue is escalated through the project governance and BOI/AKTU coordination mechanism under the Asaan Karobar Act 2025 (Sec.No1.1.5, p.151) — including, where applicable, to the relevant federal/provincial minister or to a designated review committee. The platform supports the configured arrangement.
49	**Will the government provide official liaison officers in each of the 6 jurisdictions to facilitate agency engagement during the TA programme.**	Departmental Focal Persons (DFPs) are the operational liaison for each participating agency. Per Section VII Sec.No1.3.3.6 (p.193): 'Each participating institution MUST be assigned a Departmental Focal Person (DFP) as the data steward responsible for accuracy, timeliness, and verification of supporting legal documents.' Each participating authority MUST review and certify the accuracy of its regulatory records at least annually or upon any regulatory amendment.Institutional facilitation provided by BOI/AKTU per Section VII Sec.No1.2.11.1 (p.177–178): regulator outreach support, focal person nomination facilitation, tranche sequencing by readiness and priority. Formal engagement letters/legal authority to the relevant federal and provincial departments are provided by BOI to facilitate timely data sharing (see S#147/row 150).The specific operational liaison arrangement per jurisdiction (whether a single jurisdiction-level liaison or per-agency DFPs only) will be confirmed during Inception. The platform supports either model through configurable RBAC and Agency Registry (Sec.No1.2.4 Mapping Enablement Module). The Supplier deploys its TA team to provide practical mapping assistance to DFPs through remote support and in-person visits (Sec.No1.2.11.1).
50	**How will the vendor get access to regulations that are classified, sensitive, or marked restricted? Is there a security clearance process for vendor staff?**	Exclusion of specific entities are identified in Clause 4 of Asaan Karobar Act, 2025. Remaining entities under RFP's scope falls under Right to Access law

51	**After the contract ends at Week 100, who is responsible for training new government officials who join after the project, is a train-the-trainer model expected?**	A train-the-trainer (ToT) model is mandatory for international Suppliers per Section VII Sec.No2.4.3 (p.213), with local technical partnerships and a capacity retention strategy. For all Suppliers, training MUST be treated as knowledge transfer (Sec.No2.4.4, p.213–214): the Supplier MUST demonstrate that BOI/AKTU can independently configure templates, taxonomies, workflows, deadlines, escalations and CMS content; manage queues, moderation and closure certificate workflows; operate dashboards and exports; perform BPMN import/export and workflow artifact approval; run cost and IT readiness assessments; and review and approve AI artifacts and RIS decision packs — all without vendor intervention. Project closure requirements (Sec.No2.4.4): Documentation Completeness Verification; Training Effectiveness Validation; Knowledge Transfer Completion Report; confirmation that GoP teams can operate PRR independently. After the contract ends at Week 100, training of new government officials joining post-project is sustained by: (i) the trained BOI/AKTU trainers and DFPs (per the ToT cascade in Sec.No2.4.5–Sec.No2.4.8); (ii) the transferred training materials — user manuals, quick reference guides, SOP checklists, slide decks, recorded sessions, sample datasets, in editable English-and-Urdu formats (Sec.No2.4.4); (iii) the institutional capacity built under the TA workstream (Sec.No2.4.5 — TA Capacity Building Purpose, p.215). Hypercare and extended transition support apply during the Warranty Period (Sec.No5.1.4, p.236).
52	**Just to clarify the cost of third-party aggregated cost, data hosting cost etc. which will be borne by BOI, would that be the part of financial evaluation?**	Costs explicitly assigned to the Purchaser under the RFP — including provisioning of GoP-provided hosting infrastructure (Section VII Sec.No3.0.2, Sec.No3.1, Sec.No3.2, Sec.No3.3 — 'No hardware is procured under this Contract') — are not part of the Proposer's priced bid and are not evaluated as the Proposer's price. Proposers must price only those items that the RFP assigns to the Supplier, in accordance with the Price Schedule structure (Section IV, p.117 onwards). Recurrent third-party usage costs that the RFP assigns to the Supplier (e.g., AI external API costs only where Purchaser-approved per Sec.No1.6.9 / Sec.No1.2.10.1) must be reflected in the Recurrent Cost Sub-Table with explicit assumptions.
53	**Can the qualifying contract value of US$ 1.5 million refer to the total project value or must it be the participating firm's own share of the contract if delivered as part of consortium and consultancy arrangements?**	Per Section III Sub-Factor 1.4.2 (Specific Experience, p.67–69), the qualifying value of USD 1.5 million each is the value ATTRIBUTABLE TO THE PARTICIPATING FIRM, not the total project value of the cited contract. Specifically: • For a single entity Proposer: the firm itself must demonstrate at least two contracts of similar nature, each of at least USD 1.5 million attributable to it. • For a Joint Venture: 'All members combined — Must meet requirements' per Section III 1.4.2 column; the JV members' qualifying experience is AGGREGATED to meet the requirement. • For a Consortium (treated equivalently to JV per S#82/row 85): aggregate across members. • Where the cited past contract was delivered in a Consortium/JV or sub-consultancy role, the firm's qualifying value is the 'Percentage of participation' share of the total contract value (Section III p.69 documentation requirement). The role 'Sub-consultant' is explicitly recognised at p.69. Supporting evidence per Section III p.68–69: signed contract/work order, completion certificate or client reference letter confirming satisfactory performance, proof of project value and scope, role of the firm, percentage of participation. The total project value of the cited contract by itself is NOT the qualifying value; only the firm's attributable share is.

54	**While we are doing integration with provinces, the data has to be mapped and cleaned, so, is the data already mapped and cleaned? Or do we have to first map and clean the data and then do integration?**	Integration with Provinces with distributed PRR systems is not part of scope. The expectation is to have a distributed front end but singular back end.Existing data is NOT pre-mapped or pre-cleaned exhaustively. Mapping, cleansing, structuring and standardisation of regulatory data are within the Supplier's TA scope per Section VII Sec.No2.5.1 (p.215) read with Sec.No1.2.11.1 (p.177–178).Per Sec.No2.5.1, the Supplier MUST conduct a data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, and records requiring manual validation. Existing data is expected to be of mixed maturity:• Some data structured and digital (databases, spreadsheets) — bulk import via Sec.No2.5.2.• Some semi-structured (PDFs, web pages) — AI-assisted extraction with mandatory Human Verification Queue (Sec.No2.5.2).• Some paper records — manual capture (see S#46/row 49).Provincial data maturity varies across the six jurisdictions (Federal, ICT, Punjab, Sindh, KP, Balochistan); the Supplier MUST design its TA wave-based delivery plan (PM-1 to PM-10) accordingly and price contingency for data-quality variability. The TA Inception & Governance Pack (PM-1 at Week 4) and the data quality assessment outputs inform the mapping work plan.For reference of existing exercises may like to visit1. Punjab eBiz Portal2. Sindh SBOSS Portal3. KP Asaan Karobar Portal4. www.business.gov.pk
55	**Is the list of 100 priority processes finalized for as-is and to-be processes?**	The list of 100 priority economic activities is NOT pre-finalised in the RFP. The list will be jointly finalized on the proposal from supplier in inception report.
56	**Will the government provide training venues and facilities in each province, or must the vendor arrange these independently?**	Venues will be required for conducting workshops as otherwise for handholding the Supplier's team will visit offices and align with DFPs. For Islamabad, the venues management will be responsibility of Supplier and Supplier is encouraged for costing details along-with workshop plan. For provinces, the venue arrangement will be responsibility of Provincial Governments. Training tools, logistics, sandbox environment setup are the Supplier's responsibility. Per Section VII Sec.No2.4.3 (p.213): 'All training tools, logistics, and sandbox environment setup MUST be the Supplier's responsibility.' Training delivery includes initial centralised bootcamp for BOI/AKTU, jurisdiction-wise DFP onboarding sessions aligned to mapping tranches, and recurring refresher clinics during mapping waves (Sec.No2.4.1, p.212). Stakeholder engagement workshops (Sec.No1.2.11.3, p.178) — physical and virtual — are required across all six jurisdictions, with a minimum of one stakeholder session per jurisdiction per mapping wave. Travel, accommodation and logistics costs across jurisdictions are the Supplier's responsibility per Sec.No2.7.1 (p.221) and MUST be reflected in the priced Proposal. Government meeting rooms and access to participating-agency facilities are facilitated by BOI/AKTU as part of the institutional engagement; however, training venue arrangements (booking, AV equipment, refreshments, internet access for hands-on training, sandbox environment) remain the Supplier's responsibility atleast for Islamabad. Where training is delivered virtually, the Supplier provides the platform and technical support. Training

		in both English and Urdu for operational SOPs and user-facing guides per Sec.No2.4.4 (p.213).
57	**Does "Low Code Platform" (10% evaluation score) mean the entire platform must be built on a commercial low-code tool like OutSystems, or does it refer only to the CMS and template manager in M1 and M8?B60:B61**	Low Code' (10% technical weight) does not mandate that the entire platform be built on a single commercial low-code product. It assesses the platform's low-code/no-code capability for rapid configuration (e.g. CMS, template manager, workflow configuration) per Section VII sub-section 1.2.x/13. Any low-code/no-code component used MUST be extensible without vendor lock-in and MUST allow full source-code export and independent deployment.
58	**If government infrastructure is not ready by Week 2 (Project Inception milestone), in this regard does the contract timeline adjust automatically?**	Where BOI/GoP-provided infrastructure or dependencies are not ready by the Project Inception milestone (Week 2) and this delays the Supplier, relief is addressed through the Extension of Time provisions (GCC 40) and the project governance/issue-resolution process; the timeline does not adjust automatically but is managed through agreed change/EoT mechanisms.
59	**Will the PRR connect to an existing centralised National Data Exchange Layer (NDEL) / ESB, or must the Supplier architect custom point-to-point APIs for all six individual jurisdictions?**	The PRR will leverage available national integration infrastructure where it exists; where it does not, the Supplier is responsible for designing and implementing the required integration interfaces/APIs (Section VII 1.3.6.2). The Supplier should architect a standards-based, API-first integration layer rather than ad-hoc point-to-point links. However, the PRR as a system must be designed to extend in jurisdictions as a unitary system not separate installations with integrations
60	**Regarding the Data Conversion and Migration requirements, the Supplier must ingest all existing regulatory inventory datasets provided by the Purchaser. From a high-level data architecture perspective, what is the current format of these legacy inventories? Are they structured relational databases, or unstructured documents (e.g. PDFs, scanned paper, Word documents)?**	The current format of legacy regulatory datasets across the six jurisdictions is expected to be mixed, and the specific format inventory will be confirmed during Inception per Section VII Sec.No2.5.1 (p.215). Expected formats include:• Structured digital: databases (relational/legacy), structured spreadsheets, structured XML/JSON extracts.• Semi-structured: PDFs (text-extractable and scanned), departmental web pages, structured Word documents.• Paper records: print-only regulatory instruments, signed paper documents.• Mixed media: web portals (no API), departmental databases (no export API), gazette publications.Supplier responsibilities (Sec.No2.5.1–Sec.No2.5.3, p.215):• Data quality assessment prior to ingestion.• Bulk import facility — Excel/CSV upload with column mapping to ANNEX VII-A Table 1 fields, validation rules, error reports, staging area review (Sec.No2.5.2).• AI-assisted extraction MAY accelerate structuring of unstructured/semi-structured sources, BUT all AI-extracted outputs MUST be placed in a Human Verification Queue and MUST NOT be promoted to Validated status without human review (Sec.No2.5.2).• Migration runbooks with rollback procedures (Sec.No2.5.3).BOI/AKTU shares all available source datasets and supports access through formal engagement letters (Sec.No1.2.11.1, p.177–178). Proposers should size their TA team with appropriate contingency for the mixed-format reality.
61	**Clause 1.1.4 mandates immutable WORM audit logs, but Section 1.6.10 requires PII redaction tools. How should the Supplier resolve the architectural conflict between strict immutability and the legal requirement to redact sensitive PII?**	There is no architectural conflict between Section VII Sec.No1.1.4 (Audit Log Retention) and Sec.No1.6.10 (Data Privacy Controls). The two requirements operate on distinct data layers: • Audit logs (Sec.No1.1.4, p.151) — complete and immutable audit logs of all system events (RLCO creation, editing, approval, publication, amendment, archival) retained for a minimum of seven (7) years. 'Audit logs MUST be protected against alteration or deletion, and MUST be exportable in machine-readable formats upon request by the Purchaser.' This is an integrity guarantee on the audit trail. • Data Privacy / PII redaction (Sec.No1.6.10, p.205) — 'Redaction tools MUST be available in the moderation console to remove personal or

		sensitive data from consultation comments prior to publication.' This applies to public-facing consultation comments BEFORE they are published, and to operational data layers where data classification (Sec.No1.3.3.4, p.192 — tier 4 Confidential) requires masking for unauthorised users. Reconciliation: • The audit log records the FACT of the redaction event (timestamp, moderator, RLCO/comment ID, action taken) — not the redacted PII content itself. Audit integrity is preserved. • Consultation submissions undergo moderation per Sec.No1.2.8 (Public Portal & CMS); the redacted version is published while the moderation event is logged. • For lawful right-of-erasure requests on USER ACCOUNT DATA (not published RLCO content), the data is pseudonymised/anonymised in operational tables while the audit trail records the action without retaining the source PII. The Supplier MUST design redaction, retention and access controls consistent with both requirements and applicable data protection legislation (per Sec.No1.1.1.3, Sec.No1.6.10).
62	**Clause 1.1.3 and 1.3.6.2 require digital signatures. Must the Supplier bear the financial cost of procuring PKI certificates/tokens for all government users, or solely build the API integration to an existing GoP e-Sign platform?**	Per Section VII Sec.No1.1.3 (p.151), all formal documents generated by the PRR that constitute official government records — including RLCO closure certificates, AKTU review gate decisions, and Regulatory Impact Statement approval records — MUST be digitally signed using certificates from a PTA-recognised Accredited Certification Authority operating under the Electronic Transactions Ordinance 2002 (ETO 2002). The cryptographic signing process MUST be integrated within the system workflow, and signed documents MUST be stored with certificate metadata, document hash and timestamp as part of the immutable audit record. Per Section VII Sec.No1.3.6.2 (p.194), the System MUST integrate with the e-Sign service for digital signatures under ETO 2002 as a priority government system integration. The Supplier's responsibility is: (a) to build the integration with the national e-Sign service / accredited Certification Authority per Sec.No1.3.6.2; (b) to implement the application-level digital-signature workflow per Sec.No1.1.3; (c) to ensure signed records are stored with certificate metadata, hash and timestamp. Where PKI certificates/tokens are issued by an accredited CA (rather than being provisioned by the Supplier), the Supplier integrates with that service. Any recurrent third-party CA cost assigned to the Supplier MUST be reflected in the Recurrent Cost Sub-Table with explicit assumptions (Section IV Price Schedules).

63	**To meet the <1hr RPO and <4hr RTO (Clause 1.3.5.3), does the GoP-provided infrastructure natively support storage-level replication across availability zones, or must the Supplier architect application-level database replication?**	Section VII Sec.No1.3.5.3 (p.193) sets the contractually binding targets: RTO ≤ 4 hours and RPO ≤ 1 hour, to be demonstrated in the annual DR drill. The Supplier MUST architect the solution to meet these targets, irrespective of which infrastructure-level capability is available.Per Sec.No1.3.5.2 (p.193) and Sec.No3.0.2 (p.222), GoP-provided infrastructure is multi-zone across at least two independent availability zones within Pakistan (with multi-city redundancy across at minimum three cities preferred for critical services). Whether storage-level replication across availability zones is natively provided by the designated GoP infrastructure will be confirmed to the selected Supplier post-award.The Supplier's responsibilities:• Where storage-level replication is natively available, the Supplier should leverage it to meet RPO/RTO.• Where storage-level replication is not available, the Supplier MUST implement application/database-level replication (e.g., synchronous primary-replica clustering, log shipping, distributed databases) to meet RPO ≤ 1 h and RTO ≤ 4 h.• Automated backups with point-in-time recovery MUST be configured for the primary registry database; scheduled snapshots MUST be maintained for search indices and analytics warehouses; all backup vaults MUST be encrypted and stored in a separate geographic zone (Sec.No1.3.5.3).• The Supplier documents the DR architecture, replication mechanism, and required infrastructure sizing in the Deployment Architecture document under Sec.No2.6.2 for Purchaser provisioning. Annual DR drills are mandatory, with results submitted to the GoP oversight body within thirty (30) days (Sec.No1.3.5.2).
64	**Clause 39.7 requires incorporating Priority 1/2 feedback at no cost. Will the Purchaser agree to a quantitative cap (e.g. function points or capped hours) to prevent new scope from being misclassified as "feedback"?**	Incorporating Priority 1/2 feedback at no cost (Clause 39.7) applies to defect correction and feedback that falls within the agreed scope/baseline; genuinely new functionality is treated as a change request under the change-control mechanism and the agreed change budget (GCC 39.5). The distinction between feedback and new scope is governed by the approved scope baseline and the Change Control process.
65	**SCC GCC 12.6 states that if the Supplier fails to perform cyber security obligations, 'an assessed amount, as determined by the Project Manager, may be withheld.' Will the Purchaser provide an objective framework or a maximum percentage cap for this withholding, to prevent indefinite or arbitrary payment blocks?**	SCC/GCC 12.6 provides for withholding an assessed amount for failure to meet cyber-security obligations, determined by the Project Manager within the project governance framework and consistent with the SLA regime (Section VII 5.1.1). Such deductions operate alongside, and within, the overall liquidated-damages cap of ten percent (10%) of the Contract Price.
66	**GCC 39.5 states 'Up to 15% of the total contract value may be allocated for Change Requests raised after MVP go-live'. Does the Purchaser intend for bidders to include a 15% funded contingency reserve within their financial bid, or does this clause imply the Supplier must absorb changes up to 15% at no extra cost?**	The 15% allowance under Section VIII GCC Clause 39.5 (p.364) is a CEILING on the value of future approved Change Requests raised after MVP go-live — it is NOT a funded contingency that bidders are expected to include within their financial bid. Bidders price the defined scope of the RFP (Activity 1 and Activity 2 line items in Section IV Forms 3.2 / 3.3 / 3.5 and the System Inventory Tables); approved changes are funded and valued separately within the 15% ceiling. The clause states verbatim: 'Up to 15% of the total contract value may be allocated for Change Requests raised after MVP go-live, subject to BOI written approval for each change and World Bank no objection for cumulative changes exceeding 10% of contract value. Changes beyond 15% require a contract amendment.' Operational rules (GCC 39.6, p.363–364): Supplier impact assessment within 5 business days; BOI decision within 10 business days; approved

		CRs into next available sprint. MVP feedback under GCC 39.7 (p.364) — Priority 1 within 30 days and Priority 2 within 60 days at NO additional cost provided not new features beyond agreed MVP scope. Pre-MVP changes are within delivery scope; post-MVP CRs use the 39.5 budget. Suppliers should not load a contingency reserve into bid prices for the 15% allowance.
67	**Regarding "GoP-provided infrastructure", does the GoP provide the underlying VMs, OS licenses, and baseline endpoint security (e.g. Antivirus/EDR)? Additionally, is the Supplier responsible for OS-level security hardening, or only application/container-level hardening?**	Per Section VII Sec.No3.0.2 (p.222) and Sec.No3.1, Sec.No3.2, Sec.No3.3 (p.223 — 'Not Applicable — No hardware is procured under this Contract'), the GoP-provided infrastructure includes the underlying compute (virtual machines or equivalent), storage, networking, GPU resources, HSM-based KMS (within Pakistan, Sec.No1.3.4.4), and the base data-centre security infrastructure (physical security, perimeter network controls, environmental controls). The split of responsibility is: • Purchaser (GoP-provided): VMs/compute capacity (CPU, RAM); storage with at-rest encryption at the storage layer where available; network connectivity and zone segmentation; data-centre physical and environmental controls; base perimeter/network security. • Supplier: container/runtime images for the PRR components, application-level security hardening, OS-level hardening of the OS images the Supplier deploys (whether bare OS or containerised), patching and configuration management of the Supplier's deployed software, application-level encryption keys (HSM-managed per Sec.No1.3.4.4), application-level WAF/runtime controls, PSS compliance for the PRR System (Sec.No1.3.4.3), OWASP Top 10 (Sec.No1.6.1), ISO/IEC 27001-aligned controls (Sec.No1.6.8). OS licences and baseline endpoint security tooling at the data-centre level are part of GoP-provided infrastructure. The Supplier documents the required OS/baseline image and configuration in the Deployment Architecture document under Sec.No2.6.2. Specifics are confirmed to the selected Supplier during Inception.
68	**To facilitate DevSecOps, CI/CD deployments, and post-go-live maintenance in the Tier-3 data centers, will the GoP provide a secure remote access solution (e.g. VPN or Jump Host) for the Supplier's engineering teams?**	The GoP-provided hosting environment (Section VII Sec.No3.0.2, p.222) accommodates the Supplier's DevSecOps, CI/CD and post-go-live maintenance access through controlled remote access mechanisms — VPN, jump host or equivalent — as required by the mandatory security baseline of Section VII Sec.No1.3.4 (p.190–192) and Sec.No1.6 (p.202–205) and as per approved mechanisms established by Ministry of IT
69	**Given the mandate for localized AI processing, will the GoP-provided infrastructure include the GPU-enabled instances required for LLM/NLU workloads?**	Given the mandate for localised AI processing within government-controlled hosting (Section VII Sec.No1.2.10.1, p.175 and Sec.No1.6.9, p.203), the GPU-enabled infrastructure required for self-hosted LLM/NLU workloads forms part of GoP-provided infrastructure. The Supplier MUST document the GPU sizing, architecture and auto-scaling requirements in the Deployment Architecture document (Sec.No3.0.2, p.222 and Sec.No2.6.2). External AI APIs may be used only with the Purchaser's prior written approval, which extends to cloud-based embedding/inference APIs (Sec.No1.6.9). Where approved, any associated recurrent third-party API cost assigned to the Supplier must be reflected in the Recurrent Cost Sub-Table with explicit assumptions. Note on evaluation: Annex Tech-I Resource Scaling (Section X, p.439) currently evaluates four resource categories (vCPU, RAM, Storage, Network); GPU sizing is declared by the Proposer in the Deployment Architecture for adequacy assessment during technical evaluation.

70	**Section 7, Schedule of Requirements: Clauses TA 08 and TA 09 require the migration of existing regulatory inventory data. How many Registrations, Licences, Certificates, and Other permissions (RLCOs) exist for migration, and in what file format?**	The TA-08 and TA-09 references relate to the TA workstream deliverables under Activity 2. Per Section VII Sec.No2.5.1 (p.215), the Supplier MUST 'provide services and tools to incorporate all existing regulatory inventory datasets provided by the Purchaser — including prior mapping outputs, departmental RLCO lists, regulatory scans, and legacy database exports — into the PRR.' • Data are expected in mixed formats — structured digital (databases, spreadsheets), semi-structured (PDFs, web pages), and paper records — varying by jurisdiction and department. Per Sec.No2.5.2 (p.215), the bulk import facility MUST support Excel and CSV upload with column mapping to Table 1 (ANNEX VII-A) fields, validation rules at import, detailed import error reports, and staging area review. Per Sec.No2.5.1, the Supplier MUST conduct a data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, and records requiring manual validation. Proposers should size their TA effort with appropriate contingency for the data-quality variability across jurisdictions.
71	**Section 7, Schedule of Requirements: Clause TA D11 requires departmental sign off for the Technical Assistance (TA) workstream. What serves as acceptable evidence for departmental sign off in each jurisdiction?**	TA deliverable TA-D11 (Departmental Sign-Off for the TA workstream) — per Table 1.2.11-A (p.179–180) and SIT-1 (p.247) — is evidenced by formal written acceptance of the relevant TA deliverable by the authorised representative of the participating department/jurisdiction. Per Section VII Sec.No1.2.11.2 (p.178), 'the Supplier MUST support BOI/AKTU to implement a formal validation and closure standard operating procedure for each participating agency. • Formal letter of acceptance from the Authorised Signatory of the participating department, on departmental letterhead. • BOI/AKTU signed proxy acceptance where the participating department has delegated sign-off authority (per the configured RBAC and gating workflow). • Workshop minutes signed by the DFP and Agency Head following the validation workshop (Sec.No1.2.11.3) — accepted where supplemented by the platform's workflow approval state. All sign-offs are logged in the Immutable Audit Store with timestamp, signing certificate metadata, document hash per Sec.No1.1.4 (p.151).
72	**Section 7 SIT-2 mentions that "The Purchaser will specify the quantities (person-days) for Technical Services rows 4.1–4.4 and 5.5 in the Proposal Data Sheet prior to issuing this RFP." However the person-days are not provided in the table above, Exactly how many man days of work per year are we expected to provide for each of the four support roles requested?**	Where the SCC/PDS indicates that the Purchaser will specify quantities (person-days) for Technical Services rows in SIT-2 (e.g., rows referenced as 4.1–4.4 and 5.5) but such quantities are not populated in the issued RFP tables, Proposers should: • Propose their own estimated person-days based on the scope of services for each role, consistent with the Service Specifications in Section VII Sec.No5.2 (Technical Support and Post-Deployment Engagement, p.237–238) and Sec.No5.3 (Requirements of Supplier's Technical Team — Post-OA, p.238). • Clearly state the underlying assumptions — service coverage hours, SLA-driven on-call expectations, role allocation, escalation regime — in the Recurrent Cost Sub-Table (Section IV Form 3.5). • Price each role consistent with Section VII Table 2.7-A (Software Development Key Expert Requirements, p.218) and Table 2.7-B (TA Key Expert Requirements, p.219–220) where applicable. Any quantities formally specified by the Purchaser through the consolidated Clarifications process or subsequent Addendum (per ITP Clause 8 — Amendment of RFP Document) will be reflected in the contract finalisation; Proposers should monitor the Clarifications Document for updates.

		In the absence of Purchaser-specified quantities, the Proposer's stated assumptions are the basis for evaluation; quantities may be reconciled during contract negotiation and finalisation.
73	**Section 7, Requirements of the Information System: Clause NFR 006 mandates compliance with Pakistan Security Standards (PSS). Which specific PSS version applies at the Operational Acceptance Test (OAT), and where can we access it?**	Pakistan Security Standards (PSS) compliance is mandatory per Section VII Sec.No1.3.4.3 (p.191). The clause states verbatim that the System and all its components MUST comply with PSS 'as issued and periodically updated by the Ministry of IT and Telecom, The applicable version at the Operational Acceptance Test (OAT) is the version in force at that time, as PSS is a living standard subject to periodic update by the issuing authorities. PSS compliance is a MANDATORY PRE-CONDITION for issuance of the Operational Acceptance Certificate (Sec.No1.3.4.3 and Sec.No1.6 preamble, p.202). The Supplier MUST submit a PSS Compliance Matrix as a mandatory deliverable, mapping each applicable PSS control to the specific implemented security feature or control in the System.
74	**Section 7, Requirements of the Information System: Clause NFR 006 outlines hardware security requirements. Is a Government of Pakistan (GoP) approved cloud based Hardware Security Module (HSM) permitted, or is a physical appliance strictly required?**	Per Section VII Sec.No1.3.4.4 (p.191), the System MUST implement a Hardware Security Module (HSM)-based Key Management System (KMS) hosted within Pakistan. Private encryption keys MUST NOT be accessible to application-layer processes beyond defined and audited roles. Role-based separation of duties for key access, automated key rotation, revocation, and lifecycle management with immutable audit records are mandatory. The RFP requires HSM-based KMS but does not explicitly mandate a particular form factor. A GoP-approved cloud HSM service may be acceptable provided it satisfies in-country hosting, data-residency (Sec.No1.1.1.4, Sec.No3.0.2) and PSS (Sec.No1.3.4.3) requirements; otherwise a physical/dedicated HSM appliance within the GoP environment is expected. The Supplier MUST document the proposed HSM form factor, sizing and KMS architecture in the Deployment Architecture document. Final approval rests with the Purchaser.
75	**Section 9, Special Conditions of Contract: Clause GCC 28.2 outlines Liquidated Damages (LD) but does not insert the exact rate. What is the exact LD rate for Activity 1 and Activity 2?**	Liquidated Damages for delay in achieving Operational Acceptance shall be charged at a rate of 0.1% of the Contract Price per week of delay.
76	**Section 9, Special Conditions of Contract: Clause GCC 28.2 outlines a 10 percent cap on LDs. Does the 10 percent cap apply to the total contract price or to each activity independently?**	10 % cap apply separately to Activity 1 (PRR Platform): maximum 10% of Activity 1 price and Activity 2 (TA Workstream): maximum 10% of Activity 2 price'.

77	**Section 7, Requirements of the Information System: Hosting Infrastructure Requirements mentions cloud hosting possibilities. Are any public cloud providers currently GoP approved?**	Hosting is on GoP-provided infrastructure — either a national government data centre OR a GoP-approved public cloud environment — meeting Tier-3 or higher standards within Pakistan, multi-zone across at least two independent availability zones (Section VII Sec.No3.0.2, p.222). The solution MUST be cloud-agnostic per Sec.No1.1.1.7 (p.149) with no dependency on a vendor-operated cloud not approved by the Government of Pakistan. The RFP does not list specific GoP-approved public cloud providers. The specific designated hosting environment for the PRR will be confirmed to the selected Supplier by the Purchaser post-award. The Supplier: • Documents the required infrastructure sizing, network/storage specifications, and auto-scaling thresholds in the Deployment Architecture document under Sec.No2.6.2. • Designs the solution as cloud-agnostic — containerised deployment (Kubernetes or equivalent, Sec.No3.4.1, p.223), portable data models, OpenAPI-compliant APIs (Sec.No1.3.6.1), and infrastructure-as-code (Sec.No1.3.2.6, p.190). • Ensures full GoP operational independence per Sec.No1.3.2.6 and Sec.NoG.3 (p.284). All PRR data — RLCO records, metadata, evidence documents, consultation submissions, audit logs, cryptographic keys, backups — MUST be hosted exclusively within Pakistan in compliance with national data residency requirements (Table 1.3.2-A; Sec.No1.1.1.4 Pakistan Data Protection Legislation, Sec.No3.0.2).
78	**Please clarify if the procurement and provisioning of physical infrastructure (including servers, storage, networking, GPUs and etc) are out of scope of this RFP, and that our financial bid should strictly exclude all hardware costs.**	Confirmed. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) each state verbatim: 'Not Applicable — No hardware is procured under this Contract.' This covers computing hardware, networking and communications, and ancillary hardware. The financial bid must therefore exclude procurement of servers, storage, networking, GPUs and ancillary hardware. All active software components and data MUST be hosted on GoP-provided infrastructure (national government data centre or GoP-approved public cloud) meeting Tier-3 or higher standards within Pakistan and configured for multi-zone availability across at least two independent availability zones (Section VII Sec.No3.0.2, p.222; Sec.No1.1.1.7, p.149). The Supplier's responsibility is limited to documenting the required infrastructure sizing, network and storage specifications, and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2, so that the Purchaser can arrange provisioning. The solution MUST be cloud-agnostic with no dependency on a vendor-operated cloud not approved by the GoP (Sec.No1.1.1.7).
79	**It is mentioned in the RFB that the Proposer is allowed to submit a bid as a Consortium. However, the relevant form/table provided in the RFB refers specifically to a Joint Venture (JV). We would like to clarify whether, in the case of bidding as a Consortium, the same Joint Venture table may be filled by providing consortium details. We understand that a Consortium is permitted under this bidding process and request confirmation that submission using the JV table**	The World Bank only recognizes a formal Joint Venture (JV) with joint and several liability. An informal consortium is not permitted. You must use the JV forms provided in the RFP.

	format will be acceptable for a Consortium arrangement	
80	**Please define a Consortium based on standard understanding and clarify how the experience of consortium members will be considered for the Lead Bidder participating in the bid.**	The standard and acceptable structure for a joint bidding arrangement is a Joint Venture (JV) . While "consortium" is sometimes used informally, the World Bank's official documentation refers exclusively to a Joint Venture. An informal consortium with no legally binding agreement is not permitted. The Joint Venture (JV) is the only recognized structure for joint bidding. You must use the JV forms provided, and all partners must accept joint and several liability.
81	**As sub-contracting is permitted under the RFP, please clarify whether the experience of sub-contractors will be considered for the Lead Bidder's experience evaluation**	No, the experience of subcontractors will not be considered for the Lead Bidder's experience evaluation. Only the qualifications and experience of the Joint Venture (JV) members carry weight; subcontractors have zero weightage in technical scoring.
82	**Clause 3.1, 3.2, and 3.3 state that no computing, network, or ancillary hardware is to be procured under this Contract. This implies that the bidder is not required to quote for compute, storage, security, or ancillary hardware, and that provisioning of the required hardware infrastructure will be the responsibility of the Purchaser. Please clarify how potential delays in the provisioning or availability of the required hardware infrastructure at the Purchaser's end will be handled, particularly with respect to:** **Project timelines and milestones** **Service commencement dates** **Bidder liability and penalties (if any)**	Confirmed. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) each state verbatim: 'Not Applicable — No hardware is procured under this Contract.' Bidders do not quote for compute, storage, security, networking or ancillary hardware. Provisioning of the required hardware infrastructure is the Purchaser's responsibility on GoP-provided Tier-3+ infrastructure (Section VII Sec.No3.0.2, p.222; Sec.No1.1.1.7, p.149). The Supplier documents the required infrastructure sizing and architecture in the Deployment Architecture document (Sec.No2.6.2). Impact of delays in Purchaser-side provisioning on project timelines, service-commencement dates, and supplier liability: any delay or shortfall that prevents the Supplier from meeting milestone dates and is beyond the Supplier's control may be addressed by the Supplier through the Extension-of-Time provisions in Section VIII GCC Clause 40 (p.364), supported by the project governance and issue-resolution process. Where such delays cause the Supplier to miss Operational Acceptance, LDs are only payable for delay within the Supplier's control (GCC 28.2).
83	**Apart from the production infrastructure, the customer is responsible for providing separate Test and Development (Test/Dev) environments to support prototype development and integration testing with customer-provided data sets. Please advise.**	Per Section VII Sec.No1.3.5.1 (p.192–193), the System MUST operate across FOUR defined environments: Development (for feature development, unit testing, schema evolution, automated validation); Staging/UAT (for integration testing across all portals, performance testing, user acceptance); Production (live national environment with HA and isolation of public read traffic from government write operations); and Disaster Recovery (maintained, tested and activated-on-demand DR environment with RTO/RPO targets per Sec.No1.3.5.3). Section VII Sec.No1.3.4.2 (p.191) additionally specifies, as a mandatory security baseline, 'environment segregation across DEV, UAT, and PROD'. SIT-1 (p.250) requires deployment packages across DEV, UAT and PROD for the supplied subsystems. First two DEV and UAT are encouraged to be used from Supplier side while PROD and DR environments are part of the GoP-provided infrastructure (Section VII Sec.No3.0.2; Sec.No3.1; Sec.No3.2; Sec.No3.3 — 'No hardware is procured under this Contract'). The Supplier documents the required sizing for each environment in the Deployment Architecture document (Sec.No2.6.2).

84	**Clause 3.0.2 states that all active software components and data must be hosted on GoP-provided infrastructure meeting Tier-3 (or higher) data centre standards within Pakistan, and that the Supplier must document infrastructure sizing, network and storage specifications, and autoscaling thresholds in the Deployment Architecture document.** **In this context, please clarify the following:**	Per Section VII Sec.No3.0.2 (p.222), all active software components and data MUST be hosted on GoP-provided infrastructure meeting the following minimum standards: Tier-3 or higher data centres physically located within Pakistan in compliance with national data residency requirements; electrical power supply conforming to the standards applicable to the GoP data centre selected for hosting; multi-zone high availability across at least two independent availability zones within Pakistan; and environmental controls (temperature, humidity, dust management) appropriate for the data centre classification. The solution MUST be cloud-agnostic per Sec.No1.1.1.7 (p.149). Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) state verbatim: 'Not Applicable — No hardware is procured under this Contract.' Procurement and provisioning of compute, storage, network, security and GPU infrastructure is the Purchaser's responsibility on GoP-provided infrastructure. The HSM-based KMS within Pakistan (Sec.No1.3.4.4) is also part of GoP-provided infrastructure. The Supplier MUST document the required infrastructure sizing, network and storage specifications, and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2. The Supplier's components run on the GoP-provided platform via containerised deployment per Sec.No3.4.1 (p.224).
85	**Availability and Readiness of Infrastructure** **Will the GoP-provided hosting infrastructure (including required availability zones, network connectivity, and storage services) be fully provisioned and made available to the Supplier prior to the commencement of deployment and configuration activities?**	The Purchaser will provide the GoP-provided hosting infrastructure (availability zones, network connectivity, storage services, HSM-based KMS, and GPU resources required for the AI Assist Module) in line with the documented Supplier requirements and the project schedule, to support the Section IX SCC Activity 1 milestone dates (M1–M12, Section IX SCC GCC 12.1, p.385–387). The Supplier delivers the Deployment Architecture document (Sec.No2.6.2) early in the Contract, documenting the required infrastructure sizing, network and storage specifications, auto-scaling thresholds, and HSM/GPU specifications. The Purchaser uses this document to plan provisioning. Any shortfall in, or delay to, Purchaser-side provisioning that prevents the Supplier from meeting milestone dates and is beyond the Supplier's control is managed through Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), through the project governance and notification process under GCC 18.2 and GCC 19. Liquidated Damages under GCC 28.2 are only payable for delay within the Supplier's control.

86	**Responsibility Boundaries** **While the Supplier is required to document sizing and architecture requirements, kindly confirm whether:** **Procurement, provisioning, and operational readiness of compute, storage, network, and security infrastructure remain entirely the responsibility of the BoI, and The Supplier's responsibility is limited to deployment, configuration, and tuning of the software stack on the provided infrastructure.**	Confirmed in principle. Per Section VII Sec.No3.0.2 (p.222), Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) and Sec.No1.1.1.7 (p.149): **Purchaser (GoP) responsibilities** — procurement, provisioning, and operational readiness of: • Compute (virtual machines / Kubernetes nodes / GPU compute as documented) • Storage (block, object, database storage) • Network connectivity and zone segmentation; multi-zone availability across ≥ 2 independent availability zones within Pakistan • Tier-3 data centre / GoP-approved cloud environment within Pakistan • HSM-based KMS within Pakistan (Sec.No1.3.4.4, p.191) • Base perimeter/network security and data-centre physical/environmental controls • Government SOC (where exists; otherwise Supplier-operated SIEM — see S#222/row 225) • Access mechanisms (VPN / jump host / bastion) for Supplier engineering access (see S#70/row 73) **Supplier responsibilities**: • Documenting required infrastructure sizing, network/storage specifications, auto-scaling thresholds in the Deployment Architecture document under Sec.No2.6.2. • Containerised software deployment (Sec.No3.4.1) including all application components. • Application-level security hardening, OS hardening of Supplier images, application encryption keys (HSM-managed). • Application-level WAF/runtime controls, configuration management, patching of Supplier-deployed software. • PSS compliance (Sec.No1.3.4.3), OWASP Top 10 (Sec.No1.6.1), ISO/IEC 27001-aligned controls (Sec.No1.6.8). • SIEM/centralised logging operation (Sec.No1.3.4.6) — see S#222/row 225. • Infrastructure-as-Code for environment configuration (Sec.No1.3.2.6). Where Purchaser-side provisioning is delayed and impacts the Supplier's milestones, EoT relief via Section VIII GCC Clause 40 (p.364) applies (see S#87/row 90, S#89/row 92, S#60/row 63).
87	**Delays and Impact on Project TimelineIn case of any delay or shortfall in the provisioning of BoI-provided infrastructure that does not meet the documented requirements (e.g., Tier-3 compliance, multi-zone availability), please clarify:How such delays will impact project milestones and delivery timelinesWhether any penalties or liabilities will be waived or timelines extended accordingly**	Where a delay or shortfall in BOI/GoP-provided infrastructure (e.g., failure to meet the Supplier's documented Tier-3 / multi-zone availability requirements per Section VII Sec.No3.0.2) impacts the project schedule and is beyond the Supplier's control, the Supplier is entitled to seek schedule relief under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), through the project governance and issue-resolution process. LDs under GCC 28.2 are only payable for delay within the Supplier's control. Documentary evidence of dependency, notification under GCC 18.2 and GCC 19, and impact analysis on the Implementation Schedule must be submitted to support an EoT request. The Purchaser will consider such requests through the formal change-management/EoT process; timelines are not adjusted automatically.

88	**Deviation Handling** **If the provided infrastructure does not fully meet the documented sizing or availability requirements submitted by the Supplier, what will be the accepted change-management or escalation mechanism?**	Where Purchaser-provided infrastructure does not fully meet the Supplier's documented sizing or availability requirements, the deviation is handled through the project governance structure under Section VII Sec.No1.4 (Systems Administration and Management) read with Sec.No2.6.2 (Architecture & Design / Agreed Project Plan): • **Documentation**: the Supplier raises a formal Deviation Notice describing the gap, expected impact (on functionality, performance, availability, security or schedule), proposed mitigation, and residual risk. • **Joint review**: BOI/AKTU, the Supplier, and where applicable the Hosting Service Provider, jointly review the deviation and decide on: – Provisioning enhancement (Purchaser-side action to close the gap). – Compensating control / architectural change (Supplier-side adjustment with no scope/cost impact where feasible). – Formal Change Request (where the deviation requires scope/cost/schedule change) per Section VIII GCC Clause 39 (p.362) and SCC GCC 39.2.1 / 39.5 (15% budget ceiling, p.364). • **Schedule relief**: where the deviation impacts milestone delivery and is beyond the Supplier's control, EoT relief is available via Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), with notification under GCC 18.2 and GCC 19. • **Liability**: LDs under GCC 28.2 (p.342) only apply for delay within the Supplier's control. • All deviation notices and resolutions logged in the project register and Immutable Audit Store (Sec.No1.1.4, p.151). See also S#87/row 90, S#88/row 91, S#60/row 63.
89	**In case of JV bidding, our understanding is that both parties shall submit the required JV forms along with all relevant information at the time of bid submission in accordance with the RFB requirements. A formal, legally binding JV agreement will be executed upon being declared the successful bidder and shall be submitted prior to contract signing.** **Kindly confirm if our understanding is correct, or advise if a duly executed JV agreement is required at the time of bid submission**	Confirmed. The procedural framework for JV/Consortium bidding is: • At proposal submission: both/all members MUST submit Section IV 'FORM ELI 1.1.2 — Proposer's JV Members Information Form' for each member, together with the Joint Venture/Consortium agreement OR a signed Letter of Intent to enter into a Joint Venture if successful. Each member separately completes the relevant Section III qualification forms (Form CON-2 Historical Contract Non-Performance, Form CON-3 SEA/SH, Form EXP 1.4.x Experience, Form CCC, Form FIN 1.3.x as applicable per Section III Sub-Factor 1.1, 1.2, 1.3). • At contract signing: a formally executed, legally binding JV/Consortium agreement is required if the Proposer is successful — per ITP Clause 4 (Eligible Proposers) and the Letter of Acceptance procedures in Section X (p.398). • All JV/Consortium members are jointly and severally liable for the Contract. • Maximum number of JV/Consortium members: THREE (3) per Section II PDS ITP 4.1 (p.46). • Beneficial Ownership Disclosure (Section X) is required for each JV member. • See also S#82/row 85 (Consortium = JV) and S#181/row 184 (member experience aggregation).

90	**Are you also looking block chain base solution same like super app tender by NITB/ DEEP ?**	The PRR is a national regulatory registry as defined in Section VII — Purchaser's Requirements. A blockchain or distributed-ledger solution is NOT specifically mandated and is NOT a requirement of this RFP. Mandatory architectural requirements: • Microservices architecture with the minimum decomposition in Table 1.3.1-A (Section VII Sec.No1.3.1, p.187) — 16 mandatory microservices. • Containerised deployment using Kubernetes or equivalent (Sec.No3.4.1, p.223). • Seven distinct datastores per Sec.No1.3.3.1 (p.189) — Primary Registry DB (relational); Document/Artifact Store; Search Index; Analytics Warehouse; BPMN Repository; Vector Database; Immutable Audit Store. • Immutable audit log per Sec.No1.1.4 (p.151) — 7-year retention; tamper-evident; protected against alteration or deletion. • Cloud-agnostic operation (Sec.No1.1.1.7, p.149). The immutable audit-log integrity requirement (Sec.No1.1.4) can be met with conventional approaches — cryptographic hash chaining, append-only object storage with WORM controls, immutable cloud object versioning — without requiring a distributed ledger (see S#225/row 228). Where a Proposer wishes to use a blockchain/DLT component for a specific function within its design, this is at the Proposer's discretion subject to the Sec.NoG.3 IP regime (perpetual government-use licence; full source-code transfer; no vendor lock-in; cloud-agnostic operation) and the Sec.No1.6.9 prohibition on data leaving GoP-controlled hosting without prior written Purchaser approval.
91	**As DEEP data base is Oracle DB , what is your focus on DB and can we propose our technology stacks or you have some expectations or define ?**	There is no mandated database product. Proposers may propose their own technology stack — open-source (e.g., PostgreSQL, MySQL, MariaDB) or commercial (e.g., Oracle Database, Microsoft SQL Server, IBM Db2) — provided it meets the Section VII Sec.No1.3 architectural mandates:• **Microservices decomposition** per Table 1.3.1-A (Sec.No1.3.1, p.187) and 7 distinct datastores per Sec.No1.3.3.1 (p.189): Primary Registry Database (relational transactional store) is one of the 7 mandated datastores.• **High availability with replication** across availability zones; **encryption at rest** for all data including database (Sec.No1.6.3); **point-in-time recovery (PITR)** for the primary registry database (Sec.No1.3.3.1).• **HSM-based KMS** within Pakistan for encryption keys (Sec.No1.3.4.4, p.191).• **Containerised deployment** (Sec.No3.4.1, p.223) — database deployment compatible with the containerised model.• **No vendor lock-in** (Sec.NoG.3.1, Sec.NoG.3.7); operational independence (Sec.NoG.3.8) — GoP MUST be able to engage third parties for maintenance/enhancement and transfer the System.• **Source-code escrow** for any pre-existing proprietary database component used as part of PRR-specific custom code base (Sec.NoG.3.6).For commercial database choice (e.g., Oracle Database): declare in Technical Proposal per Sec.NoG.3.5; perpetual government-use licence per SCC GCC 15.4 (p.390); recurrent licence/support costs reflected in the Recurrent Cost Sub-Table (Section IV Form 3.5). For pre-existing GoP-licensed enterprise databases (where the Purchaser separately holds licences), the Supplier should state the assumption clearly. Note: the DEEP project's existing Oracle DB is NOT a substantive constraint for the PRR architecture — the Supplier proposes its own technology stack within the Sec.No1.3 mandates.

92	**Can we propose online training LMS along with for technical proposal ? 2nd hardwr**	Proposers MAY propose a Learning Management System (LMS) capability as part of the Technical Proposal, where it supports the training and capacity-building requirements under Section VII Sec.No2.4 (Training and Training Materials, p.212–215). The LMS would support the Training Plan (Sec.No2.4.1), training delivery and recording (Sec.No2.4.3), training materials repository (Sec.No2.4.4), and the TA capacity-building programme (Sec.No2.4.5–Sec.No2.4.8). If proposed, the LMS: • Operates within the GoP-provided hosting environment (Sec.No3.0.2) and complies with the security regime (Sec.No1.3.4 Security Architecture, Sec.No1.6 Cyber Security Requirements). • Supports both English and Urdu content per Sec.No3.0.1 (p.222). • Complies with the IP regime (Sec.NoG.3) — full ownership of LMS configuration and content vests in GoP; pre-existing proprietary LMS components require declaration with perpetual government-use licensing per SCC GCC 15.4 (p.390). • Is reflected as a software-component line item within the Supply and Installation pricing structure (Section IV Forms 3.2 / 3.4) and any recurrent licence/hosting costs in the Recurrent Cost Sub-Table (Form 3.5). Note on the bidder's reference to 'hardware': Per Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223): 'Not Applicable — No hardware is procured under this Contract.' Bidders do NOT quote for hardware. See S#80/row 83.
93	**Please share response of quries Cloud Infrastructure: Multi-cloud and hybrid cloud deployment capabilities**	The PRR is hosted on GoP-provided infrastructure per Section VII Sec.No3.0.2 (p.222) — either a national government data centre OR a GoP-approved public cloud environment — meeting Tier-3 or higher standards within Pakistan, multi-zone across at least two independent availability zones within Pakistan. Per Sec.No1.1.1.7 (p.149), the solution MUST be cloud-agnostic with no dependency on a vendor-operated cloud not approved by the Government of Pakistan. Multi-cloud / hybrid cloud deployment IS NOT a mandatory requirement of this RFP. The applicable model is: • Single designated GoP-provided environment (national government data centre OR GoP-approved cloud), confirmed to the selected Supplier post-award. • Multi-zone (≥ 2 AZs) within that environment within Pakistan for HA/DR. • Multi-city redundancy across at minimum three cities preferred for critical services (Sec.No1.3.5.2, p.193). • Cloud-agnostic architecture (Sec.No1.1.1.7) — portable container images, IaC for environment configuration (Sec.No1.3.2.6, p.190), OpenAPI-compliant APIs (Sec.No1.3.6.1). The cloud-agnostic mandate enables the Government of Pakistan to migrate the PRR to a different GoP-approved cloud environment or to on-premises GoP data centre infrastructure without re-development, supporting GoP's operational independence (Sec.NoG.3.8, p.284). The Supplier documents portability and exit-strategy provisions in the Architecture document under Sec.No2.6.2. See also S#79/row 82, S#86/row 89, S#210/row 213.

94	**Cybersecurity: Zero Trust architecture, SOC, endpoint protection, and compliance**	Security requirements are set out in Section VII Sec.No1.3.4 (Security Architecture, p.190–192) and Sec.No1.6 (Cyber Security Requirements, p.202–205); they are contractually binding:• Zero-Trust segmentation — Sec.No1.3.4.1 (p.190): four distinct security zones (Public, Application, Protected Data, Integration) with strict policy controls, private subnets, least-privilege routing; no service communicates across zone boundaries without explicit authorisation.• SOC / SIEM monitoring — Sec.No1.3.4.6 (p.191) and Sec.No1.6.7 (p.203): centralised logging aggregating logs from all gateways, microservices, workflow engine, search cluster and IAM service; tamper-evident controls; retention in the Immutable Audit Store; distributed tracing end-to-end; SIEM-based security monitoring with privileged session logging; real-time alerts for outages, suspicious access and rate-limit breaches; 4-hour security incident notification.• Endpoint protection and infrastructure security baseline — Sec.No1.3.4.2 (p.191): WAF; DDoS protection; SSO with mandatory MFA for all government portal users; RBAC with least-privilege enforcement; TLS 1.2+/1.3; secrets vault; environment segregation across DEV/UAT/PROD; encrypted backup vaults; rehearsed DR plan.• Compliance: PSS (Sec.No1.3.4.3); OWASP Top 10 (Sec.No1.6.1); ISO/IEC 27001-aligned controls (Sec.No1.6.8); PECA 2016, Pakistan Data Protection legislation, PTA regulatory requirements (Sec.No1.6.8); HSM-based KMS within Pakistan (Sec.No1.3.4.4); Post-Quantum Cryptography readiness with upgrade capability by 2027 or earlier (Sec.No1.3.4.5).Privileged Access Management and least-privilege enforcement per Sec.No1.6.5. Annual third-party VAPT per Sec.No1.6.6: Critical/High remediation ≤30 days, Medium ≤90 days.
95	**Enterprise Applications: Custom ERP, CRM, workflow automation, and portal development**	The functional scope of this RFP is set out in Section VII — Purchaser's Requirements. Specifically, the Supplier MUST deliver the ten (10) mandatory PRR modules per Section VII Sec.No1.2 (p.155–177): • Module 1 — Registry Core (Sec.No1.2.1) • Module 2 — Workflow Engine and Work Queues (Sec.No1.2.2, Sec.No1.2.3) • Module 3 — MIS Dashboards and Reporting (Sec.No1.2.3) • Module 4 — Mapping Enablement (Sec.No1.2.4) • Module 5 — BPR / AS-IS / TO-BE (Sec.No1.2.5) • Module 6 — IT Readiness Assessment (Sec.No1.2.6) • Module 7 — Cost Impact Assessment SCM/RIA-lite (Sec.No1.2.7) • Module 8 — Public Portal and CMS (Sec.No1.2.8) • Module 9 — RIS/AKTU Gating (mandatory subsystem) (Sec.No1.2.9) • Module 10 — AI Assist (mandatory subsystem) (Sec.No1.2.10) Architectural mandates in Section VII Sec.No1.3 (p.187–195): microservices decomposition (Table 1.3.1-A); OpenAPI-compliant APIs (Sec.No1.3.6.1); containerised deployment (Sec.No3.4.1); cloud-agnostic (Sec.No1.1.1.7); no vendor lock-in (Sec.NoG.3); HSM-based KMS within Pakistan (Sec.No1.3.4.4). Standard Software Specifications in Sec.No3.4 (p.223+) cover BPM/workflow engine (Sec.No3.4.8), LCNC platform (Sec.No3.4.9), Form Builder (Sec.No3.4.10). Custom ERP, CRM and generic portal-development capabilities of the Supplier's wider portfolio are relevant to demonstrate experience under Section III Sub-Factor 1.4 (Specific Experience). For this engagement, deliverables must conform to the PRR-specific requirements of Section VII.

96	**Data & Analytics: Business intelligence, big data platforms, and AI/ML solutions**	Data & Analytics requirements are within scope and are specified across Section VII Sec.No1.2 and Sec.No1.3: • **Analytics Warehouse** (Sec.No1.3.3.1, p.189): a separate reporting store for management dashboards and KPI reporting, isolated from the transactional database. No dashboard or reporting workload MUST directly query the primary transactional database. • **MIS Dashboards and Reporting** (Module 3, Sec.No1.2.3): real-time and historical operational dashboards. • **IT Readiness dashboards** (Sec.No1.2.6.4): readiness distribution by jurisdiction, agency, sector; top blockers report; integration dependency matrix. • **Cost Impact reporting** (Sec.No1.2.7): AS-IS vs TO-BE quantified impact reports. • **Public Portal analytics** (Module 8, Sec.No1.2.8): consultation participation, RLCO views, search analytics. • **AI Assist Module** (Module 10, Sec.No1.2.10): NLU classification, sentiment analysis, similarity/conflict detection, regulatory knowledge graph queries (Sec.No1.2.10.6); workflow generation assistance (Sec.No1.2.10.x); AI governance per Sec.No1.6.9 (advisory only, human-in-the-loop, no external AI APIs without prior written Purchaser approval). • **Vector Database** (Sec.No1.3.3.1): for AI-assisted semantic similarity and knowledge graph queries. • **Real-User Monitoring (RUM) and APM** (Sec.No1.5.6) for system observability. AI/ML solutions operate exclusively within GoP-controlled hosting (Sec.No1.6.9). All AI models, prompts, scoring logic and orchestration logic developed under the Contract are GoP IP (Sec.NoG.3.5).
97	**Networking & Hardware: NVIDIA-based server solutions, data centers, and structured cabling**	**No hardware is procured under this Contract.** Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) each state verbatim: 'Not Applicable — No hardware is procured under this Contract.' This covers networking and server hardware (including NVIDIA-based GPU servers for AI workloads), data centre infrastructure, and structured cabling.Hardware infrastructure for the PRR is part of GoP-provided infrastructure (Section VII Sec.No3.0.2, p.222; Sec.No1.1.1.7, p.149):• Tier-3 or higher data centres within Pakistan, multi-zone across ≥ 2 AZs.• Compute (including any GPU compute required for self-hosted AI workloads — see S#71/row 74, S#194/row 197).• Storage, networking and security infrastructure.• HSM-based KMS within Pakistan (Sec.No1.3.4.4).Supplier responsibilities:• Document required infrastructure sizing, including GPU sizing/architecture, in the Deployment Architecture document under Sec.No2.6.2.• Containerised software deployment (Sec.No3.4.1) on the GoP-provided platform.• Cloud-agnostic operation enabling portability between GoP-provided environments.Specific networking, data-centre or GPU brand/model preferences are NOT relevant to the Supplier's bid — the Supplier proposes sizing/architecture, the Purchaser provisions. See also S#80/row 83, S#117/row 120 (next-door duplicate).

98	**Government Integration: NADRA CNIC, FBR, SBP Raast, SECP, and inter-agency APIs**	The mandatory priority government integrations are listed in Section VII Sec.No1.3.6.2 (p.194): • NADRA and government SSO platforms (identity verification and authentication) • Government email and SMS gateways (notification delivery) • Pakistan Gazette and official publication systems (Gazette reference capture and linkage) • e-Sign service for digital signatures under the Electronic Transactions Ordinance 2002 (ETO 2002) • Provincial government systems and e-governance platforms where available An open, read-only API layer for published RLCO data MUST be provided for future integration with additional government portals, including the Pakistan Business Portal (PBP). Integration modes per Sec.No1.3.6.3 (p.194): secure REST APIs for real-time synchronous queries; scheduled ETL pipelines for batch data exchange; CSV/Excel import staging with validation; webhooks/event triggers for asynchronous notifications. FBR, SBP Raast and SECP are not listed as mandatory priority integrations in Sec.No1.3.6.2. Where they are required for a specific RLCO workflow identified during inception, integration is approached through the BOI/AKTU governance and may be covered by the GCC 39 Change Control process. The Supplier is responsible for the technical integration with the mandatory priority systems; BOI/AKTU facilitates access to the relevant agencies and provides integration documents during Inception. Readiness/availability of each system will be confirmed at that time.
99	**How many maxium sub contractor are allowed in the bid .**	There is no fixed cap on the maximum number of subcontractors in a bid. Subcontracting is permitted subject to the ITP, GCC and SCC provisions, including: • The Supplier remains fully responsible for all subcontracted work (Section VIII GCC Clause 20, p.327). • The Supplier MUST identify each proposed subcontractor and the scope subcontracted in the Proposal, on the Subcontractor's Agreement form in Section IV (p.115). • The Supplier MUST notify and obtain the Purchaser's no-objection prior to engaging each subcontractor (the 28-day pre-mobilisation notice requirement under GCC Clause 20). • Subcontractor eligibility under Section V — Eligible Countries (p.133) and ITP 4 applies. The maximum number of JV/Consortium MEMBERS, however, is capped at THREE (3) per Section II PDS ITP 4.1 (p.46) — a JV cap is distinct from the subcontractor regime. Subcontractor experience is NOT credited towards the Proposer's qualifying experience under Section III Sub-Factor 1.4 unless the Evaluation Criteria expressly provide for it (see S#83).

100	**In "BIM 5" All mandatory standards need to be addressed in the architecture compliance matrix?**	YES. All mandatory standards relevant to the architecture MUST be addressed in the Architecture Compliance Matrix delivered under Section VII Sec.No2.6.2 (Architecture & Design / Agreed Project Plan). BIM-5 (Background and Informational Material 5) provides the reference framework. The Architecture Compliance Matrix MUST address all mandatory standards including:• **Legal and Regulatory** (Sec.No1.1.1, p.149): ETO 2002; PECA 2016; Pakistan Data Protection Legislation; PTA Regulations; National Cybersecurity Policy; Asaan Karobar Act 2025; Digital Nation Pakistan Act; WCAG 2.1 AA; ISO/IEC 27001.• **Architectural** (Sec.No1.3): microservices (Table 1.3.1-A); 4 environments (Sec.No1.3.5.1); 7 datastores (Sec.No1.3.3.1); containerised deployment (Sec.No3.4.1); cloud-agnostic (Sec.No1.1.1.7); OpenAPI (Sec.No1.3.6.1); IaC (Sec.No1.3.2.6).• **Security** (Sec.No1.3.4, Sec.No1.6): Zero-Trust; PSS compliance; HSM-based KMS; OWASP Top 10; ISO/IEC 27001-aligned; PQC readiness by 2027; mandatory MFA; encryption; SIEM/centralised logging; annual VAPT.• **Performance** (Sec.No1.5, Table 1.5-A): concurrency targets; P95 response times; availability; RTO/RPO.• **Data**: ANNEX VII-A Table 1 minimum dataset; ANNEX VII-A Table 2 extended fields; ISIC Rev.4 classification; 4-tier data classification (Sec.No1.3.3.4); 7-year audit retention (Sec.No1.1.4).• **Multilingual** (Sec.No3.0.1): English + Urdu; Unicode NFC; Jameel Noori Nastaleeq; Urdu language analyser.• **Multi-jurisdictional** (Sec.No1.1.1.9): equal operational weight to all 6 jurisdictions; configurable without code changes.• **IP & Operational Independence** (Sec.NoG.3; SCC GCC 15.4): GoP ownership; source-code transfer; escrow; cloud-agnostic.The Architecture Compliance Matrix is a mandatory deliverable forming part of the Architecture & Design milestone (M1 at Week 2).
101	**For Module 9 - RIS/AKTU Gating Module (Mandatory Subsystem) & Module 10 — AI Assist Module (Mandatory Subsystem), is it mandatory to give separate pricing for both or we can provide the pricing of it as a whole?**	Both subsystems MUST be priced as SEPARATE mandatory line items. Section VII SIT-1 (p.247) introduction states verbatim: 'Subsystems 8 (RIS/AKTU Gatekeeping) and 9 (AI Assist) MUST be priced as separate mandatory subsystem line items.' (Note: SIT-1 numbers these as Subsystems 8 and 9; the equivalent technical clauses are Sec.No1.2.9 Module 9 RIS/AKTU Gating and Sec.No1.2.10 Module 10 AI Assist.) For the AI Assist Module, Section VII Sec.No1.2.10 (p.174) commercial requirement states: 'This module MUST be priced as a separate subsystem line item in the System Inventory Tables and the Implementation Schedule. The module is mandatory; separate pricing is required for commercial transparency only.' Proposers MUST follow the Price Schedule line-item structure (Section IV Sec.No3.1–Sec.No3.5) and SIT-1; combining mandated separate line items renders the Proposal non-compliant on this point.

102	**In SCC we need to propose separate pricing for Activity 1 & Activity 2 so need to understand that the timeline for Activity 1 is 40 weeks and for the Activity 2 is 60 weeks like the total of both is 100 weeks or for Activity 2 its alone 100 weeks?**	The two Activities run IN PARALLEL within the overall 100-week programme; the schedules are NOT additive (i.e., the total programme is 100 weeks, not 40 + 60 or 40 + 100): • Activity 1 — PRR System Development Contract: 12 milestones M1–M12 spanning Week 2 to Week 40 plus post-go-live stabilisation, per Section IX SCC GCC 12.1 (p.385–387). MVP at Week 10 (M2). Integrated System Acceptance & Operational Go-Live at Week 40 (M11, cumulative 95%). Final Documentation, Handover & Stabilization Completion post-go-live (M12, cumulative 100%). • Activity 2 — PRR RLCO Mapping & Workflow Reform Programme: 10 milestones PM-1 to PM-10, spanning Week 4 (PM-1 TA Inception & Governance Pack) through Week 100 (PM-10 Final RLCO Closure, Reform Pack Handover and Programme Audit), per Section IX SCC GCC 12.1 (p.387–388). Activity 1 software platform development concludes at Week 40; Activity 2 TA workstream continues to Week 100, drawing on the platform delivered under Activity 1 for RLCO mapping, validation, publication and reform pack issuance across the six jurisdictions. Pricing for both Activities MUST be submitted separately and is linked to the respective milestone schedules (Section IV Price Schedules).
103	**For the AMC we need to give pricing for Year 1-3 so do we also need to give budgetary pricing for year 4 & 5?**	AMC pricing for Years 1, 2 and 3 (Y1–Y3) is MANDATORY for each line item in the Recurrent Cost Sub-Table (Section VII SIT-2 rows 2.1–2.5, p.252). The SIT-2 Note states verbatim: 'AMC pricing MUST be quoted separately for Years 1 through 3 (Y1–Y3) as a mandatory line item in the Recurrent Cost Sub-Table. Proposals failing to include a three-year AMC quote are non-responsive.' For Years 4 and 5 (Y4–Y5), the SIT-2 column 'Year 4+ (Yn)' is marked 'Optional (Purchaser's discretion)'. Per Section VII Sec.No5.2.3 (p.238), the Purchaser reserves the right to extend the AMC for up to two (2) additional years at the agreed annual rate. Proposers should therefore quote Y1–Y3 firmly (mandatory) and may, at their option, provide indicative/budgetary pricing for Y4–Y5 to support the Purchaser's discretionary extension decision. Section IX SCC GCC 1.1(e)(xiii), p.384 defines the contractual Post-Warranty Services Period as TWENTY-FOUR (24) MONTHS; the mandatory AMC quote horizon (3 years) is provided as the Recurrent Cost Sub-Table requirement under SIT-2.
104	**For the AMC we need to give pricing for Year 1-3 so do we also need to give budgetary pricing for year 4 & 5?**	AMC pricing for Year 1, Year 2 and Year 3 (Y1–Y3) is MANDATORY for each line item in the Recurrent Cost Sub-Table (Section VII SIT-2 rows 2.1–2.5, p.252). The SIT-2 Note states verbatim: 'AMC pricing MUST be quoted separately for Years 1 through 3 (Y1–Y3) as a mandatory line item in the Recurrent Cost Sub-Table. Proposals failing to include a three-year AMC quote are non-responsive.' For Years 4 and 5 (Y4–Y5), the SIT-2 column 'Year 4+ (Yn)' is marked 'Optional (Purchaser's discretion)'. Per Section VII Sec.No5.2.3 (p.238), the Purchaser reserves the right to extend the AMC for up to two (2) additional years at the agreed annual rate. Proposers should quote Y1–Y3 firmly (mandatory) and may provide indicative/budgetary pricing for Y4–Y5 to support the Purchaser's discretionary extension decision. Y4–Y5 indicative pricing is not a basis for non-responsiveness; only the absence of mandatory Y1–Y3 pricing is.

105	**Infrastructure sizing needs to be provided by the supplier?**	YES — infrastructure sizing MUST be defined, documented and delivered by the Supplier in the Deployment Architecture document under Section VII Sec.No2.6.2 early in the Contract.Per Sec.No3.0.2 (p.222), Sec.No3.1, Sec.No3.2, Sec.No3.3 (p.223 — 'No hardware is procured under this Contract') and Sec.No1.1.1.7 (p.149): procurement and provisioning of the infrastructure (compute including GPU, storage, networking, HSM-based KMS, security) is the Purchaser's responsibility on GoP-provided Tier-3+ infrastructure within Pakistan.The Supplier documents:• Required vCPU/RAM/storage/network/GPU sizing per component and per environment (Dev, Staging/UAT, Production, DR per Sec.No1.3.5.1).• Auto-scaling thresholds and horizontal scaling architecture (Sec.No1.5.3, p.198) — for the public portal and search tier under peak load (≥ 25,000 concurrent public users at consultation surge per Table 1.5-A, p.201).• Network and storage specifications (Sec.No3.0.2).• HSM-based KMS sizing and architecture (Sec.No1.3.4.4).• Annex Tech-I Resource Scaling rubric (Section X, p.439) evaluates vCPU, RAM, Storage, Network (4 scored categories; weighted vCPU 30% / RAM 30% / Storage 20% / Network 20%). GPU sizing is documented and assessed during technical evaluation but is not part of the 4-category Resource Scaling rubric (see S#190/row 193). See also S#208/row 211 (duplicate).
106	**Will the costs of all third-party APIs, gateways, and external integrations be covered separately by the client?**	Third-party API, gateway and external integration arrangements operate under the principle that the Supplier delivers the technical integration and the Purchaser facilitates the commercial/access arrangement, with the cost allocation responsibility of Supplier following the Price Schedule structure: • Government priority integrations (Section VII Sec.No1.3.6.2, p.194) — NADRA, government SSO, gazette/publication systems, government email/SMS gateways, e-Sign service under ETO 2002, BOI/National One Window, provincial e-governance platforms: Supplier is responsible for the technical integration; BOI/AKTU facilitates access and the commercial agreement with the agency/CA. • Where a recurring third-party usage cost is assigned to the Supplier under the RFP (e.g., where the Purchaser determines the Supplier is the contracting party with the third-party provider), it MUST be reflected as a Recurrent Cost line item with explicit assumptions stated, in the Recurrent Cost Sub-Table (Section IV Form 3.5). • Where the cost is borne directly by the Purchaser (e.g., NADRA inter-agency arrangement, CA certificate issuance), the Supplier does not include it. • Proposers MUST state their assumptions clearly in the Technical Proposal and Recurrent Cost Sub-Table. The specific allocation per integration target will be confirmed during Inception (Sec.No1.3.6.3 integration modes apply).
107	**Could you please mention any email address where we can also send our queries**	pms.deep@invest.gov.pk

108	**Please confirm the provisioning of hardware is BOI responsibility or vendor responsibility?**	Provisioning of hardware/infrastructure is the **Purchaser's (BOI/GoP)** responsibility. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) each state verbatim: 'Not Applicable — No hardware is procured under this Contract.' Bidders neither procure nor price hardware. Per Sec.No3.0.2 (p.222), hosting is on GoP-provided infrastructure — Tier-3 or higher, within Pakistan, multi-zone across ≥ 2 independent AZs. Per Sec.No1.1.1.7 (p.149), the solution MUST be cloud-agnostic. Supplier responsibility is limited to: • Documenting required infrastructure sizing, network and storage specifications, and auto-scaling thresholds in the Deployment Architecture document under Sec.No2.6.2. • Delivering containerised software for deployment on the GoP-provided platform. • Cloud-agnostic operation to enable Purchaser flexibility. See also S#80/row 83, S#84/row 87, S#86/row 89, S#107/row 110, S#118/row 121, S#208/row 211, S#210/row 213.
109	**If the provisioning of hardware is vendor responsibility then what is the preferable brand for servers**	Not applicable.
110	**Will the costs of all third-party APIs, gateways, and external integrations be covered separately by the client?**	Third-party API, gateway and external integration arrangements operate under the principle that the Supplier delivers the technical integration and the Purchaser facilitates the commercial/access arrangement, with the cost allocation responsibility of Supplier
111	**RFP mentions integration with provincial Business Facilitation Center Nadra, API protocol and documentation has been finalized or will the selected vendor be responsible for defining these connectivity standards.**	Integration with the provincial Business Facilitation Centres (BFCs) and NADRA is mandatory under Section VII Sec.No1.3.6.2 (p.194): the System MUST integrate with NADRA and with provincial government systems and e-governance platforms where available. An open, read-only API layer for published RLCO data MUST be provided for future integration with additional government portals. Per Section VII Sec.No1.3.6.1 (p.194), all services MUST be exposed through a centralised API Gateway with OpenAPI-compliant documentation, canonical data exchange formats, versioned and backward-compatible APIs, and a dedicated sandbox testing environment for integration partners. Where the counterparty agency (NADRA, BFCs, or another integration target) has not yet finalised or published its API protocols/documentation, the Supplier is responsible for defining and implementing the integration to recognised standards (REST/JSON, OAuth 2.0/OpenID Connect, SAML 2.0 where applicable) consistent with Sec.No1.3.6.3 integration modes (REST APIs; scheduled ETL pipelines; CSV/Excel import staging; webhooks/event triggers). BOI/AKTU facilitates the commercial/access arrangement with the counterparty agency. Final integration design and API specifications are agreed during Inception.

112	**Regarding the Requirement 1.2.5 does the BOI have a preference for open-source BPM engine or a proprietary solution like a custom solution, oracle BPM? As there is some cost involved with Oracle BPM SAP BPM etc.**	There is no mandated BPM/workflow engine. The Supplier MAY propose either an open-source (e.g., Camunda, Flowable, jBPM) or a commercial (e.g., Oracle BPM, IBM Business Automation Workflow) BPM engine, provided it meets the Section VII Sec.No1.2.5 functional requirements and the architectural mandates of Sec.No1.3:• BPMN 2.0 compliance — XML authoring/import/export, model representation, structured workflow data model (Sec.No1.2.5.1, p.163).• No vendor lock-in (Sec.NoG.3.1, Sec.NoG.3.3 — full source code transfer for any PRR-specific custom development built on top).• Operational independence (Sec.NoG.3.8) — GoP MUST be able to engage third parties for maintenance/enhancement, transfer the System to provincial governments, and replicate/scale without Contractor consent.• Cloud-agnostic operation within GoP-provided hosting (Sec.No1.1.1.7; Sec.No3.0.2; Sec.No3.4.1 containerised deployment).• Source-code escrow per Sec.NoG.3.6 if a pre-existing proprietary component is used.For pre-existing proprietary BPM components (e.g., Oracle BPM, SAP BPM): perpetual government-use licence under SCC GCC 15.4 (p.390); explicit declaration in Technical Proposal (Sec.NoG.3.5); sufficient transparency and documentation including build reproducibility; escrow at go-live, major version releases, and annually (Sec.NoG.3.6). No viral/copyleft licences (Sec.NoG.3.4).Any licensing/subscription cost assigned to the Supplier MUST be priced in the appropriate Section IV Form (Supply & Installation for one-time costs; Recurrent Cost Sub-Table for ongoing subscriptions/maintenance). See also S#211/row 214 for licensing models, S#274/row 274 for pre-existing proprietary components.
113	**For the AI module, conflict and duplication features, will BOI provide data for training purpose of AI model or the firm has to prepare it?**	For the AI Module conflict and duplication detection features (Section VII Sec.No1.2.10.6 AI Feature 5, p.177), the Supplier is responsible for preparing, curating and maintaining the training/reference data corpus from the RLCO registry and project data, operating exclusively within government-controlled hosting per Sec.No1.6.9 (p.204). Data access: • BOI/AKTU provides access to the relevant regulatory inventory and historical mapping data per Section VII Sec.No2.5.1 (p.215) — prior mapping outputs, departmental RLCO lists, regulatory scans, legacy database exports — during Inception and through the mapping waves. • The Supplier ingests structured RLCO data via the bulk import facility (Sec.No2.5.2) and uses the resulting curated corpus for training/embedding/indexing the AI features. • AI-extracted outputs are placed in a Human Verification Queue (Sec.No2.5.2) and MUST NOT be promoted to Validated status without human review. Constraints: • External transmission of PRR data for model training, fine-tuning, or evaluation requires explicit prior written Purchaser approval per Sec.No1.6.9 — including for cloud-based embedding/inference APIs (see S#233/row 236). • The Government of Pakistan is the Data Controller; the Supplier acts as Data Processor (Section VII Sec.NoG.4.1, p.285). • Re-use of PRR data by the Supplier for purposes outside the Contract is not permitted (Sec.NoG.3.2, p.284 — data ownership). • All model versions, prompts, training-data manifests, and evaluation logs are GoP IP (Sec.NoG.3.5) and MUST be transferred with documentation.

114	**In RFP it specified it is mentioned that there is tier 3 data center hosting, but the configuration of hardware and costing is not mentioned, do we have to give you the hardware so we include the cost or will you procure by on your own?**	The Supplier prices only the software solution and the documented infrastructure-sizing exercise; the underlying Tier-3 hardware/infrastructure itself is GoP-provided and is NOT procured or priced under this Contract. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) each state verbatim: 'Not Applicable — No hardware is procured under this Contract.' Per Section VII Sec.No3.0.2 (p.222), all active software components and data MUST be hosted on GoP-provided infrastructure meeting Tier-3 or higher standards within Pakistan, multi-zone across at least two independent availability zones. The Supplier's responsibility is: • Document the required infrastructure sizing, network and storage specifications, and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2 — including compute (vCPU/RAM), storage, network, GPU (for AI Module), and HSM-based KMS specifications. • Provide containerised deployment images and deployment scripts (Sec.No3.4.1, p.224). • Deliver and operate the System on the GoP-provided platform. The specific designated hosting environment (data centre or GoP-approved cloud) and the indicative sizing will be confirmed in collaboration with the selected Supplier during Inception. The Supplier MUST also ensure cloud-agnostic operation per Sec.No1.1.1.7 (p.149). See also S#80/row 83, S#84/row 87, S#86/row 89, S#210/row 213 for hosting details, and S#87/row 90, S#89/row 92 for infrastructure provisioning/EoT.
115	**Digital signing of formal records/RLCOs; is there any number of digital records that will be signed off and in what form do you have the data of RLCOs? If we use third party API for digital signature, it will have recurrent cost, will BOI bear the recurring cost or do the firm bear the cost?**	Per Section VII Sec.No1.1.3 (p.151), all formal documents generated by the PRR that constitute official government records — including RLCO closure certificates, AKTU review gate decisions, and Regulatory Impact Statement approval records — MUST be digitally signed using certificates from a PTA-recognised Accredited Certification Authority under the Electronic Transactions Ordinance 2002 (ETO 2002). Per Sec.No1.3.6.2 (p.194), e-Sign service integration under ETO 2002 is a priority government system integration.The Supplier's responsibilities (Sec.No1.1.3): build the application-level digital-signature workflow integrated within the system, ensure signed documents are stored with certificate metadata, document hash and timestamp as part of the immutable audit record, and integrate with the national e-Sign service or accredited Certification Authority.The expected volume and data form of RLCO records to be signed will be confirmed during Inception and through the mapping waves, scoped against the 100 priority economic activities across the six jurisdictions. Where digital-signature certificates/tokens are issued by an accredited CA rather than provisioned by the Supplier, the Supplier integrates with that service. Any recurrent third-party digital-signature API or per-transaction cost that the Purchaser assigns to the Supplier MUST be reflected in the Recurrent Cost Sub-Table (Section IV Form 3.5) with explicit assumptions stated.

116	**There is mention of AI, in API if we use paid API, who will bear the cost of these paid APIs and if Second if you are going through self-hosted AI models then do you have your own GPUs available?**	(a) Paid/external AI APIs: The default expectation per Section VII Sec.No1.2.10.1 (p.175) and Sec.No1.6.9 (p.204) is that the AI Assist Module operates entirely within government-controlled hosting and MUST NOT transmit PRR data to external AI platforms, model APIs or cloud-based AI services unless explicitly approved in writing by the Purchaser. Where such external API use is approved by the Purchaser, the recurrent API cost assigned to the Supplier MUST be reflected in the Recurrent Cost Sub-Table (Section IV Form 3.5, p.117 onwards) with explicit assumptions stated. (b) GPU availability: GPU/compute capacity for self-hosted AI/LLM/NLU workloads forms part of GoP-provided infrastructure (Section VII Sec.No3.0.2, p.222; Sec.No3.1, Sec.No3.2 and Sec.No3.3, p.223 — 'No hardware is procured under this Contract'). The Supplier MUST document the required GPU sizing, architecture and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2 early in the Contract, enabling the Purchaser to provision the required GPU capacity. Indicative GPU specifications will be developed in collaboration with the selected Supplier during Inception.
117	**But are you flexible for payment of APIs in dollars in recurrent cost?**	Currency rules are set by ITP Clause 18 — Currencies of Proposal and Payment (Section I, p.18). Section II PDS ITP 18.1 (p.48) requires the Proposer to quote in Pakistan Rupees (PKR) for the portion of the Proposal price corresponding to expenditure incurred in PKR. Per ITP 18.2, the Proposer may express the Proposal price in any currency, and may quote price in a combination of currencies — but shall use no more than three foreign currencies in addition to PKR. For evaluation, all currencies are converted to a single currency, PKR, using the State Bank of Pakistan selling rate prevailing 18 days prior to the last date of proposal submission (Section II PDS ITP 36.2, p.52). Section IX SCC GCC 12.4 (p.389) applies State Bank of Pakistan exchange rates prevailing on the contract signing date for payment conversion. Accordingly, recurrent third-party API costs (including USD-denominated charges) may be quoted in foreign currency subject to these rules; Proposers MUST clearly state the currency and the assumptions used.
118	**Are there any existing digital systems like any existing portals, any databases that you guys have for the tracking of your regulatory documentation which is basically being replaced by this project. Is there something that you were using in the past?**	No existing system available

119	**So is there a mechanism for any kind of possible disagreements between the stakeholders and the provincial and federal stakeholders on the classification, template standards or any workflow designs? Is there any mechanism that you have decided if there is any disagreement between the provincial stakeholders and the federal stakeholders?**	Disagreements between federal and provincial stakeholders on RLCO classification, template standards, workflow design or other governance issues are resolved through the project governance and AKTU institutional mechanisms established under the Asaan Karobar Act 2025 (Section VII Sec.No1.1.5, p.151) and the PRMI Strategy: • Operational level: Module 9 RIS/AKTU Gating workflow (Section VII Sec.No1.2.9) provides the configured review/return/approve states for RLCO records and reform proposals, with audit trail. • Departmental sign-off SOP: Section VII Sec.No1.2.11.2 (p.178) requires the Supplier to support BOI/AKTU in implementing a formal validation and closure SOP for each participating agency, including resolution of gaps and discrepancies until records are publishable. • Stakeholder engagement: Section VII Sec.No1.2.11.3 (p.178) requires structured validation workshops and targeted resolution sessions with key regulators across all six jurisdictions, with a minimum of one stakeholder session per jurisdiction per mapping wave. • Strategic level: BOI/AKTU as the central coordinating authority under the Asaan Karobar Act 2025 with formal coordination mechanism for harmonisation across federal and provincial governments. • Contract-level disputes (between Supplier and Purchaser): Settlement under Section VIII GCC Clause 43 (p.380) — Adjudicator (SCC GCC 43.1.4: Centre for International Investment and Commercial Arbitration of Pakistan, p.395) and ICC arbitration for non-Pakistan Suppliers (SCC GCC 43.2.3). The Supplier's proposed approach (classifications, templates, workflows) is subject to BOI/AKTU and stakeholder approval through the gating workflow; nothing is deemed accepted without explicit sign-off.
120	**PBP portal will also be integrated into PRR?**	PBP development RFP is yet to be published. PRR will eventually integrate with PBP
121	**And is there any expected number of concurrent users that you have the estimations? And do you have any expected number of the users that will be coming after the deployment?**	Mandatory concurrency targets (Section VII Sec.No1.5.3, p.198 and Table 1.5-A, p.201) — these are contractually binding minima, not estimates:• **2,000 simultaneous authenticated DFP/AKTU sessions** (national mapping campaign scenario).• **≥ 5,000 simultaneous unauthenticated public portal users** (normal operations, auto-scaling baseline).• **≥ 25,000 simultaneous public portal users** (peak consultation surge, auto-scaling activated).Total user population:• DFPs/AKTU/agency staff across federal and provincial departments (estimated population in the low thousands across the 6 jurisdictions).• General public users (citizens, businesses, civil society, journalists, professional services firms) — population not pre-defined; auto-scalable to surge demand.Other performance binding targets (Table 1.5-A):• P95 page-load: public search/browse ≤ 2 s; RLCO detail retrieval ≤ 3 s; workflow state transition ≤ 5 s; record save/create ≤ 3 s; bulk-import validation 1,000 records ≤ 30 s.• Availability ≥ 99.9% monthly (target 99.95%).• RTO ≤ 4 hours; RPO ≤ 1 hour (Sec.No1.3.5.3).Specific user-population estimates per jurisdiction will be refined during Inception based on Agency Registry data (Sec.No1.2.4); platform MUST remain horizontally scalable per Sec.No1.5.3. See also S#29/row 32, S#206/row 209, S#285/row 285.

122	**All 10 modules expected to be fully operational at a single go-live or is there any phase launch acceptable?**	A phased delivery approach is required by the RFP and explicitly recognised in the milestone structure. Per Section VII Sec.No1.3.5.5 (p.193), the Supplier MUST submit a Sprint Plan covering the full project timeline and clearly marking MVP scope, Phase 1 and Phase 2 deliverables. Per Section IX SCC GCC 12.1 — Payment Release Schedule for Activity 1 (p.385–387), the modules are delivered against twelve sequential milestones over Weeks 2–40: • M2 (Week 10): MVP — PRR Registry Core (Subsystem 1) • M3 (Week 16): Subsystem 2 — Workflow Engine & Compliance Controls • M4 (Week 18): Subsystem 3 — MIS Dashboards & Reminders/Escalations • M5 (Week 20): Subsystem 4 — Public Portal & Consultation System • M6 (Week 22): Subsystem 5 — BPMN/BPR Workflow Library + Reform Packs • M7 (Week 24): Subsystem 6 — IT Readiness Assessment • M8 (Week 26): Subsystem 7 — Cost Impact Assessment (SCM/RIA-lite) • M9 (Week 28): Subsystem 8 — RIS/AKTU Gatekeeping • M10 (Week 28): Subsystem 9 — AI Assist modules operational • M11 (Week 40): Subsystem 10 — Integrated System Acceptance & Operational Go-Live • M12 (Post Go-Live): Final Documentation, Handover & Stabilization Completion Integrated Operational Acceptance of the ten mandatory modules occurs at M11 (Week 40), with the Sprint Plan and Agreed Project Plan documenting the detailed sprint sequencing within these gates. PSS compliance is a mandatory pre-condition for issuance of the Operational Acceptance Certificate (Sec.No1.3.4.3, p.191).
123	**Who will conduct the operational acceptance test? Is there any third party? Is that BOI itself?**	Operational Acceptance Testing (OAT) is conducted by the Purchaser (BOI), in coordination with AKTU and the relevant line departments/provincial authorities, with the support of independent third parties where applicable. The OAT framework is set out in Section VII Sec.No4.3 (p.232–233): • OAT-1 — Performance and Concurrency Testing: validates the mandatory targets in Section VII Table 1.5-A (p.201) — 2,000 concurrent DFP/AKTU sessions; ≥ 5,000 concurrent public users normal; ≥ 25,000 peak; P95 page-load targets; availability ≥ 99.9%. • OAT-2 — Security Controls and Access Management: validates RBAC, MFA, encryption, audit logging, PSS compliance. • OAT-3 — Resilience and Disaster Recovery: validates RTO ≤ 4 h, RPO ≤ 1 h (Sec.No1.3.5.3). • OAT-4 — Multi-Jurisdiction Operations: validates jurisdiction-specific configuration and tenancy across the six jurisdictions. • OAT-5 — Training Effectiveness: validates institutional independence per Sec.No2.4.4. • OAT-6 — Operational Readiness: validates documentation, runbooks, hypercare readiness. Third-party components: • Annual third-party VAPT including source-code review (Sec.No1.6.6, p.203) is conducted by an independent third party acceptable to the Purchaser; cost is a mandatory Recurrent Cost line item (SIT-2 row 5.2 / Sec.No5.2.4, p.252) priced by the Proposer for Y1–Y3. • PSS compliance verification is performed through the PSS Compliance Matrix (Sec.No1.3.4.3, p.191) — a mandatory pre-condition for issuance of the Operational Acceptance Certificate.

		Formal Operational Acceptance Certificate issuance follows Section VIII GCC Clause 27 (p.339–340).
124	**What would be the expected duration and process of that acceptance time?**	The deliverable acceptance process and target duration are set in the Agreed Project Plan (Section VII Sec.No2.6.2) and the GCC acceptance provisions:• Process — Section VIII GCC Clauses 25 (Inspections and Tests, p.337), 26 (Installation, Commissioning, p.339), 27 (Operational Acceptance, p.339–340), and the Pre-commissioning Tests per Section VII Sec.No4.2 (p.229–232) and Operational Acceptance Tests per Sec.No4.3 (p.232–233).• Indicative review windows (finalised in the Agreed Project Plan, Sec.No2.6.2): routine deliverables typically within fifteen (15) business days; complex milestone deliverables involving formal testing within a longer window agreed per milestone. Sprint deliverables have a separate review/acceptance cycle per Sec.No1.3.5.5 (p.193).• Change Request Turnaround (Section IX SCC GCC 39.6, p.363–364): Supplier impact assessment within 5 business days; BOI decision within 10 business days; approved CRs into next available sprint.• MVP feedback (GCC 39.7, p.364): Priority 1 within 30 days, Priority 2 within 60 days, at no additional cost provided not new features.• No automatic deemed-acceptance (see S#251/row 251).• Schedule relief for Purchaser-side delay via GCC Clause 40 (p.364).Operational Acceptance Certificate is issued by the Purchaser following successful completion of OAT (Sec.No4.3) and the formal sign-off process under GCC 27 — including PSS compliance (Sec.No1.3.4.3) as a mandatory pre-condition (see S#187/row 190, S#185/row 188, S#132/row 135).
125	**there is a lot of different type of API structure being going on So I just wanted to know that if any case, any API fallback, what is the next level? How are we going to interoperate these things? The API is not going to be negotiated with any node, any endpoints.**	The platform MUST implement a standards-based, API-first integration layer with defined error-handling and fallback strategies. Per Section VII Sec.No1.3.6.1 (p.194), all services MUST be exposed through a centralised API Gateway with OpenAPI-compliant documentation, canonical data exchange formats, versioned and backward-compatible APIs. Per Sec.No1.3.6.3 (p.194), integration modes include: secure REST APIs (real-time synchronous); scheduled ETL pipelines (batch); CSV/Excel import staging (with validation); webhooks/event triggers (asynchronous). Fallback strategies the Supplier MUST design and document (in the Architecture document under Sec.No2.6.2): • **Retry logic**: configurable retry with exponential backoff for transient failures on outbound integrations. • **Circuit breaker pattern**: open-circuit on persistent counterparty failures to protect PRR services; auto-reset on recovery. • **Cached/stale-data fallback**: cached lookup with periodic refresh and fallback to last-known-good values during external-system outages (e.g., for SSO/IdP, NADRA, dropdown lookups). • **Asynchronous queueing**: scheduled retry queue for failed outbound integrations (e.g., gazette publication, e-Sign). • **Alternative-channel fallback**: e.g., where the priority SMS gateway is down, fallback to secondary SMS gateway or email channel. • **Manual fallback workflow**: where automated integration is unavailable, route to manual processing queue with full audit trail. • **Graceful degradation**: partial-functionality mode where non-critical integrations are unavailable; critical workflows pause with operator notification. All fallback events logged in the Immutable Audit Store (Sec.No1.1.4) for traceability. SIEM-based alerts on persistent integration failures (Sec.No1.3.4.6). See also S#108/row 111, S#135/row 138, S#196/row 199, S#242/row 245.

126	**1. Who will bear the cost of WhatsApp API?** **2. Handshake with NADRA is already done, or it will be initiated later? Who will arrange the NADRA API?** **3. Who will bear NADRA API Cost?** **4. Who will bear SMS Gateway Cost?** **5. Do Vendor's team will be travelling across the provinces for meeting with stakeholders during or after implementation?**	For the listed items: 1. WhatsApp Business API cost: WhatsApp is not listed as a mandatory integration in Section VII Sec.No1.3.6.2 (p.194). If the Supplier proposes WhatsApp as a notification channel within its design, the associated cost is the Supplier's, reflected in the Recurrent Cost Sub-Table with assumptions stated. Government email and SMS gateways (Sec.No1.3.6.2) are the mandated notification channels. 2. NADRA handshake / API arrangement: NADRA is a mandated integration target per Sec.No1.3.6.2. The Supplier is responsible for the technical integration; BOI/AKTU facilitates the commercial/access arrangement with NADRA (formal engagement, MoU, API credentials, sandbox). Current handshake status will be confirmed during Inception. 3. NADRA API cost: Any recurrent transaction or licence cost that the Purchaser assigns to the Supplier under the Contract MUST be reflected in the Recurrent Cost Sub-Table with assumptions stated; otherwise the Purchaser arranges the commercial agreement directly. The allocation is confirmed during Inception. 4. SMS gateway cost: SMS gateway is a mandated integration per Sec.No1.3.6.2. Same principle as NADRA — Supplier integrates technically; BOI/AKTU facilitates access; recurrent transaction costs that the Purchaser assigns to the Supplier are quoted in the Recurrent Cost Sub-Table. 5. Cross-province travel: Yes — per Section VII Sec.No2.7.1 (Field Deployment Capacity, p.221) and Sec.No1.2.11.3 (Stakeholder Engagement and Capacity Building, p.178), the Supplier's team is required to travel across the six jurisdictions (Federal, ICT, Punjab, Sindh, Khyber Pakhtunkhwa, Balochistan) for in-person stakeholder engagement sessions, validation workshops, and DFP support during the TA workstream, with a minimum of one stakeholder session per jurisdiction per mapping wave. Travel and accommodation costs are the Supplier's; they MUST be reflected in the priced Proposal.
127	**Our principal companies deeply appreciate the opportunity to participate in multiple business opportunities under the DEEP project. We need firm assurance on transparency, fairness and competitive bidding process. We also need firm assurance that payment processes will be prompt, no undue delay etc.**	Confirmed. This procurement is conducted under the World Bank's Procurement Regulations for IPF Borrowers (referenced in Section II PDS ITP 50.1, p.53) and the Financing Agreement for the Digital Economy Enhancement Project (DEEP), Loan No. 75140-PK and Project ID P174402. All Proposers are treated equally; all clarifications are issued to all Proposers as a single consolidated set through this process. The Standstill Period and Procurement-related Complaint mechanism (Section II PDS ITP 50.1, p.53) protect bidders during award.Payment processes are governed by:• Section IX SCC GCC 12.1 — Payment Release Schedule (p.385–388): Activity 1 milestones M1–M12, Activity 2 milestones PM-1 to PM-10, with each payment triggered by formal Purchaser acceptance of the linked deliverable.• Section VIII GCC 12.3 (p.313–314): interest on payment delay where the Purchaser is delayed beyond the period specified in the SCC.• Section IX SCC GCC 12.4 (p.389): currency rules with State Bank of Pakistan exchange rate at contract signing date for payment conversion.• World Bank prior-review/no-objection regime applies to payments under the Financing Agreement.• Settlement of disputes per Section VIII GCC 43 (p.380) — Adjudicator under SCC 43.1.4 (Centre for International Investment and Commercial Arbitration of Pakistan, p.395), ICC arbitration for non-Pakistan Suppliers.
128	**Are foreign companies allowed to participate in these business activities**	Yes. Foreign firms are eligible to participate, subject to Section V (Eligible Countries) and the eligibility provisions of the ITP, and may participate as a single entity, as a JV member, or as a subcontractor, in accordance with the RFP.

129	**How the payments will be processed, would these be processed under the oversight of World Bank**	Payments will be made by the Purchaser in accordance with the payment schedule in Section IX-SCC and the milestone/acceptance provisions of the Contract. As the Project is financed under the World Bank-funded Digital Economy Enhancement Project (DEEP), the procurement and disbursement are conducted in accordance with the applicable World Bank Procurement Regulations and the Financing Agreement, which the Purchaser is obligated to follow.
130	**In order to assure uninterrupted project activities, we are of the view that mobilisation advance will be paid ? Is it so**	Payment schedule are as per clearly mentioned in Section IX , Special Condition of Contract 12.1 of RFP, where NO advance payment is provided.
131	**What are the mitigation measures to minimise the risk of cost overruns, undue delay in payments as each delay entails extra cost**	The Contract addresses cost-overrun and payment-delay risks through the following mechanisms: • Defined Payment Release Schedule (Section IX SCC GCC 12.1, p.385–388) with milestones, linked deliverables, acceptance weeks and percentages — Activity 1 milestones M1–M12, Activity 2 milestones PM-1 to PM-10. • Acceptance and approval provisions: Section VIII GCC Clauses 25–27 (Inspections and Tests; Installation; Commissioning and Operational Acceptance), with milestone payments triggered by Purchaser acceptance of the linked deliverable. • Interest on payment delay: GCC Clause 12.3 (Section VIII, p.313–314) — if the Purchaser is delayed beyond the period specified in the SCC, interest is payable at the rate and from the period specified in the SCC. • Currency-conversion and invoicing rules: SCC GCC 12.4 (p.389), using State Bank of Pakistan exchange rates at the contract signing date. • Extension of Time for Achieving Operational Acceptance: GCC Clause 40 (Section VIII, p.364) for delays beyond the Supplier's control, with proper notification under GCC 18.2 and GCC 19. • Force Majeure: GCC Clause 38 (Section VIII, p.358) for events outside the parties' reasonable control. • Settlement of Disputes: GCC Clause 43 (Section VIII, p.380) — Adjudicator and arbitration mechanism. The Purchaser endeavours to issue acceptance/approval of complete deliverables within the project governance timelines.
132	**We expect the highest standards of transparency, fairness in the procurement process under the oversight of the world bank. Please confirm**	Confirmed. This procurement is conducted under the World Bank's Procurement Regulations for IPF Borrowers (Fifth Edition, as applicable), referenced in Section II PDS ITP 50.1 (p.53), and the Financing Agreement for the Digital Economy Enhancement Project (DEEP), Loan No. 75140-PK and Project ID P174402. Material safeguards in this RFP include: a single-stage process with separate Technical and Financial Parts (Section I ITP); evaluation per Section III Evaluation and Qualification Criteria; non-discriminatory eligibility under Section V (no countries excluded under ITP 4.8(a) or 4.8(b)); the Bank's standard fraud and corruption requirements (Section VI, p.135–139); the Proposal-Securing Declaration (Section II PDS ITP 20.1, p.48); the Standstill Period and Procurement-related Complaint mechanism (Section II PDS ITP 50.1, p.53); the Beneficial Ownership Disclosure Form (Section X Contract Forms); independent settlement of disputes via Adjudicator and ICC arbitration where the Supplier is from outside Pakistan (Section IX SCC GCC 43.1.4 and 43.2.3, p.395); and Bank prior-review/no-objection over key procurement decisions and payments under the Loan Agreement.

133	**My all questions are related to the governance and stakeholders' management as this is highly critical and always have been sought as one of the major factors contributing to project slippage (delays) from schedule.**	Governance and stakeholder management arrangements are addressed at multiple levels:• Strategic: Asaan Karobar Act 2025 establishes BOI/AKTU as the central coordinating authority (Section VII Sec.No1.1.5, p.151) with statutory mandate for cross-jurisdictional harmonisation.• Operational governance: Agreed Project Plan and governance structure (Section VII Sec.No2.6.2); project oversight committee; Module 9 RIS/AKTU Gating workflow (Sec.No1.2.9).• Stakeholder engagement: BOI/AKTU facilitates formal engagement letters/legal authority to federal and provincial departments (Section VII Sec.No1.2.11.1, p.177–178); structured engagement sessions across all six jurisdictions per Sec.No1.2.11.3.• Schedule risk protection: Extension of Time under Section VIII GCC Clause 40 (p.364) for Purchaser-attributable delays; Liquidated Damages under GCC 28.2 payable only for delay within Supplier control; Force Majeure under GCC 38 (p.358).• Scope baseline & change control: AS-IS/TO-BE sign-off as scope baseline (Sec.No1.2.5.3, Sec.No1.2.11.2); GCC 39 with SCC 39.2.1 Minor/Major classification and 5/10 business-day turnaround under GCC 39.6 (p.363–364); 15% Change Request budget ceiling under GCC 39.5.• Settlement of Disputes: GCC Clause 43 (Section VIII, p.380) — Adjudicator (SCC 43.1.4: Centre for International Investment and Commercial Arbitration of Pakistan, p.395); ICC arbitration for non-Pakistan Suppliers (SCC 43.2.3).The Supplier MUST propose and cost its own engagement and risk-management model as part of the Technical Proposal.
134	**Part 1:** **Will formal sign-off of the AS-IS assessment and TO-BE design documents constituting scope baseline approval for subsequent development and acceptance activities?** **Part 2:** **After TO-BE approval, how will additional functional or regulatory requirements be governed under change-control mechanisms?** **Part 3:** **Who will be the final approving authority for AS-IS and TO-BE deliverables across Federal and Provincial stakeholders?**	Part 1 — Scope baseline: Yes. Formal BOI/AKTU sign-off of the AS-IS assessment and TO-BE design documents for each mapping tranche establishes the approved scope baseline for subsequent development and acceptance activities, in the workflow approval framework of Section VII Sec.No1.2.5.3 (Draft → Under Review → Returned for Revision → Verified/Approved → Archived/Superseded), Section VII Sec.No1.2.11.2 (Validation, Closure and Departmental Sign-Off, p.178), and Section VII Sec.No1.2.11.4 (BPR methodology approval, p.178). Approved versions are locked; edits create new versions with full audit history. Part 2 — Change-control: Additional functional or regulatory requirements arising after TO-BE approval are governed by Section VIII GCC Clause 39 — Changes to the System (p.362) read with Section IX SCC GCC 39.2.1 (p.393): changes are classified as Minor (no cost/schedule impact) or Major (subject to detailed review/approval where applicable); all changes follow a documented change-control procedure with Change Order forms per Section X Contract Forms (p.425–432). Per SCC GCC 39.4 (p.393), Value Engineering Proposals will NOT be considered. Part 3 — Final approving authority: See S#20 / row 22 (BOI/AKTU final approval through project governance with departmental sign-off).
135	**These questions are strategically important because there are several key stakeholders involved from including but not limited to:** **Multiple ministries/departments** **RLCO harmonization** **Regulatory process reengineering** **Cross-provincial coordination** **Evolving integrations** **And without formal TO-BE baseline approval, vendors can later face issues like:** **Unlimited requirement expansion**	Stakeholder coordination, RLCO harmonisation, regulatory reengineering and cross-provincial coordination are managed through the project governance and AKTU institutional mechanisms under the Asaan Karobar Act 2025 (Section VII Sec.No1.1.5, p.151): • BOI/AKTU facilitates engagement with federal and provincial ministries/departments — including formal engagement letters and DFP nomination support (Section VII Sec.No1.2.11.1, p.177–178). • Structured stakeholder engagement sessions across all six jurisdictions — minimum one session per jurisdiction per mapping wave, including validation workshops and targeted resolution sessions (Sec.No1.2.11.3, p.178). • Module 9 RIS/AKTU Gating workflow (Sec.No1.2.9) provides the formal review/return/approve states for RLCO records and reform proposals.

	Rework cycles **Delayed milestone acceptance**	• Scope baseline established by formal sign-off of AS-IS and TO-BE deliverables per Sec.No1.2.5.3 + Sec.No1.2.11.2; post-baseline additions managed under Section VIII GCC Clause 39 — Changes to the System (p.362) and SCC GCC 39.5 (15% change ceiling, p.364) — preventing unlimited requirement expansion. • MVP feedback under GCC 39.7 (p.364) — Priority 1 within 30 days, Priority 2 within 60 days at no cost, provided not new features beyond agreed MVP scope. • Extension of Time under GCC 40 (p.364) for Purchaser-attributable delays — preventing Supplier exposure to LDs for delays outside its control. See also S#21/row 23 and S#143/row 146 for the baseline approval and change-control treatment.
136	**Will BOI facilitate the stakeholder consultation process with regulators? Will they provide letter of engagement to all regulators for assistance in stakeholder engagement?** **ITP 33.8 at least two authorized representatives are required to sign of financial proposal. Can you clarify it?**	Part 1 — Stakeholder consultation facilitation: YES. BOI/AKTU facilitates the stakeholder-consultation process with federal and provincial regulators through formal engagement letters and legal-authority introductions (Section VII Sec.No1.2.11.1, p.177–178). Structured stakeholder engagement sessions are required across all six jurisdictions per Sec.No1.2.11.3 (p.178), with BOI/AKTU support for regulator outreach, focal person nomination facilitation, and tranche sequencing by readiness and priority. Part 2 — ITP 33.8 (authorised representatives at opening of Financial Parts): Per Section I ITP 33.8 and Section II PDS, Proposers may have their authorised representatives attend the opening of the Financial Parts of Proposals. The Proposer's representatives in attendance MUST sign the Record of Opening. Authorisation is evidenced by the Power of Attorney accompanying the Letter of Proposal — Technical Part (Section IV, p.70). Proposers should confirm the precise procedural detail in the SCC and ensure the named authorised representatives carry valid identification and the original Power of Attorney for verification at opening.
137	**Will independent penetration testing be conducted before each phase acceptance? just want to undetstand the testing process**	Security testing/VAPT is conducted as part of the Operational Acceptance regime and on an ongoing annual basis. The testing structure is: • Pre-commissioning Tests (Section VII Sec.No4.2, p.229–232): each subsystem (Subsystems 1–10 per SIT-1) has documented test criteria — including for MVP (Sec.No4.2.1) where database encryption at rest, TLS in transit, and admin MFA must be active. • Operational Acceptance Tests (Sec.No4.3, p.232–233): include OAT-1 (performance and concurrency), OAT-2 (security controls and access management), OAT-3 (resilience and disaster recovery), OAT-4 (multi-jurisdiction operations), OAT-5 (training effectiveness), OAT-6 (operational readiness). • Mandatory PSS Compliance (Sec.No1.3.4.3, p.191): 'PSS compliance MUST be a mandatory pre-condition for the issuance of the Operational Acceptance Certificate.' PSS Compliance Matrix is a mandatory deliverable. • Annual third-party VAPT including source-code review (Sec.No1.6.6, p.203 and Sec.No5.2.4, p.238): a mandatory Recurrent Cost line item (SIT-2 row 5.2, p.252) priced by the Proposer for Y1–Y3. The independent security firm MUST be acceptable to the Purchaser. Remediation: Critical and High severity findings within 30 days; Medium within 90 days. Independent penetration testing is therefore conducted (i) as part of OAT-2 prior to Operational Go-Live (M11 at Week 40) and (ii) annually thereafter under Sec.No1.6.6. The detailed testing process is set in the Agreed Project Plan during Inception.

138	**Will the BOI provide the 'Legal Authority' or a letter of introduction to the various provincial departments to ensure they share their internal RLCO data with our technical team in a timely manner?**	YES. BOI will provide the legal authority/letter of introduction to the relevant federal and provincial departments to facilitate timely sharing of internal RLCO data with the Supplier's TA team. This is a core institutional facilitation provided by BOI/AKTU under the project governance framework. Specifically, per Section VII Sec.No1.2.11.1 (p.177–178), the Supplier is supported through 'regulator outreach support, focal person nomination facilitation, tranche sequencing by readiness and priority.'The legal basis for the engagement is the Asaan Karobar Act 2025 (Section VII Sec.No1.1.5, p.151), which mandates the establishment of the PRR and provides the legal basis for the standardisation of regulatory and registry information at the national level — including by all federal and provincial regulators.Where a department's delay or non-cooperation despite the legal authority/introduction letter impacts the milestone schedule and is beyond the Supplier's control, the Supplier may seek schedule relief under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364) through the project governance and notification process under GCC 18.2 and GCC 19. Escalation paths are agreed in the Agreed Project Plan during Inception.
139	**Project Scope & Objectives**	The Project scope and objectives are set out across Part 2 (Section VII — Purchaser's Requirements) of this RFP: • Scope: Designing, developing and operationalising the Pakistan Regulatory Registry (PRR) and providing Technical Assistance for phase-wise mapping, streamlining and cataloguing of Regulatory Laws, Conditions and Obligations (RLCOs) — RFP No. PK-BOI-542104-GO-RFP. • Two parallel Activities (Section IV Price Schedules; Section IX SCC GCC 12.1, p.385–388): – Activity 1 — PRR System Development (Weeks 2–40+): the ten (10) mandatory modules — Registry Core; Workflow Engine; MIS Dashboards; Mapping Enablement; BPR (Module 5); IT Readiness (Module 6); Cost Impact SCM/RIA-lite (Module 7); Public Portal & CMS (Module 8); RIS/AKTU Gating (Module 9); AI Assist (Module 10). – Activity 2 — PRR RLCO Mapping & Workflow Reform Programme (Weeks 4–100): TA workstream covering RLCO mapping, AS-IS workflow documentation, TO-BE reengineering, IT readiness assessment and cost-impact analysis across 100 priority economic activities × 5 ISIC Rev.4 sectors × 6 jurisdictions (Federal, ICT, Punjab, Sindh, Khyber Pakhtunkhwa, Balochistan). • Legal basis: Asaan Karobar Act 2025 (Section VII Sec.No1.1.5, p.151) and the PRMI Strategy. • Financing: World Bank Loan No. 75140-PK; Digital Economy Enhancement Project (DEEP-BOI), Project ID P174402. • Total programme duration: 100 weeks; MVP within 10 weeks; Operational Go-Live at Week 40 (Activity 1); TA workstream completion at Week 100 (Activity 2).
140	**Is the Minimum Viable Product (MVP) expected to cover all modules or only the core registry module initially?**	The Minimum Viable Product (MVP) is defined in Section VII Sec.No1.3.5.5 (p.193) verbatim as 'the minimum system capability required to enable early RLCO data entry by DFPs and early review by BOI/AKTU', and MUST be delivered within ten (10) weeks of the Contract Effective Date. The detailed MVP scope is reflected in SIT-1 Subsystem 1 — 'PRR MVP Core for Early Data Entry' (p.247), which includes: PRR Registry Core Application (Table 1 baseline template engine, versioning, legal linkage and attachments); Agency Registry + User Provisioning (DFP accounts, RBAC, MFA for privileged roles); MVP RLCO submission loop (Draft/Submit/Return/Resubmit/Validate/Publish); Bulk Import to Staging

		+ Validation Error Reports; Search and Index baseline; and Deployment Package for MVP across DEV, UAT and PROD. The remaining mandatory modules (Subsystems 2–10) are delivered against the SCC Activity 1 payment milestones M2–M11, with Subsystem 10 (Integrated System Acceptance & Operational Go-Live) at Week 40 — see Section IX SCC Payment Release Schedule (p.386–387). The Supplier proposes the detailed sprint/phase plan as part of its Technical Proposal (Sec.No1.3.5.5).
141	**Is there a target number of regulatory authorities and RLCO records expected for Phase 2?**	Phase 2 scope (additional regulatory authorities and RLCO records beyond the initial 100 priority economic activities) is NOT pre-specified in the RFP. The engagement is scoped around the binding 100 priority activities × 5 ISIC Rev.4 sectors × 6 jurisdictions per Section VII Sec.No1.2.11.4 (p.178). Subsequent expansion is governed by: • Platform scalability: per Sec.No1.1.5 (p.151), 'The Information System MUST be capable of accommodating jurisdiction-specific provisions arising from equivalent provincial enactments and subordinate legislation **without architectural modification**.' The platform MUST remain horizontally scalable per Sec.No1.5.3 (p.198) for growth in records and concurrent users (≥ 25,000 peak public users at consultation surge). • Change Control mechanism: Where BOI/AKTU determines that additional activities/agencies should be brought into scope during contract execution, this is managed through Section VIII GCC Clause 39 (p.362) read with Section IX SCC GCC 39.2.1 (p.393) — Minor / Major classification — with 15% Change Request budget ceiling under SCC GCC 39.5 (p.364). Indicative volumes will be confirmed via the 'ISIC Rev.4 Activity Selection Note' (Table 1.2.11-A row TA-D6 / SIT-1 row TA-02) during the early TA phase and through the wave-based mapping per Section IX SCC Activity 2 Payment Release Schedule (PM-1 to PM-10, p.387–388). See also S#5/row 7 (100 activities), S#44/row 47 (Total RLCO count), S#179/row 182 (Min agencies), S#261/row 264.

142	**What level of process reengineering or regulatory reform consulting is expected from the vendor?**	The TA workstream (Activity 2) requires substantive regulatory process reengineering and reform consulting across the six jurisdictions. Specifically:• AS-IS workflow documentation (Section VII Sec.No1.2.11.4, p.178; Sec.No1.2.5.1, p.163): documented at minimum for the 100 priority economic activities × 5 sectors, capturing process steps, actors and lanes, decision points, required documents, fees and time bands, service channels, and inter-agency handoffs.• TO-BE redesign (Sec.No1.2.5.4, p.163): redesigned workflows with bottleneck tagging (redundant approvals, duplicate documents, physical visits, manual verification, queue delays), structured redesign rationale, digitisation interventions and dependencies on legal changes or IT integrations.• Cost Impact Assessment (Module 7, Sec.No1.2.7, p.166–168): Standard Cost Model (SCM) and RIA-lite quantification of AS-IS vs TO-BE administrative and compliance cost — process steps, time bands, fee components, documents, channel mode, agency contact frequency, rework rates.• IT Readiness Assessment (Module 6, Sec.No1.2.6, p.165): Quick Win / Medium Complexity / Complex classification with sub-scores for data, channel, integration, and authentication/payments readiness; top blockers report; integration dependency matrix.• Sector Reform Packages (Sec.No1.2.5.5, p.163): minimum five sectors consolidated as complete reform packs (mapped RLCOs + approved workflows + bottleneck analysis + IT readiness + cost impact + linked legal change items + first-cut draft amendment text where applicable).• TA workstream stakeholder engagement and reform facilitation (Sec.No2.4.8, p.215): structured seminars and capacity building with regulators, provincial governments, chambers of commerce.The Supplier provides the analytical content, methodology and consulting capability through Key Experts (KE-01 to KE-05 per Table 2.7-B) and supporting non-key staff. BOI/AKTU validates and approves through the project governance and Module 9 RIS/AKTU Gating workflow.

143	**Are there preferred technology stacks or architecture standards mandated by the government?**	There is no single mandated technology stack — Proposers may propose their stack within the binding architectural constraints in Section VII Sec.No1.3 (p.187–195): Mandatory architectural standards: • Microservices architecture with minimum required service decomposition per Table 1.3.1-A (p.187): Identity & Access Service; Registry Core Service; Workflow Engine Service; Mapping Enablement Service; BPR Service; IT Readiness Service; Cost Impact Service; Public Portal Service; RIS/AKTU Service; AI Assist Service; Search Service; Notification Service; Audit Service; Reporting Service; Integration Service; API Gateway Service. • Containerised deployment using Kubernetes or equivalent (Sec.No3.4.1, p.224). • OpenAPI-compliant API specifications for all services (Sec.No1.3.6.1, p.194). • Cloud-agnostic operation with no dependency on a vendor-operated cloud not approved by the GoP (Sec.No1.1.1.7, p.149). • PostgreSQL-class relational database for transactional/registry data (referenced in Table 1.3.2-A); search tier (e.g., Elasticsearch/OpenSearch/Solr); vector database for AI Feature 5 (Sec.No1.2.10.6); object storage for documents. • Workflow engine BPMN 2.0-compliant (Sec.No1.2.5.1; Sec.No3.4.8). • Low-Code/No-Code (LCNC) platform component per Sec.No3.4.9. • Form builder per Sec.No3.4.10. • Identity provider supporting SAML 2.0 / OpenID Connect / OAuth 2.0 for SSO with mandatory MFA (Sec.No1.6.2; Sec.No1.3.6.2). • HSM-based KMS within Pakistan (Sec.No1.3.4.4). • Post-Quantum Cryptography readiness with upgrade capability by 2027 or earlier (Sec.No1.3.4.5). Other constraints: no vendor lock-in (Sec.NoG.3); full source-code transfer for custom components (Sec.NoG.3.3); open-source disclosure with no viral/copyleft (Sec.NoG.3.4); operational independence (Sec.NoG.3.8). Proposers propose specific technologies within these constraints and justify in the Architecture document under Sec.No2.6.2.
144	**Besides integration frameworks with PBP, how many other integrations will there be with other government portals in this project?**	Beyond the Pakistan Business Portal (PBP) — which is supported via an open, read-only API layer for published RLCO data per Section VII Sec.No1.3.6.2 (p.194) — the mandatory priority government integrations are six (6) categories: 1. NADRA and government SSO platforms (identity verification / authentication) 2. Government email and SMS gateways (notification delivery) 3. Pakistan Gazette and official publication systems 4. e-Sign service for digital signatures under ETO 2002 5. BOI / National One Window (regulatory business facilitation) 6. Provincial government systems and e-governance platforms where available (i.e., separate counterparts in Punjab, Sindh, Khyber Pakhtunkhwa, Balochistan, ICT) Additional integration targets that may arise from specific RLCO workflows identified during mapping (e.g., agency-specific licensing systems) are approached through the BOI/AKTU governance and the Change Control process under GCC 39 if outside baseline scope. The per-system readiness, sandbox availability and credentials will be confirmed during Inception (Sec.No1.3.6.3 integration modes apply throughout).

145	**Is the purchaser expecting a microservices architecture or a monolithic system?**	A microservices architecture is REQUIRED. Section VII Sec.No1.3.1 (p.187) — Software Architecture — and Table 1.3.1-A (Minimum Required Microservice Decomposition, p.187) mandate a microservices architecture with the following minimum decomposition:• Identity & Access Service • Registry Core Service • Workflow Engine Service • Mapping Enablement Service • BPR Service • IT Readiness Service • Cost Impact Service • Public Portal Service • RIS/AKTU Service • AI Assist Service • Search Service • Notification Service • Audit Service • Reporting Service • Integration Service • API Gateway Service.Other architectural mandates of Section VII Sec.No1.3:• Containerised deployment using Kubernetes or equivalent (Sec.No3.4.1, p.223).• OpenAPI-compliant APIs for all services (Sec.No1.3.6.1, p.194).• Centralised API Gateway with versioned, backward-compatible APIs and sandbox environment.• Cloud-agnostic operation (Sec.No1.1.1.7, p.149).• Stateless services with horizontal auto-scaling for the public portal and search tier (Sec.No1.5.3, p.198).• Infrastructure-as-Code (Sec.No1.3.2.6, p.190).• No vendor lock-in (Sec.NoG.3); full source-code transfer for custom components (Sec.NoG.3.3); operational independence (Sec.NoG.3.8).A monolithic architecture would NOT satisfy these mandates. The Supplier proposes the specific decomposition, inter-service communication patterns (synchronous REST/event-driven), and supporting infrastructure in the Architecture document under Sec.No2.6.2.
146	**Will historical regulatory data be provided in structured formats for migration?**	Historical regulatory data will be provided in the form available, which is expected to be mixed (structured digital, semi-structured, paper) — per Section VII Sec.No2.5.1 (p.215): 'Volume, type, structure, and format of existing data available will be confirmed during the Inception phase.' Data is NOT guaranteed to be in structured digital format ready for direct migration. The Supplier is responsible for the format adaptation, mapping, cleansing, structuring and migration into the PRR per Sec.No2.5.1–Sec.No2.5.3: • Bulk import facility — Excel/CSV upload with column mapping to ANNEX VII-A Table 1 fields, validation rules, error reports, staging area review (Sec.No2.5.2). • AI-assisted extraction with mandatory Human Verification Queue (Sec.No2.5.2) for semi-structured sources. • Manual capture via Module 4 Mapping Enablement for paper records (see S#46/row 49). • Migration runbooks with rollback procedures (Sec.No2.5.3). BOI/AKTU provides available source data and facilitates access through formal engagement letters (Sec.No1.2.11.1, p.177–178). Proposers should plan for mixed-format reality and size their TA effort accordingly. See also S#56/row 59, S#62/row 65.
147	**Are there data standards or taxonomies already defined for RLCO classification?**	Not defined The data standards and taxonomies for RLCO classification are to be proposed by Supplier as defined in the RFP itself: • ANNEX VII-A — RLCO Data Structure Reference (Section VII BIM-3, p.323 onwards) — comprises Table 1 (Base Template: Minimum Dataset for RLCO Data Collection) and Table 2 (Extended Fields covering AS-IS governance, statutory forms, lifecycle gaps). Table 1 is the mandatory minimum dataset that all federal and provincial RLCO records MUST conform to. • ISIC Rev.4 sector classification — applies to economic activity classification (Section VII Sec.No1.2.11.4). • Configurability — BOI/AKTU administrators MUST be able to configure additional vocabulary lists and classification schemes (Section VII

		Sec.No1.2.1, Sec.No1.2.6.2 readiness data model) without code changes. Beyond ANNEX VII-A and ISIC Rev.4, the Purchaser does not specify a pre-existing departmental classification taxonomy in the RFP.
148	**Could you clarify the number of RLCO workflows currently existing in regulatory platforms? How many platforms will require data ingestion and possible re-engineering?**	Cannot be ascertained without the development of PRR as Activity 1 and undertaking Mapping i.e. Activity 2
149	**Are there requirements for open data portals or external developer APIs?**	YES. Open data and external developer-facing APIs are mandatory requirements: • **Public Portal — Module 8** (Sec.No1.2.8, p.171–173): full public access to published RLCO records — search, browse, view, download — across all six jurisdictions, in English and Urdu (Sec.No3.0.1, p.222). • **Open read-only API layer** (Sec.No1.3.6.2, p.194): 'An open, read-only API layer for published RLCO data MUST be provided for future integration with additional government portals including the Pakistan Business Portal (PBP).' • **OpenAPI-compliant documentation** (Sec.No1.3.6.1, p.194): published API specifications enabling third-party developer integration. • **Dedicated sandbox testing environment** for integration partners (Sec.No1.3.6.1). • **API Gateway** (Sec.No1.3.6.1): centralised access with rate limiting, authentication, and audit logging; versioned and backward-compatible APIs. • **Public consultation feedback** (Sec.No1.2.8): public users can submit comments during consultation windows (minimum 30 days per Sec.No4.2.2); subject to moderation and PII redaction (Sec.No1.6.10). • **Bulk data export**: published RLCO data exportable in machine-readable formats. Data classification (Sec.No1.3.3.4): only tier-1 'Public' classification data is exposed via the open APIs and public portal; tiers 2–4 (Government Restricted, Internal, Confidential) are NOT accessible through these channels. See also S#129/row 132 (PBP), S#129–S#130 (concurrent users).
150	**Who will be responsible for data cleansing and validation during migration?**	Data cleansing and validation during migration are the SUPPLIER's responsibility under the TA workstream, supported by BOI/AKTU facilitation and departmental validation of substantive content. Per Section VII Sec.No2.5.1 (p.215):• 'The Supplier MUST provide services and tools to incorporate all existing regulatory inventory datasets provided by the Purchaser ... into the PRR.'• 'The Supplier MUST conduct a data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, and records requiring manual validation.'Per Sec.No2.5.2 (p.215):• Bulk import facility with validation rules at import; detailed import error report; staging area review before records are confirmed.• AI-assisted extraction MAY accelerate structuring, BUT all AI-extracted outputs MUST be placed in a Human Verification Queue and MUST NOT be promoted to Validated status without human review.Per Sec.No2.5.3 (p.215):• Migration runbooks with rollback procedures; cutover plans with point-in-time recovery.BOI/AKTU and DFPs (Sec.No1.3.3.6) validate substantive RLCO content (legal correctness, completeness, currency); formal departmental sign-off per Sec.No1.2.11.2 (p.178) closes each agency's inventory. The Supplier provides the platform,

		tooling, methodology, and field staffing across the six jurisdictions (Sec.No2.7.1, p.221). See also S#29/row 32, S#56/row 59.
151	**Are suppliers required to hold ISO 27001 certification, or is alignment/compliance sufficient?**	Per Section VII Sec.No1.6.8 (p.203), the System and the Supplier's delivery organisation MUST implement ISO/IEC 27001-aligned information security management controls — including documented Information Security Management System (ISMS) covering risk assessment, controls implementation, monitoring and continuous improvement. ISO/IEC 27001 alignment/compliance is MANDATORY. ISO/IEC 27001 CERTIFICATION of the Supplier's delivery organisation or of the System is PREFERRED but not separately mandated as a qualification criterion (Sec.No1.6.8). Proposers holding such certification are encouraged to demonstrate it; non-certification does not by itself render a Proposal non-responsive provided demonstrable alignment with ISO/IEC 27001 controls is shown. Mandatory pre-condition for Operational Acceptance (Sec.No1.3.4.3, p.191): PSS compliance — the PSS Compliance Matrix is a mandatory deliverable submitted by the Supplier, with PSS issued and periodically updated by the Ministry of IT and Telecom, the National Telecommunication Corporation (NTC), and IGNITE. PSS compliance is therefore the binding gating standard at OAT; ISO/IEC 27001-aligned controls provide the broader management-system framework. See also S#75/row 78 (PSS at OAT), S#165/row 168 (security frameworks summary).
152	**Will the government provide PKI infrastructure for digital signatures, or must the supplier integrate with existing accredited certification authorities?**	The Supplier integrates with the existing national PKI / PTA-recognised Accredited Certification Authority operating under the Electronic Transactions Ordinance 2002 (ETO 2002). The Supplier is NOT required to establish a new PKI/CA. Per Section VII Sec.No1.1.3 (p.151), all formal documents generated by the PRR that constitute official government records — including RLCO closure certificates, AKTU review gate decisions, and Regulatory Impact Statement approval records — MUST be digitally signed using certificates from a PTA-recognised Accredited Certification Authority operating under ETO 2002. Per Sec.No1.3.6.2 (p.194), e-Sign service integration under ETO 2002 is a priority government system integration. The Supplier's responsibilities: • Build the application-level digital signature workflow integrated within the system (Sec.No1.1.3). • Integrate with the national e-Sign service / accredited Certification Authority via secure REST APIs per Sec.No1.3.6.3 (p.194). • Ensure signed documents are stored with certificate metadata, document hash and timestamp as part of the immutable audit record (Sec.No1.1.3; Sec.No1.1.4, p.151). • HSM-based Key Management System (KMS) hosted within Pakistan for any internal cryptographic keys (Sec.No1.3.4.4, p.191). The Supplier integrates with the existing PKI; any recurrent third-party CA / e-Sign per-transaction cost assigned to the Supplier must be reflected in the Recurrent Cost Sub-Table with explicit assumptions stated. See also S#64/row 67, S#124/row 127.

153	**What specific security frameworks or national standards must be followed?**	The mandated security frameworks and standards are set out in Section VII Sec.No1.6 — Cyber Security Requirements (p.202–205) and Sec.No1.3.4 — Security Architecture (p.190–192). The following are contractually binding:• Pakistan Security Standards (PSS) compliance — issued and periodically updated by the Ministry of IT and Telecom, the National Telecommunication Corporation (NTC), and IGNITE (Sec.No1.3.4.3). PSS compliance is a mandatory pre-condition for OAT.• OWASP Top 10 compliance across all portals and APIs (Sec.No1.6.1).• ISO/IEC 27001-aligned information security management controls (Sec.No1.6.8). ISO 27001 certification of the Supplier's delivery organisation or the System is preferred (Proposers encouraged to demonstrate).• HSM-based KMS hosted within Pakistan (Sec.No1.3.4.4).• TLS 1.2 or higher in transit; encryption at rest for all stores (Sec.No1.6.3).• Mandatory MFA for all publishers, reviewers, administrators and AI reviewers; SSO integration with government identity providers (Sec.No1.6.2).• Mandatory annual third-party VAPT including source code review, with Critical/High findings remediated ≤30 days, Medium ≤90 days (Sec.No1.6.6).• Post-Quantum Cryptography readiness with upgrade capability by 2027 or earlier (Sec.No1.3.4.5).• Compliance with applicable national laws: Electronic Transactions Ordinance 2002 (ETO 2002), Prevention of Electronic Crimes Act 2016 (PECA 2016) and amendments, Pakistan data protection legislation, PTA regulations, Asaan Karobar Act 2025, Digital Nation Pakistan Act (Sec.No1.1.1.1–Sec.No1.1.1.12).
154	**Will security testing (VAPT) be conducted by the vendor, a government-appointed third party, or a third-party provider recommended by the vendor?**	The annual third-party VAPT including source-code review is conducted by an INDEPENDENT third-party security firm — NOT the Supplier itself. Per Section VII Sec.No1.6.6 (p.203), the independent security firm MUST be acceptable to the Purchaser; final selection rests with the Purchaser.
155	**Can the purchaser clarify the priority modules for Phase 1 implementation?**	The phased delivery is set out in the Section IX SCC Activity 1 Payment Release Schedule (SCC GCC 12.1, p.385–387). 'Phase 1' priority modules in the binding milestone sequence are: • M2 Week 10 — Subsystem 1 PRR MVP Core (Registry Core, Standardisation and Early Data Entry per Sec.No4.2.1, p.229). • M3 Week 16 — Subsystem 2 Workflow Engine & Compliance Controls. • M4 Week 18 — Subsystem 3 MIS Dashboards & Reminders/Escalations. • M5 Week 20 — Subsystem 4 Public Portal & Consultation System. All ten (10) mandatory modules are delivered against M2–M11 over Weeks 10–40, with **Integrated System Acceptance & Operational Go-Live at M11 Week 40** (cumulative 95%); Final Documentation, Handover & Stabilization at M12 (post Go-Live, cumulative 100%). The detailed sprint sequencing within each milestone gate is set out in the Supplier's Sprint Plan (Section VII Sec.No1.3.5.5, p.193) and Agreed Project Plan (Sec.No2.6.2). The MVP scope (Sec.No1.3.5.5) is binding as the Week-10 minimum; subsequent modules are sequenced against the milestone gates. PSS compliance is a mandatory pre-condition for Operational Acceptance at M11 (Sec.No1.3.4.3, p.191). See also S#131/row 134, S#149/row 152 for module sequencing.

156	**What level of customization should administrators be able to perform without vendor support?**	BOI/AKTU administrators MUST be able to perform substantial configuration without vendor support, in line with the Low-Code/No-Code (LCNC) capability requirement (Sec.No3.4.9, p.224) and the configurability mandate across modules. Specifically, administrators MUST be able to configure (without code changes / vendor support): • **Templates and data model**: RLCO record templates with field-level metadata, validation rules, vocabularies — including Draft → Pilot → Approved version transitions and historical version retention (Sec.No1.2.1.2). • **Dynamic forms**: form builder with conditional logic and multi-language labels per Sec.No3.4.10 (p.224). • **Workflow configuration**: BPMN authoring and editing per Sec.No1.2.5.2 (p.163); workflow types (RLCO, end-to-end business journey, internal review), approval routes. • **SLA timers and escalations**: time limits per agency and per workflow state with multi-channel notifications and 3-level escalation per Sec.No1.2.3.3 (p.156–157). • **Dashboards, reports and exports** per Sec.No1.2.3 / Sec.No1.2.6.4. • **Bottleneck categories** (Sec.No1.2.5.4): bottleneck tagging vocabulary. • **IT Readiness scoring** (Sec.No1.2.6.2, Sec.No1.2.6.3): readiness data model, controlled vocabularies, scoring thresholds. • **Cost Impact formulas and parameters** (Sec.No1.2.7): SCM/RIA-lite parameter library and formula composition (see S#204/row 207). • **CMS content** (Sec.No1.2.8): public portal content, FAQs, announcements, multi-language content. • **RBAC** (Sec.No1.6.2): role definitions, jurisdiction-scoped permissions. • **Notification templates** (multi-channel: email, SMS, in-app). • **AI prompt templates and rule thresholds** (Sec.No1.2.10), subject to AI governance review. Source-level code modification is NOT expected of administrators; that is performed under the Supplier's AMC or via the Change Control mechanism.
157	**Who will act as the central governing authority for the system?**	The Board of Investment (BOI), Government of Pakistan — Prime Minister's Office, Islamabad — is the Purchaser and the central governing authority for the PRR programme. Per Section VII Sec.No1.1.5 (p.151), the Asaan Karobar Act 2025 establishes BOI/AKTU as the central coordinating authority and 'designates [the PRR] as the authoritative platform through which regulatory information is standardised, published, and made accessible to businesses and the public across all jurisdictions.'Governance structure:• BOI — Purchaser, programme owner, contractual counterpart to the Supplier.• AKTU (Asaan Karobar Tagheeri Unit) — regulatory reform unit under BOI exercising the RIS/AKTU gating function (Module 9, Sec.No1.2.9) and reform facilitation across jurisdictions.• Federal and Provincial line departments — sectoral owners of RLCO content with Departmental Focal Persons (DFPs) per Sec.No1.3.3.6 (p.193).• Project governance per Section VII Sec.No1.4 and Sec.No2.6.2 Agreed Project Plan — project oversight committee with BOI/AKTU and relevant stakeholders.• World Bank — Financing institution under DEEP Loan 75140-PK / Project ID P174402, exercising prior-review and no-objection over key procurement decisions per the Financing Agreement.Within the PRR platform, the Module 9 RIS/AKTU Gating workflow operationalises the central gating function across all six jurisdictions while preserving

		departmental ownership of substantive RLCO content (see S#48/row 51, S#175/row 178).
158	**How will federal and provincial jurisdictions coordinate governance and approvals?**	Under constitution of Islamic Republic of Pakistan
159	**Will there be a formal onboarding process for each regulatory authority?**	YES. A formal onboarding process for each regulatory authority/agency is supported through the platform's agency-provisioning functionality and the configured governance workflow. Per Section VII Sec.No1.2.4 — Module 4 Mapping Enablement (p.160): • **Agency Registry**: master data for each agency including jurisdiction, sector, contact information, designated focal persons, status, on-boarding/closure dates. • **Agency provisioning workflow**: account creation, RBAC role assignments, jurisdiction-scoped permissions per Sec.No1.6.2 (p.203). • **DFP nomination and registration** (Sec.No1.3.3.6, p.193): Departmental Focal Person assignment as data steward responsible for accuracy, timeliness, verification of supporting legal documents. • **MFA and SSO onboarding** (Sec.No1.6.2): mandatory MFA for all publishers, reviewers, administrators. • **Initial RLCO inventory upload** via bulk import (Sec.No2.5.2, p.215): Excel/CSV upload with validation rules and staging area review. • **Validation and closure SOP** (Sec.No1.2.11.2, p.178): data quality checks, gap resolution, formal departmental sign-off (see S#73/row 76 for sign-off evidence). • **Training**: jurisdiction-wise DFP onboarding sessions per the Training Plan (Sec.No2.4.1, p.212) aligned to mapping tranches, plus recurring refresher clinics (Sec.No2.4.3, p.213). The institutional onboarding is facilitated by BOI/AKTU through formal engagement letters (see S#147/row 150) and aligns with the wave-based jurisdiction onboarding plan (Sec.No1.2.11.1).
160	**Who will be responsible for ongoing policy updates and legal instrument management?**	Ongoing policy updates and legal-instrument management are the responsibility of BOI/AKTU and the relevant federal/provincial line departments (the substantive regulatory owners). The PRR platform supports this through: • **Version Control and Time-Aware Design** (Sec.No1.3.3.5, p.192): effective date tracking; historical snapshot retrieval; future-dated regulatory changes; automatic deactivation upon expiry. Regulatory time-state machine-readable and queryable via API; comparison between current, historical, and future versions of any RLCO. • **Workflow approval states** (Sec.No1.2.5.3, p.163): Draft → Under Review → Returned for Revision → Verified/Approved → Archived/Superseded. • **Legal Amendment Traceability and Sector Packages** (Sec.No1.2.5.5, p.163): linkage from RLCO records to linked legal change items and first-cut draft amendment text; sector reform packages. • **DFP role** (Sec.No1.3.3.6, p.193): each participating institution has a Departmental Focal Person responsible for accuracy, timeliness, verification of supporting legal documents. • **Annual review obligation** (Sec.No1.3.3.6): each participating authority MUST review and certify the accuracy of its regulatory records at least annually or upon any regulatory amendment. • **Module 9 RIS/AKTU Gating workflow** (Sec.No1.2.9): formal review/return/approve states for RLCO amendments and new RIS

		submissions. • **Immutable audit** (Sec.No1.1.4, p.151): 7-year minimum retention. During the Warranty Period (2 years) and AMC (Y1–Y3 mandatory, Y4–Y5 optional), the Supplier maintains the platform supporting BOI/AKTU's ongoing policy update operations under the SLA regime of Table 5.1-A (p.237). See also S#49/row 52, S#229/row 232.
161	**How will conflicts between federal and provincial regulatory frameworks be handled?**	Under constitution of Islamic Republic of Pakistan
162	**Will the vendor need to provide regulatory mapping support for all jurisdictions?**	YES — regulatory mapping support is required across all SIX jurisdictions: Federal, Islamabad Capital Territory (ICT), Punjab, Sindh, Khyber Pakhtunkhwa, and Balochistan. Per Section VII Sec.No1.2.11.1 (p.177–178), the Supplier MUST support BOI/AKTU to implement a jurisdiction-wise onboarding plan covering all six jurisdictions, including regulator outreach support, focal person nomination facilitation, tranche sequencing by readiness and priority, and structured RLCO data capture using PRR workflows.Per Section VII Sec.No1.2.11.4 (p.178), AS-IS workflow documentation MUST be produced for a minimum of one hundred (100) priority economic activities across five ISIC Rev.4 sectors, covering the relevant RLCOs across the six jurisdictions.Per Section VII Sec.No1.1.1.9 (p.149), the Information System MUST 'support and give equal operational weight to the regulatory frameworks of all jurisdictions it serves.'The mapping is delivered in waves per Section IX SCC Activity 2 Payment Release Schedule (PM-4 Federal+ICT at Week 40; PM-5 first provincial wave; PM-6 second provincial wave). Resource sharing across jurisdictions is permitted where mapping waves are staged (see S#14/row 16). Travel and field staffing across all six jurisdictions are the Supplier's responsibility (Sec.No2.7.1, p.221; Sec.No1.2.11.3, p.178).
163	**Will there be local consultants and Project Managers embedded within regulatory agencies?**	• Per Section VII Sec.No1.2.11.1 (p.177–178), the Supplier 'MUST deploy dedicated TA resources to provide practical mapping assistance to DFPs through a combination of remote support and in-person visits' — implying field deployment across the six jurisdictions. • Per Sec.No2.7.1 — Field Deployment Capacity (p.221): the Supplier MUST demonstrate adequate field staffing to execute activities in parallel across all six jurisdictions and meet the milestone schedule. • Per Sec.No1.2.11.3 (p.178): structured stakeholder engagement sessions across all jurisdictions, with a minimum of one stakeholder session per jurisdiction per mapping wave. • KE-04 Jurisdiction Deployment & Mapping Lead (Table 2.7-B, p.219–220) is a Key Expert role with engagement weeks set per the Supplier's proposed methodology. • KE-01 Project Director / Engagement Lead is Full-Time per Table 2.7-B. The specific embedding model — whether named consultants are physically located within agency offices, whether they rotate across jurisdictions, or whether a hybrid in-person + virtual approach is used — is proposed by the Supplier in the Technical Proposal consistent with Sec.No2.7.1 and Sec.No1.2.11.3 and confirmed in the Agreed Project Plan. AKTU institutional embedding (e.g., placement of TA resources within AKTU offices) is part of the TA capacity-building programme (Sec.No2.4.5–Sec.No2.4.8). The Supplier prices the embedded-team approach including travel, accommodation and logistics across the six jurisdictions in the priced Proposal.

164	**Is there a minimum number of agencies to be onboarded during the contract period?**	The RFP does not specify a fixed minimum number of agencies for onboarding. The scope is bounded by: • 100 priority economic activities × 5 ISIC Rev.4 sectors (Section VII Sec.No1.2.11.4, p.178). The number of regulatory agencies in scope is the set of federal, ICT, and provincial agencies with jurisdiction over the 100 priority activities. • 6 jurisdictions (Federal, ICT, Punjab, Sindh, Khyber Pakhtunkhwa, Balochistan) per Sec.No1.1.1.9 (p.149) and Sec.No1.2.11.1 (p.177). • Wave structure per Section IX SCC Activity 2 Payment Release Schedule (p.387–388): PM-4 Wave 1 Federal + ICT; PM-5 Wave 2 first provincial wave; PM-6 Wave 3 second provincial wave; PM-7 to PM-10 rolling AS-IS workflow and TO-BE design completion through Week 100. The specific list of agencies onboarded in each wave will be defined through the 'ISIC Rev.4 Activity Selection Note' (Table 1.2.11-A row TA-D6 / SIT-1 row TA-02, p.179–180, p.247) during the early TA phase and the agency registry maintained in Module 4 Mapping Enablement (Sec.No1.2.4, p.160). Departmental sign-off SOPs apply per Sec.No1.2.11.2 (p.178). The platform MUST remain scalable for additional agencies and RLCOs without architectural modification (Sec.No1.1.5).
165	**Are there minimum experience requirements for consortium partners?**	Please refer to section III ,1.4.2 Eligibility. Each (Joint Venture) partner must individually meet certain minimum experience requirements, while other requirements apply to the combination of all partners.
166	**Will local partner participation be mandatory?**	The Proposer MUST be able to mobilise and sustain delivery locally across the six jurisdictions throughout the Contract Period. Per Section VII Sec.No2.7.1 (p.221) — Field Deployment Capacity — the Supplier MUST demonstrate adequate field staffing to execute activities in parallel across all six jurisdictions and meet the milestone schedule. For international Suppliers specifically, Section VII Sec.No2.4.3 (p.213) mandates: 'For international Suppliers, a train-the-trainer approach with local technical partnerships MUST be included, and a capacity retention strategy MUST be explained.' This is a delivery methodology requirement, not an eligibility/qualification requirement — international Proposers MUST include the train-the-trainer cascade and may partner locally for technical capability building, but a formal Pakistan-registered local partner is not separately required by ITP 4 or Section III. Joint Venture/Consortium with a Pakistan-registered partner is permitted (see S#82/row 85; S#181/row 184) — max 3 members per ITP 4.1 — but is optional. Subcontracting is permitted (see S#83/row 86; S#101/row 104) — also optional.
167	**Are there minimum key personnel roles?**	Mandatory Key Expert positions are specified in Section VII Tables 2.7-A and 2.7-B with minimum qualifications, experience and engagement requirements.

168	**How will technical assistance services be evaluated compared to software delivery?**	Both Activity 1 (PRR System Development) and Activity 2 (PRR RLCO Mapping & Workflow Reform Programme) are evaluated together under the technical evaluation framework of Section III — Evaluation and Qualification Criteria, with separate costing in Section IV Price Schedules:• Technical Evaluation (Annex Tech-I, Section X, p.434 onwards): the scoring matrix covers BOTH workstreams in an integrated assessment, including Registry Architecture (15%), Low Code (10%), Resource Scaling (10%), Methodology & Approach (covering both PRR delivery and TA delivery), Key Expert Templates (for both software-side roles KE-06 through KE-12 and TA-side roles KE-01 through KE-05). The total technical scoring is per the Annex Tech-I rubric.• Financial Evaluation per Section I ITP Clause 36 (Evaluation of Financial Part): the total Contract Price is compared, with Activity 1 and Activity 2 prices submitted separately in Section IV Form 3.2 Supply & Installation Cost Summary and Form 3.3 Recurrent Cost Summary, plus the linked sub-tables.• Combined evaluation per ITP 39 — Combined Evaluation, Most Advantageous Proposal: technical and financial scores are combined per the weighting set in Section II PDS.Both Activities are subject to the same mandatory minimum technical threshold; failure to meet the minimum on either workstream renders the Proposal non-responsive.
169	**30. What are the key milestones and acceptance criteria for each phase?**	Detail already available in RFP Milestones and acceptance criteria are set in Section IX SCC GCC 12.1 — Payment Release Schedule (p.385–388) read with Section VIII GCC Clauses 25–27 (Inspections and Tests; Installation, Commissioning; Operational Acceptance, p.337–340) and Section VII Sec.No4.2 (Pre-commissioning Tests, p.229–232) and Sec.No4.3 (Operational Acceptance Tests, p.232–233). Activity 1 milestones (PRR System Development, Weeks 2–40+): • M1 Week 2 (10%) — Project Inception (Project Plan, Architecture, Standards Finalization) • M2 Week 10 (15%) — Subsystem 1 PRR MVP Core operational • M3 Week 16 (10%) — Subsystem 2 Workflow Engine & Compliance Controls • M4 Week 18 (5%) — Subsystem 3 MIS Dashboards + Reminders/Escalations • M5 Week 20 (10%) — Subsystem 4 Public Portal & Consultation System • M6 Week 22 (5%) — Subsystem 5 BPMN/BPR Workflow Library + Reform Packs • M7 Week 24 (10%) — Subsystem 6 IT Readiness Assessment • M8 Week 26 (10%) — Subsystem 7 Cost Impact Assessment (SCM/RIA-lite) • M9 Week 28 (5%) — Subsystem 8 RIS/AKTU Gatekeeping • M10 Week 28 (5%) — Subsystem 9 AI Assist operational • M11 Week 40 (10%) — Subsystem 10 Integrated System Acceptance & Operational Go-Live • M12 Post Go-Live (5%) — Final Documentation, Handover & Stabilization Completion Activity 2 — 10 milestones PM-1 to PM-10 (Weeks 4–100). Acceptance criteria per milestone are defined by the corresponding Pre-commissioning Test (Sec.No4.2.1 through Sec.No4.2.11) and OAT-1 to OAT-6 (Sec.No4.3). PSS compliance is a mandatory pre-condition for OAT (Sec.No1.3.4.3). Formal written sign-off is required for each milestone (no automatic deemed-acceptance — see S#251/row 251).

170	**31. Will acceptance be based on functional testing, user acceptance testing (UAT), or operational rollout?**	Detail already available in RFP Acceptance under this Contract combines all three layers, applied per milestone: • Functional testing — by the Supplier, against the Architecture & Design Pack and Requirements Traceability Matrix; outputs feed into the Pre-commissioning Test Report. • Pre-commissioning Tests (Section VII Sec.No4.2, p.229–232) — per subsystem, per milestone (Subsystem 1 PRR MVP Core through Subsystem 10 Integrated System Acceptance; plus TA workstream tests under Sec.No4.2.11): validates the technical implementation against the corresponding requirements. • User Acceptance Testing — by BOI/AKTU/DFP users, per sprint (Sec.No1.3.5.5) and per milestone, with structured feedback that the Supplier incorporates per GCC 39.7 (MVP feedback: Priority 1 within 30 days, Priority 2 within 60 days, at no cost provided not new features). • Operational Acceptance Tests (Sec.No4.3, p.232–233) — OAT-1 through OAT-6 (see S#132/row 135): performance, security, resilience/DR, multi-jurisdiction, training effectiveness, operational readiness. Conducted by/under the Purchaser with independent third parties for VAPT. • PSS Compliance Matrix — mandatory pre-condition for issuance of the Operational Acceptance Certificate (Sec.No1.3.4.3, p.191). • Operational rollout (deployment to live environment) confirmed at Milestone M11 (Week 40) — 'Integrated System Acceptance & Operational Go-Live.' Formal written sign-off is required at each milestone per Section VIII GCC Clauses 25–27 (p.337–340). There is no automatic deemed-acceptance (see S#251/row 251).
171	**32. What are the penalties for delays or non-performance?**	Detail already available in RFPPenalties for delay and non-performance are governed by the following provisions:• Liquidated Damages (LDs) for delay in achieving Operational Acceptance — GCC Clause 28.2 (Section VIII, p.342) read with the SCC entry at Section IX GCC 28.2 (p.393). LDs are payable per week (or part thereof) of delay beyond the scheduled Operational Acceptance date.• Aggregate LD cap — Section IX SCC GCC 28.3 (p.394): maximum 10% of the Contract Price excluding Recurrent Costs, applied SEPARATELY per Activity (Activity 1 max 10% of Activity 1 price; Activity 2 max 10% of Activity 2 price). Once the LD maximum is reached, the Purchaser may consider termination pursuant to GCC Clause 41.2.2.• Cyber security obligation failures — GCC Clause 12.6 (Section VIII, p.314): the Project Manager may withhold an assessed amount until the obligation has been performed.• Warranty / SLA defect-repair regime — Section VII Table 5.1-A (p.237): Critical 2 h response / 24 h resolution; High 4 h / 72 h; Medium 1 business day / 10 business days; Low 2 business days / 30 business days.• Termination for Default or Convenience — GCC Clause 41 (Section VIII), with payment and step-in consequences.• Performance Security — Section IX SCC GCC 13.3.1 (p.389): 5% of the Contract Price excluding Recurrent Costs, by unconditional/irrevocable bank guarantee from any scheduled bank in Pakistan, valid for two (2) years; reduced to 2.5% during the Warranty Period (SCC GCC 13.3.4, p.390).

172	**33. What level of post-implementation support or maintenance is required?**	Detail already available in RFP Post-implementation support comprises three layers: • Warranty / Defect Liability Period — TWO (2) YEARS from issuance of the Final Acceptance Certificate (Section IX SCC GCC 29.1, p.394). Defect repair, security patches, AI module recalibration, software/licence renewals are included in the Supply and Installation Price (Section VII SIT-2 rows 1.1–1.4, p.252). • Hypercare Support (Section VII Sec.No5.1.4, p.236): mandatory minimum 3–6 months immediately following go-live, with on-call technical assistance under the Warranty SLAs; extended transition support of 6–12 months strongly recommended. • Post-Warranty Annual Maintenance Contract (AMC): Years 1–3 (Y1–Y3) MANDATORY line items (Section VII SIT-2 Notes, p.251–252); Y4–Y5 optional at Purchaser's discretion (Sec.No5.2.3, p.238). Post-Warranty Services Period defined as TWENTY-FOUR (24) MONTHS per SCC GCC 1.1(e)(xiii), p.384. Service Level Agreements (Section VII Table 5.1-A, p.237): • Critical: response 2 hours / resolution 24 hours • High: response 4 hours / resolution 72 hours • Medium: response 1 business day / resolution 10 business days • Low: response 2 business days / resolution 30 business days Helpdesk hours, on-call coverage, escalation matrix, transition-out plan and AMC scope details are set in the Agreed Project Plan and Recurrent Cost Sub-Table assumptions.
173	**In the RFP the evaluation is based on vCPU, RAM, Storage, Network resources, however the solution may require GPUs for the AI module. How will BOI evaluate and compare the GPU resources quoted by bidders .**	The Annex Tech-I Resource Scaling rubric (Section X, p.439) currently evaluates four resource categories — vCPU, RAM, Storage and Network — using the formula: Score = 100 × (Lowest Declared Value Among All Bidders) / (Bidder's Declared Value), weighted vCPU 30% / RAM 30% / Storage 20% / Network 20%. The rubric does not explicitly include GPU as a fifth scored category. Bidders proposing AI module components requiring GPU MUST declare the required GPU sizing/architecture in the Deployment Architecture document (Section VII Sec.No2.6.2 / Sec.No3.0.2). The adequacy of declared GPU resources will be assessed during technical evaluation in the context of the AI Module requirements (Sec.No1.2.10) and the mandate for localised AI processing (Sec.No1.2.10.1, Sec.No1.6.9). Because no hardware is procured under this Contract (Sec.No3.1, Sec.No3.2, Sec.No3.3), the GPU infrastructure forms part of GoP-provided infrastructure; the declared GPU sizing informs Purchaser provisioning.
174	**If the bidder proposes a commercial grade (OEM backed) solution without source code handover, will that lead to disqualification?**	YES

175	**Can the bidder propose a different expected delivery milestones and total required delivery time for the software part OR compliance to the delivery timelines in the tender is mandatory**	The delivery timelines and mandatory milestones in this RFP are binding minima. Specifically: • MVP at Week 10 — Section VII Sec.No1.3.5.5 (p.193): 'A Minimum Viable Product (MVP) … MUST be delivered within ten (10) weeks of Contract Effective Date.' • Activity 1 Final Acceptance at Week 40 (Milestone M11 — Integrated System Acceptance & Operational Go-Live, Section IX SCC GCC 12.1, p.386). • Activity 2 (TA Workstream) completion at Week 100 (Milestone PM-10 — Final RLCO Closure, Reform Pack Handover and Programme Audit, Section IX SCC GCC 12.1, p.388). • Total programme duration: 100 weeks. Within these binding timelines, the Supplier proposes the detailed Sprint Plan and Agreed Project Plan (Section VII Sec.No1.3.5.5 and Sec.No2.6.2) and may propose an accelerated delivery sequence for individual subsystem milestones (M2–M10), provided the binding gates — MVP at Week 10 and Operational Go-Live at Week 40 — are met. Acceleration proposals that compress between-milestone activities are at the Supplier's risk and require Purchaser acceptance through the project governance. Proposals quoting a later Final Acceptance date than Week 40 (Activity 1) or Week 100 (programme) would not be compliant with the mandatory Implementation Schedule.
176	**The scale, structure, and format of the existing historical data mentioned in the bidding document will only be confirmed during the project initiation phase. Can the buyer provide an estimated reference value (such as approximate number of records, attachment storage scale GB/TB) to enable the bidding party to accurately evaluate the data cleaning workload and provide a reasonable quotation?**	Indicative reference values for the scale, structure and format of existing historical data are NOT specified in the RFP cannot be ascertained at this stage. The engagement is scoped around:• 100 priority economic activities × 5 ISIC Rev.4 sectors × 6 jurisdictions (Sec.No1.2.11.4, p.178).• AS-IS workflow documentation for all 100 activities, capturing process steps, actors, decision points, required documents, fees and time bands, service channels, and inter-agency handoffs (Sec.No1.2.11.4).• Linked RLCO data structured to ANNEX VII-A Table 1 (mandatory minimum dataset, Section VII BIM-3, p.323) and Table 2 (extended fields).

177	**Does the provided government infrastructure include GPU computing power that supports the operation of large models? If not, is it allowed to call secure commercial grade cloud AI (such as Chat GPT OpenAI) through APIs to meet the intelligence requirements of module 10?**	GPU compute capacity for self-hosted AI workloads (LLM inference, NLU classification, semantic embeddings, similarity/conflict detection) forms part of GoP-provided infrastructure under Section VII Sec.No3.0.2 (p.222) and Sec.No3.1–Sec.No3.3 (p.223 — 'Not Applicable — No hardware is procured under this Contract'). The Supplier documents the required GPU sizing, architecture and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2 early in the Contract, enabling the Purchaser to plan and provision the required GPU capacity. Use of secure commercial-grade cloud AI services (e.g., OpenAI, Azure OpenAI, Google Vertex AI, AWS Bedrock) is permitted ONLY with the Purchaser's prior written approval, per Section VII Sec.No1.2.10.1 (p.175) and Sec.No1.6.9 (p.204) — 'AI Assist Module MUST operate exclusively within government-controlled hosting and MUST NOT transmit PRR data to external AI platforms, model APIs, or cloud-based AI services unless explicitly approved in writing by the Purchaser.' The prohibition extends to cloud-based embedding APIs (see S#233/row 236). Where external API use is approved by the Purchaser for a specific function, supporting documented data-protection safeguards are required (data minimisation, retention controls, no model-training-on-PRR-data clauses, contractual protections). Any approved recurrent third-party API cost assigned to the Supplier MUST be reflected in the Recurrent Cost Sub-Table with explicit assumptions. The default expectation is self-hosted AI within GoP-provided infrastructure using open-source or licensed embedding/inference models, with GPU sizing documented in the Deployment Architecture (Sec.No2.6.2). See also S#16/row 18, S#71/row 74, S#125/row 128, S#190/row 193, S#233/row 236.
178	**There are many demonstration contents in this chapter. Is it necessary to demonstrate them during the acceptance stage or during the bidding stage**	Demonstration / Proof of Concept content is addressed in two distinct contexts: • **Proposal evaluation (technical evaluation per Annex Tech-I, Section X, p.434+)**: Proposers describe their proposed approach, methodologies, sample outputs, prior project demonstrations, and supporting evidence in the Technical Proposal. The Purchaser may require oral presentations / clarification per ITP Clause 35 (if specified in the PDS). At this stage, deliverable demonstration is descriptive/evidential, not live functional demonstration. • **Functional acceptance during execution**: functional demonstrations and validations occur progressively: – **Sprint reviews** — UAT of each sprint deliverable per Sec.No1.3.5.5 (p.193), with structured feedback that the Supplier MUST incorporate. – **MVP Pre-Commissioning Test** (Sec.No4.2.1, p.229–230) at Milestone M2 Week 10. – **Subsystem Pre-Commissioning Tests** (Sec.No4.2.2 through Sec.No4.2.11) per milestone. – **Operational Acceptance Tests** (Sec.No4.3, p.232–233) — OAT-1 to OAT-6 at Milestone M11 Week 40. – **MVP feedback** under GCC 39.7 (p.364) — Priority 1 within 30 days, Priority 2 within 60 days, at no cost provided not new features. – **Operational Acceptance Certificate** issuance under Section VIII GCC Clause 27 (p.339–340) following successful OAT and PSS Compliance (mandatory pre-condition per Sec.No1.3.4.3). Demonstration content described in the Technical Proposal is validated against the actual delivered system through these acceptance gates.

179	**Regarding the technological boundaries of digital signatures: Does the software only need to interface with Pakistan's existing national level PKI services through APIs? Can you provide corresponding interface specifications?**	Confirmed. The System interfaces with Pakistan's existing national PKI/e-Sign services through APIs — there is no requirement to establish a new PKI/CA. Per Section VII Sec.No1.1.3 (p.151) and Sec.No1.3.6.2 (p.194): • Formal documents constituting official government records MUST be digitally signed using certificates from a PTA-recognised Accredited Certification Authority operating under ETO 2002. • e-Sign service integration under ETO 2002 is a priority integration target. • The System MUST maintain an immutable record of every signed document — signing certificate, timestamp, document hash — as part of the immutable audit record (Sec.No1.1.3; Sec.No1.1.4, p.151 — 7-year retention). Interface specifications: • The Supplier integrates via the centralised API Gateway with OpenAPI-compliant documentation per Sec.No1.3.6.1 (p.194). • Integration modes per Sec.No1.3.6.3 (p.194): secure REST APIs for real-time synchronous signature operations; supporting webhooks for asynchronous notifications. • Cryptographic key management within the PRR uses an HSM-based KMS hosted in Pakistan (Sec.No1.3.4.4, p.191).
180	**Regarding the data acquisition method: Do the dropdown menus or field contents of dynamic forms need to support "dynamic calling of external government agency APIs" or only perform static maintenance within the system?**	Both static and dynamic data acquisition methods are supported. Per Section VII Sec.No1.2.1 (Registry Core), the System MUST provide a configurable template manager for RLCO records, in which Table 1 fields (ANNEX VII-A) are the mandatory minimum dataset. Per Sec.No1.3.6.1 (p.194), all services MUST be exposed through a centralised API Gateway with OpenAPI documentation.Dynamic form behaviour:• Static configuration: BOI/AKTU administrators configure dropdown vocabularies, lookup lists, classification schemes (e.g., jurisdictions, agencies, ISIC sectors, legal instrument types) without code changes, per Sec.No1.2.1.x.• Dynamic external population: for fields requiring real-time lookup from authoritative external sources (e.g., live entity verification against NADRA, real-time exchange-rate lookup against State Bank of Pakistan for fee calculations, business entity verification against SECP), the System MUST support dynamic population via the priority integration APIs of Sec.No1.3.6.2 (p.194) and integration modes of Sec.No1.3.6.3 (p.194) — secure REST APIs for real-time synchronous queries.• Hybrid: cached lookup with periodic refresh and fallback to static last-known-good values during external-system outages.The specific fields requiring live external API calls are determined per service during Architecture & Design and confirmed in the Agreed Project Plan (Sec.No2.6.2). The template/dynamic-form manager MUST be configurable by administrators without code changes.
181	**Can you provide a list of items and their attributes, such as item name, item code, department to which the item belongs, and PRMI policy**	Cannot be ascertained without establishment of PRR and Mapping activities while the taxonomy and classification is to be proposed by Supplier. PRMI Strategy document is available at www.business.gov.pk
182	**Can you provide the original text of the Pakistan Regulatory Modernization Initiative (PRMI) policy and the indicator points of the existing evaluation model**	PRMI Strategy document is available at www.business.gov.pk

183	**Regarding SLA timer logic: Is the automatic upgrade time limit calculation based on simple natural days, or does it require the system to build and maintain a set of "dynamic statutory holiday/working day calendars for Pakistan's national and provincial governments" to accurately exclude rest days?**	Per Section VII Sec.No1.2.3.3 (p.156–157), the System MUST support 'configurable time limits per agency and per workflow state, enforced through automated multi-channel notifications via email, SMS, and in-app alerts. A configurable reminder schedule MUST be implemented (e.g., fifteen, seven, and three days before deadline, on the deadline, and at defined intervals thereafter). The escalation ladder MUST comprise at minimum: Level 1 (DFP), Level 2 (Agency Head/Authorized Signatory), and Level 3 (BOI/AKTU oversight). Escalations MUST trigger automatically on overdue thresholds and MUST continue until compliance is recorded or AKTU documents a formal exception. All notification events MUST be logged and exportable.' The clause requires configurability per agency and per workflow state, which is consistent with — and intended to support — a configurable working-day / statutory-holiday-aware calendar covering Pakistan's national and provincial public holidays, weekend conventions per jurisdiction (where these differ), and agency-specific working calendars. Simple natural-day counting alone would not meet the configurability requirement. The Supplier MUST therefore propose, build and maintain a dynamic statutory holiday/working-day calendar dataset for the federal and provincial governments — supporting per-jurisdiction overrides and BOI/AKTU runtime configuration without code changes — as part of the Module 3 MIS / SLA timer implementation. The final calendar design is documented in the Agreed Project Plan and Module 3 specification deliverables during Inception.
184	**What does Sector Package mean here**	Sector Package' is defined by Section VII Sec.No1.2.5.5 (p.163) — Legal Amendment Traceability and Sector Packages. It is a grouped, consolidated artefact for an economic sector — one of the five ISIC Rev.4 sectors covered by the 100 priority economic activities of Sec.No1.2.11.4 — containing for that sector: • The mapped RLCO set (all RLCOs linked to the priority activities in that sector across the relevant agencies and jurisdictions). • Approved AS-IS workflows (BPMN 2.0 with structured workflow data model and PDF rendering, per Sec.No1.2.5.1). • Approved TO-BE workflows with structured redesign rationale and bottleneck analysis (Sec.No1.2.5.4). • Linked IT Readiness Assessment data (Quick Win / Medium / Complex classification, blockers and dependency matrix, per Module 6 Sec.No1.2.6). • Linked Cost Impact (SCM/RIA-lite) data — AS-IS vs TO-BE administrative and compliance cost comparison (Module 7 Sec.No1.2.7). • Linked legal change items — first-cut draft amendment text artifacts traceable to the relevant legal instrument clauses (Sec.No1.2.5.5). Per Sec.No1.2.5.5, sector packages are 'exportable as a complete reform pack' (referenced in Figure 6: Workflow Artifact Linkage — PRR Record → BPMN → Reform Pack). The minimum coverage is FIVE sectors selected in consultation with BOI (the five ISIC Rev.4 sectors of the engagement); the System could be configured to support additional sector packages in future. Sector Packages are a primary TA delivery artefact and a structured PRR record at the same time.

185	**Regarding the quantitative evaluation engine: is it allowed to solidify the "weight allocation matrix" for calculating evaluation indicators in the underlying code, or is it necessary to provide a visual "rule configuration backend" for business personnel to adjust indicators and score weights at any time?**	The quantitative evaluation / readiness-scoring engine MUST provide a CONFIGURABLE rule/weight-allocation capability — NOT a hard-coded/fixed weight allocation. Per Section VII Sec.No1.2.6 — Module 6 IT Readiness Assessment (p.165):• Sec.No1.2.6.2 Readiness Data Model: structured readiness schema with controlled vocabularies and **configurable scoring**.• Sec.No1.2.6.3 Readiness Scoring and Prioritisation: 'BOI/AKTU administrators MUST be able to configure vocabulary lists and scoring thresholds without code changes.' The System MUST compute an overall readiness rating (Quick Win / Medium / Complex) with optional sub-scores for channel/data/integration/payments-authentication readiness.Similarly for Module 7 Cost Impact Assessment (Sec.No1.2.7, p.166–168): configurable formulas, parameter libraries, and multi-currency support (see S#204/row 207).And for Annex Tech-I Resource Scaling (Section X, p.439): vCPU 30% / RAM 30% / Storage 20% / Network 20% — these are the proposal evaluation weights set by the Purchaser and are fixed for proposal scoring purposes.The platform configurability requirement means:• Weight values per criterion / sub-criterion are configurable by BOI/AKTU administrators.• Scoring thresholds (Quick Win / Medium / Complex band thresholds) are configurable.• Versioning of scoring schemes — historical scoring schemes retained with effective dates.• Audit trail of configuration changes (Sec.No1.1.4, p.151).Solidifying a fixed weight allocation matrix that cannot be reconfigured by BOI/AKTU administrators would NOT meet Sec.No1.2.6.3 and Sec.No1.2.7 mandates. See also S#216/row 219, S#169/row 172.
186	**Regarding the cost calculation formula: Does the SCM engine require a "custom formula editing ability" similar to Excel (allowing users to customize variable concatenation such as Cost=A * (B+C)), or only provide preset fixed logic calculations?** **Regarding data sources: Where did the data on administrative and compliance costs come from before and after the reform?**	Cost calculation formula: Per Section VII Sec.No1.2.7 (p.166–168) — Module 7 Cost Impact Assessment Module — the SCM/RIA-lite engine MUST support 'configurable formulas, parameter libraries, and multi-currency support', enabling BOI/AKTU to define and adjust calculation logic without code changes. This is a parameter-driven, configurable formula engine — NOT a fixed preset-only calculator. Expected capability: • Reusable cost parameters with parameter library management (e.g., hourly wage rates, document/form costs, transport costs by region) configurable by administrators. • Formula composition for cost expressions (e.g., Cost = unit_cost × frequency × population × adjustment_factor), with support for arithmetic, logical conditions, lookups, and aggregations. • Multi-currency support with currency-conversion handling. • Versioned formulas with audit trail (Sec.No1.2.5.3 workflow approval pattern applies). • Validation/sandbox testing of new formulas before publication. Data sources for AS-IS and TO-BE administrative and compliance costs: • AS-IS: captured during the TA workstream — process step time bands, fee components, document and form requirements, channel mode, agency contact frequency, rework rates (Sec.No1.2.7, Sec.No1.2.5.1) — derived from stakeholder workshops, agency data, and validation per Sec.No1.2.11. • TO-BE: derived from the redesign rationale and digitisation interventions (Sec.No1.2.5.4), with assumptions agreed with BOI/AKTU. The standard methodology pack and parameter library (TA Capacity Building Toolkit per Table 1.2.11-A, p.179–180) is developed in consultation with BOI/AKTU during Inception. See also S#216/row 219.

187	**Regarding offline data conflict strategy: When network synchronization is restored, what conflict resolution strategy should the system adopt (such as overwriting, retaining multiple versions, or manual arbitration) if it detects that the same record has been modified by multiple parties or people simultaneously during the offline period?**	For offline resilience and queueing per Section VII Sec.No1.3.2.5 (p.190), draft RLCO entries, saved checklists, and consultation drafts MUST be locally cached and queued for secure submission upon reconnection. Minimum offline draft retention MUST be configurable by BOI/AKTU, with a default of up to thirty (30) days for government users and public consultation drafts. On reconnection, where the System detects that the same record has been modified by multiple parties or sessions during the offline period, the Supplier MUST implement a defined conflict-resolution strategy that preserves auditability. Acceptable approaches include: • Optimistic concurrency control with version timestamping — server-side rejection of a stale-version write attempt with structured error feedback to the offline user. • Version retention with controlled three-way merge for non-conflicting field changes and a manual arbitration queue for conflicting changes. • Last-writer-wins is NOT acceptable for authoritative records. Blind overwrite without conflict detection is NOT acceptable. • All conflict-resolution events MUST be logged in the Immutable Audit Store (Sec.No1.1.4) — capturing the offline session ID, conflicting versions, resolution decision, and the user/role who made the resolution. • Re-submission MUST go through the same validation rules as online submission (mandatory-field validation, legal basis reference validation, classification tagging per Sec.No1.3.3.4). The detailed conflict-resolution policy is documented in the Architecture document under Sec.No2.6.2 and configured per workflow type. For approved/locked records (per Sec.No1.2.5.3), offline edits are not permitted; only Draft and Returned-for-Revision states support offline editing.
188	**Regarding the level of multi tenant data isolation: In the operation mode of the federal and provincial platforms, must the business dictionaries (such as industry classifications) of each province achieve "Tenncy Isolation" at the provincial level?**	Multi-jurisdictional operation requires logical tenant-level isolation between federal and provincial jurisdictions for jurisdiction-specific data, while supporting shared national reference data where appropriate. Per Section VII Sec.No1.1.1.9 (p.149), the Information System MUST 'support and give equal operational weight to the regulatory frameworks of all jurisdictions it serves — Federal, ICT, Punjab, Sindh, Khyber Pakhtunkhwa, and Balochistan. The system architecture MUST accommodate jurisdiction-specific configuration, content, templates, workflows, dashboards, escalation rules, and user role assignments without code modification.'For business dictionaries / classifications:• National-level taxonomies (ISIC Rev.4 sector codes, ANNEX VII-A Table 1 minimum dataset structure, classification vocabularies issued by BOI/AKTU centrally) are SHARED across jurisdictions to preserve consistency.• Jurisdiction-specific extensions to vocabularies, jurisdiction-specific fees and time bands, jurisdiction-specific approval workflows and reviewer roles are ISOLATED at the jurisdiction level — accessible only to the respective jurisdiction's authorised roles, configurable independently, audited separately.• Cross-jurisdiction read-only viewing is supported for AKTU oversight and federal coordination, governed by RBAC (Sec.No1.6.2).The detailed isolation model — including database multi-tenancy approach (separate schemas, row-level security, separate databases), tenancy boundary for files/objects, cross-jurisdiction analytics aggregation — is finalised in the design phase and documented in the Architecture document under Sec.No2.6.2.

189	**As one of the committee members about the To-Be processes. Could you please elaborate does the consultants have to digitize the To be Processess along with the As-Is.**	YES. Both AS-IS and TO-BE workflows MUST be digitised — i.e., modelled in BPMN 2.0 and configured/captured in the PRR platform — as part of the reengineering scope. Per Section VII Sec.No1.2.5.2 (p.163) — Workflow Types and Creation: 'The System MUST support As-Is workflows representing the current administrative process, To-Be workflows representing the redesigned process, and end-to-end business journey workflows spanning multiple RLCOs and agencies.' Both AS-IS and TO-BE artifacts are stored in three synchronised representations: BPMN 2.0 XML (authoritative machine-readable); structured workflow data model (for analytics and rule-based checks); human-readable PDF rendering (Sec.No1.2.5.1, p.163). Per Sec.No1.2.5.4 (p.163), TO-BE workflows MUST capture structured redesign rationale including change summary, expected impact categories, digitisation interventions proposed, and dependencies on legal changes, IT integrations, or policy decisions. Approval (Sec.No1.2.5.3): all workflow artifacts pass through Draft → Under Review → Returned for Revision → Verified/Approved → Archived/Superseded. Volume: per Sec.No1.2.11.4, AS-IS workflows MUST be documented for a minimum of 100 priority economic activities × 5 ISIC sectors. TO-BE workflows are produced for the same set as part of the reengineering deliverables. The Module 5 (BPR/AS-IS/TO-BE) platform capability supports system-assisted draft generation from structured RLCO data and manual authoring via the web-based BPMN editor (Sec.No1.2.5.2).
190	**Infrastructure sizing needs to be provided by the supplier?**	YES — infrastructure sizing MUST be defined, documented and delivered by the Supplier in the Deployment Architecture document under Section VII Sec.No2.6.2 early in the Contract. Per Sec.No3.0.2 (p.222), Sec.No3.1, Sec.No3.2, Sec.No3.3 (p.223 — 'No hardware is procured under this Contract') and Sec.No1.1.1.7 (p.149): procurement and provisioning of the infrastructure (compute including GPU, storage, networking, HSM-based KMS, security) is the Purchaser's responsibility on GoP-provided Tier-3+ infrastructure within Pakistan, multi-zone across ≥ 2 independent AZs. The Supplier documents: • Required vCPU/RAM/storage/network/GPU sizing per component and per environment (Dev, Staging/UAT, Production, DR per Sec.No1.3.5.1). • Auto-scaling thresholds and horizontal scaling architecture (Sec.No1.5.3, p.198). • Network and storage specifications (Sec.No3.0.2). • HSM-based KMS sizing and architecture (Sec.No1.3.4.4). The Annex Tech-I Resource Scaling rubric (Section X, p.439) evaluates vCPU, RAM, Storage, Network at proposal stage. Indicative platform specifications are developed in collaboration with the selected Supplier during Inception. See also S#107/row 110, S#88/row 91 (responsibility boundaries).
191	**Which team members are necessary to be on-site for the entire project?**	On-site presence requirements will be based on the supplier's implementation approach, subject to Purchaser approval, with the team mobilised throughout the Contract Period and adequate presence across the six jurisdictions; related costs are the supplier's responsibility. Please also refer to S# 14 and 35 (team mobilisation).
192	**In the presence of Govt Cloud First Policy, Would it be acceptable to propose tier-3 data center hosting that would be compliant with govt. Cloud first policy.**	Yes — Tier-3 data centre hosting within Pakistan, compliant with the GoP Cloud and Infrastructure Policy and the national data-residency framework, is the required hosting model. Per Section VII Sec.No3.0.2 (p.222), hosting MUST be on GoP-provided infrastructure (a national government data centre or a GoP-approved public cloud environment) meeting Tier-3 or

		higher standards, physically located within Pakistan, multi-zone across at least two independent availability zones. Per Sec.No1.1.1.7 (p.149), the solution MUST be cloud-agnostic with no dependency on a vendor-operated cloud not approved by the Government of Pakistan.The Supplier does not procure, supply or price the underlying hosting infrastructure (Sec.No3.1, Sec.No3.2, Sec.No3.3 — 'No hardware is procured under this Contract'). The specific designated hosting environment (data centre or GoP-approved cloud) is selected by the Purchaser and will be confirmed to the selected Supplier post-award.
193	**Can Software be proposed on perpetual License model or Software as Service Model is acceptable? As their might be some module that will be charged on Annual basis like AI module**	Both perpetual licensing and subscription/SaaS-style licensing models may be proposed for the relevant components, subject to the mandatory IP, no-lock-in, source-code transfer and operational-independence requirements of Section VII Sec.NoG.3 (p.284–285) and Section IX SCC GCC 15.4 (p.390). • Custom-developed components (built specifically for the PRR under this Contract): IP vests in GoP immediately upon creation (Sec.NoG.3.1); full source code transfer is mandatory (Sec.NoG.3.3); SaaS-only licensing without source-code transfer is NOT acceptable for custom-developed components. • Pre-existing proprietary OEM components: a perpetual government-use licence with rights to appoint third parties for maintenance/enhancement/integration is required (SCC GCC 15.4); subscription/SaaS licensing is acceptable for such pre-existing components provided the no-lock-in regime is met — explicit declaration in the Technical Proposal, sufficient transparency and documentation (Sec.NoG.3.5), source-code escrow at go-live, major version releases, and annually during maintenance (Sec.NoG.3.6), and no embedded proprietary lock-in (Sec.NoG.3.3). • AI artefacts (prompt templates, scoring logic, feature engineering, orchestration logic) developed/customised under the Contract: GoP IP (Sec.NoG.3.5); the underlying AI engine where pre-existing and proprietary may operate on perpetual or subscription terms with the conditions above. Recurring licence/subscription costs MUST be reflected in the Recurrent Cost Sub-Table (Section IV Form 3.5).
194	**Is there any earnest money involved in RFP?**	No.
195	**Could you please clarify how the outputs of the BPR As-Is / To-Be workflows, IT Readiness Assessment, and Cost Impact Assessment (SCM / RIA-lite) activities are expected to relate to the PRR platform?**	The outputs of the BPR AS-IS/TO-BE, IT Readiness Assessment, and Cost Impact Assessment (SCM/RIA-lite) activities BOTH inform AND populate the PRR platform as structured, traceable records: • BPR (AS-IS/TO-BE) outputs are stored as BPMN 2.0 XML artifacts with a structured workflow data model and human-readable PDF rendering, with full versioning and immutable audit (Section VII Sec.No1.2.5.1, p.163). They are linked to the PRR RLCO Record ID and version, and to the agency/jurisdiction/sector (Sec.No1.2.5.5). • IT Readiness records are linked bidirectionally to the PRR RLCO Record ID and version, the AS-IS and TO-BE workflow artifact IDs and versions, the agency/jurisdiction/sector (Section VII Sec.No1.2.6.1, p.165). Readiness scoring drives Quick Win / Medium / Complex prioritisation for PBP and phased automation (Sec.No1.2.6.3). • Cost Impact (SCM/RIA-lite) outputs are linked to RLCO records and contribute to the Reform Pack (Section VII Sec.No1.2.7). • Sector Reform Packages (minimum five sectors per Sec.No1.2.5.5) consolidate mapped RLCO set, approved AS-IS and TO-BE workflows, bottleneck analysis, linked IT readiness and cost impact data, and linked

		legal change items, exportable as a complete reform pack. These artefacts are therefore not consulting deliverables alone; they are first-class, configurable PRR functionality and structured records.
196	**Could you please clarify whether the As-Is / To-Be workflow outputs are expected to become structured PRR records linked to RLCOs, or whether it would be sufficient to submit them as consulting deliverables with references or attachments maintained in PRR?**	AS-IS and TO-BE workflow outputs MUST become structured PRR records linked to the relevant RLCOs — they are not acceptable as consulting deliverables alone. Section VII Sec.No1.2.5.1 (p.163) requires workflow artifacts to be maintained in three synchronised representations: BPMN 2.0 XML (authoritative machine-readable), structured workflow data model (for analytics and rule-based checks), and human-readable PDF rendering. Each artefact MUST capture process steps, actors, swimlanes, decision points, inputs/outputs, required documents, fees and time bands, service channels, and inter-agency handoffs. Per Section VII Sec.No1.2.11.4 (p.178), AS-IS workflows MUST be documented for a minimum of one hundred (100) priority economic activities across five sectors, with PRR-linkage to mapped RLCO processes. Per Sec.No1.2.6.1, IT readiness records are bidirectionally linked to the RLCO and to the AS-IS / TO-BE workflow artefact IDs and versions. The Module 5 BPR module (Sec.No1.2.5) and Module 4 Mapping Enablement (Sec.No1.2.4) provide the platform capability for this; the TA workstream produces the analytical content. The same artefacts are also delivered as TA deliverables (Table 1.2.11-A — TA Minimum Deliverables, p.179–180).
197	**Could you please clarify whether PRR should include dedicated functionality for IT Readiness Assessment scoring, classification and tracking, or whether it is only expected to store the final assessment outputs and recommendations prepared during implementation?**	PRR MUST include dedicated, configurable functionality for IT Readiness Assessment scoring, classification and tracking — not merely storage of final outputs. Per Section VII Sec.No1.2.6 (p.165) — Module 6 IT Readiness Assessment Module:• Sec.No1.2.6.1 Linkage and Traceability: each IT readiness assessment record MUST be bidirectionally linked to the PRR RLCO Record ID and version, the associated AS-IS and TO-BE workflow artifact IDs and versions, and the agency/jurisdiction/sector.• Sec.No1.2.6.2 Readiness Data Model: structured readiness schema with controlled vocabularies and configurable scoring; BOI/AKTU administrators MUST be able to configure vocabulary lists and scoring thresholds without code changes.• Sec.No1.2.6.3 Readiness Scoring and Prioritisation: the System MUST compute an overall readiness rating for each RLCO — at minimum Quick Win, Medium Complexity, or Complex — with optional sub-scores for channel readiness, data readiness, integration readiness, and payments and authentication readiness. The System MUST support prioritisation tags and automation pathway classification. All readiness assessments MUST pass through a draft-to-approved workflow with versioning and immutable approval records.• Sec.No1.2.6.4 Reports and Exports: readiness distribution dashboards by jurisdiction, agency and sector; top blockers report by category frequency; integration dependency matrix. IT readiness records MUST be restricted to internal roles only with every access and export event logged.The IT Readiness functionality is a permanent, configurable PRR module — both used during TA execution and retained as part of the platform for ongoing IT Readiness assessments by BOI/AKTU post-go-live.

198	**Could you please clarify whether PRR should include calculation functionality and reusable cost parameters for the Cost Impact assessment component, or whether maintaining the final outputs and reports would be sufficient?**	The PRR MUST include calculation functionality and reusable cost parameters for the Cost Impact Assessment component — not only storage of final reports. Per Section VII Sec.No1.2.7 (p.166–168) — Module 7 Cost Impact Assessment Module (SCM/RIA-lite) — the Module MUST: • Support structured capture of cost drivers — process steps; time bands per step; fee and charge components; document and form requirements; channel mode; agency contact frequency; rework rates. • Provide built-in calculations supporting Standard Cost Model (SCM) and RIA-lite methodologies with configurable formulas, parameter libraries and multi-currency support. • Support reusable cost parameters (the parameter library — average hourly wage rates by role/region; document/form preparation costs; transport costs; opportunity costs; etc.) configurable by BOI/AKTU without code changes. • Enable AS-IS versus TO-BE comparison reports with quantified impact (time-saving, cost-saving, document-elimination, fee-rationalisation). • Provide exports of cost impact assessments as structured records linked to the RLCO Record ID and workflow artefact. The Supplier MUST therefore deliver the Cost Impact module as configurable PRR functionality with calculation engine, parameter management UI, and report generation, in addition to producing the AS-IS/TO-BE cost-impact assessment outputs as TA deliverables.
199	**Could you please clarify whether these assessments are expected to be performed at the individual RLCO level, or at the level of broader business processes / reform packages covering multiple RLCOs?**	Assessments operate at multiple linked levels, depending on the analytical purpose: • Individual RLCO level: each RLCO record carries linkage to its IT Readiness Assessment (Section VII Sec.No1.2.6.1, p.165) and to its associated AS-IS and TO-BE workflow artefact IDs and versions, the agency/jurisdiction/sector. This linkage is bidirectional and visible from both the RLCO record and the workflow artefact. • Business process / journey level: AS-IS and TO-BE workflow artefacts (Section VII Sec.No1.2.5) can represent processes spanning multiple RLCOs and agencies — 'Sec.No1.2.5.2 Workflow Types and Creation: The System MUST support … end-to-end business journey workflows spanning multiple RLCOs and agencies' (p.163). • Sector Reform Package level: per Sec.No1.2.5.5 (p.163), the System MUST support consolidation of sector packages covering at minimum five sectors, each containing the mapped RLCO set, approved AS-IS and TO-BE workflows, bottleneck analysis, linked IT readiness and cost impact data, and linked legal change items, exportable as a complete reform pack (referenced in Figure 6). • Aggregation/analytics: dashboards and reports aggregate up — readiness distribution by jurisdiction/agency/sector (Sec.No1.2.6.4); top blockers report by category frequency; integration dependency matrix. In practice, primary capture is at the individual RLCO/workflow level; analytical packaging and reform-pack delivery happens at the sector and business-journey levels. The Supplier proposes the analytical hierarchy for each TA wave in the Agreed Project Plan.

200	**Could you please clarify which parts of the BPMN/BPR, IT Readiness and Cost Impact assessment components are expected to be built as permanent PRR system functionality, and which may be delivered as consulting outputs?**	The BPMN/BPR (Module 5), IT Readiness Assessment (Module 6) and Cost Impact Assessment (Module 7) capabilities are MANDATORY permanent PRR system functionality, not consulting outputs. Section VII Sec.No1.2.5–Sec.No1.2.7 (p.163–168) specify these as Modules of the system with detailed mandatory functional requirements:• Module 5 (Sec.No1.2.5): BPMN 2.0 authoring/import/export; workflow approval states; bottleneck tagging with configurable categories; TO-BE redesign rationale capture; legal amendment traceability; sector reform package consolidation.• Module 6 (Sec.No1.2.6): IT readiness data model with controlled vocabularies; configurable scoring; Quick Win / Medium / Complex prioritisation; readiness distribution dashboards by jurisdiction/agency/sector; top blockers report; integration dependency matrix.• Module 7 (Sec.No1.2.7): Cost driver capture; built-in SCM/RIA-lite calculations; multi-currency support; AS-IS versus TO-BE comparison; exports.All three modules MUST be configurable by BOI/AKTU without code changes (where specified) and MUST integrate via the RLCO linkage and traceability model. The associated analytical and reform outputs produced using these modules (mapped activity sets, completed assessments, sector reform packs) are also delivered as TA workstream deliverables (Table 1.2.11-A, p.179–180).
201	**The RFP requires an HSM-based Key Management System hosted within Pakistan. Is a shared government HSM service available, or must each deployment provision its own dedicated HSM appliance? What HSM form factor is expected — network-attached appliance, cloud HSM, or PCIe card?**	Section VII Sec.No1.3.4.4 (p.191) requires an HSM-based Key Management System (KMS) hosted within Pakistan. The clause does not prescribe a specific HSM form factor (network-attached appliance, cloud HSM, or PCIe card); the Supplier MUST document the proposed HSM form factor, sizing and KMS architecture in the Deployment Architecture document delivered under Sec.No2.6.2. Whether a shared government HSM service is available will be confirmed to the selected Supplier. Where a shared service is not available, the Supplier may propose a dedicated HSM (physical appliance or GoP-approved cloud HSM) meeting in-country hosting and PSS compliance requirements (Sec.No1.3.4.3) and data-residency requirements (Sec.No3.0.2). Mandatory functional requirements per Sec.No1.3.4.4: no application-layer access to private keys beyond defined and audited roles; role-based separation of duties for key access; automated key rotation, revocation, and lifecycle management; immutable audit records of all key operations. The HSM-based KMS forms part of GoP-provided infrastructure (Sec.No3.1, Sec.No3.2, Sec.No3.3 — 'No hardware is procured under this Contract'). Final HSM approach is subject to Purchaser approval.

202	**The RFP mandates a Web Application Firewall protecting all public and government portal entry points. Is the WAF expected to be provisioned by the Supplier as part of the application stack, or is a governmentoperated WAF already in place at the data center perimeter that the application will sit behind?**	The Web Application Firewall (WAF) protecting all public and government portal entry points is part of the security architecture that the Supplier MUST design and configure per Section VII Sec.No1.3.4.2 (p.191) and Sec.No1.6.4 (p.203). WAF ownership and operation: • **Supplier responsibility**: design the WAF architecture, configure rules, integrate with the API Gateway and microservices (Sec.No1.3.6.1), tune and maintain WAF rules during Warranty (2 years per SCC GCC 29.1) and AMC (Y1–Y3 mandatory per SIT-2 Notes). • **Hosting**: the WAF runs as a software component within the GoP-provided infrastructure (per Sec.No3.0.2; Sec.No3.1–Sec.No3.3 — 'No hardware is procured under this Contract'); WAF compute resources are part of the documented infrastructure sizing in the Deployment Architecture document under Sec.No2.6.2. • **Technology choice**: the Supplier may propose a commercial WAF (e.g., F5, Akamai, Cloudflare on-prem version, Imperva, Citrix NetScaler) or an open-source/self-managed WAF (e.g., ModSecurity with OWASP Core Rule Set, NAXSI), provided the Sec.NoG.3 IP regime, the cloud-agnostic mandate (Sec.No1.1.1.7) and OWASP Top 10 compliance (Sec.No1.6.1, p.202) are met. • **DDoS protection** (Sec.No1.6.4): may be provided through the WAF or as a separate component; the Supplier proposes the design. • **Pre-existing proprietary WAF components**: declare in Technical Proposal per Sec.NoG.3.5; perpetual government-use licence per SCC GCC 15.4 (p.390); escrow at go-live, major version releases, annually (Sec.NoG.3.6). Recurring WAF licence/subscription costs MUST be reflected in the Recurrent Cost Sub-Table (Section IV Form 3.5).
203	**The security architecture requires four distinct network zones — Public, Application, Protected Data, and Integration — separated by strict policy controls and private subnets. Does the GoP data center support software-defined networking that allows the Supplier to define and manage these zones independently, or are network topology changes subject to a separate government network team approval process?**	The four distinct network zones — Public, Application, Protected Data, Integration — with strict policy controls and private subnets MUST be implemented by the Supplier per Section VII Sec.No1.3.4.1 (p.190) — Network Architecture and Zero-Trust Segmentation. Verbatim:• **Public Zone**: serves public users; no direct access to internal services; protected by WAF and DDoS controls.• **Application Zone**: hosts the microservices (Identity & Access, Registry Core, Workflow Engine, Mapping Enablement, BPR, IT Readiness, Cost Impact, Public Portal, RIS/AKTU, AI Assist, Search, Notification, Audit, Reporting, Integration, API Gateway per Table 1.3.1-A).• **Protected Data Zone**: hosts the 7 datastores (per Sec.No1.3.3.1, p.189) — Primary Registry DB, Document Store, Search Index, Analytics Warehouse, BPMN Repository, Vector Database, Immutable Audit Store. Access limited to authorised services in the Application Zone.• **Integration Zone**: hosts the integration adapters / outbound connectors for priority government systems (NADRA, gazette, e-Sign, BOI/One Window, provincial systems per Sec.No1.3.6.2).Inter-zone controls:• No service communicates across zone boundaries without explicit authorisation (Sec.No1.3.4.1).• Private subnets with least-privilege routing.• Inter-zone traffic via authenticated and encrypted channels (mutual TLS, service mesh, or equivalent).• Centralised SIEM monitoring of all inter-zone flows (Sec.No1.3.4.6).The Supplier proposes the specific network technology and segmentation mechanism (VPCs, security groups, service mesh, container network policies, network virtualisation) in the Deployment Architecture document under Sec.No2.6.2. The four-zone segmentation operates within the GoP-provided infrastructure environment.

204	**The RFP requires SIEM-based security monitoring feeding key events from all gateways, microservices, and IAM service. Is the Supplier expected to deploy and operate a SIEM instance as part of the solution, or does a government-operated SOC and SIEM already exist that the PRR must integrate with?**	Per Section VII Sec.No1.3.4.6 (p.191) — Centralised Logging and Monitoring — 'The System MUST implement centralised logging, distributed tracing end-to-end, and SIEM-based security monitoring' with key events from all gateways, microservices, workflow engine, search cluster and IAM service. The Supplier is responsible for deploying and operating the SIEM and security monitoring capability AS PART OF THE PRR SOLUTION, within the GoP-provided hosting environment. Supplier responsibilities: • Deploy a SIEM instance (commercial or open-source — e.g., Wazuh, Elastic Security, Splunk; subject to the IP and licensing regime of Sec.NoG.3 and SCC GCC 15.4, p.390) within the GoP-provided environment per Sec.No3.0.2. • Configure log feeds from all PRR components — gateways, microservices, workflow engine, search cluster, IAM service, API Gateway — into the centralised SIEM with tamper-evident controls and retention in the Immutable Audit Store (Sec.No1.3.4.6, Sec.No1.1.4 — 7-year retention). • Configure SIEM-based detection rules, privileged session logging, real-time alerts for outages, elevated error rates, suspicious access patterns, and rate-limit breaches. • Implement security incident response per Sec.No1.6.7 — notification within four (4) hours of confirmed detection. • Distributed tracing end-to-end (Sec.No1.3.4.6) — typically via OpenTelemetry or equivalent. Government SOC integration: • Where a government-operated SOC exists, the Supplier integrates the SIEM with the government SOC through standard log-forwarding protocols (syslog, SIEM API, log-aggregator). The current status of any central GoP SOC will be confirmed during Inception. • Where a government SOC does not exist, the Supplier's SIEM is the operational security monitoring capability for the PRR. SIEM operations during Warranty (2 years) and AMC (Y1–Y3 mandatory) are included in the respective scopes. Ongoing SIEM operations costs (licences, tooling) MUST be reflected in the Recurrent Cost Sub-Table (Section IV Form 3.5).

205	**The RFP requires mandatory MFA for all government portal users. Also, there is a requirement to support integration with government SSO platforms. Which specific government SSO platform or identity provider is the Supplier expected to integrate with — is there a single federal SSO service, multiple agency-level identity providers, or a combination? Does the existing government SSO platform natively support MFA, or does MFA need to be enforced at the application layer by the PRR system itself as a compensating control when SSO is the authentication mechanism? If the SSO platform does not support MFA natively, is OTP-based fallback authentication considered sufficient to meet the mandatory MFA requirement for government users, or must the Supplier implement an additional MFA layer on top of the SSO token? Are provincial government users expected to authenticate through the same federal SSO platform, or do provincial governments operate separate identity providers that the Supplier must also integrate with? What protocol does the government SSO platform expose — SAML 2.0, OpenID Connect, or a proprietary protocol — and is technical documentation and a sandbox environment available for integration development?**	Section VII Sec.No1.3.6.2 (p.194) lists 'government SSO platforms' as a priority integration target without specifying the particular platform, protocol or sandbox arrangement. Per Sec.No1.6.2 (p.203), mandatory MFA applies to all publishers, reviewers, administrators and AI reviewers, with SSO integration with government identity providers required.The specific government SSO platform(s), protocol (SAML 2.0 / OpenID Connect / proprietary), MFA support at IdP level, and provincial vs federal arrangement will be confirmed to the selected Supplier during Inception. The PRR MUST be architected to accommodate any combination of these:• A single federal SSO with provincial branches, OR multiple jurisdiction-specific identity providers — supported via configurable IdP federation.• MFA enforced natively at SSO/IdP, OR enforced at PRR application layer as a compensating control where the IdP does not natively support MFA — the requirement that mandatory MFA applies to all privileged users (Sec.No1.6.2) is met irrespective of which layer enforces it.• OTP-based MFA (TOTP / SMS / email OTP) is acceptable to meet the mandatory MFA requirement; the Supplier should propose hardware-token or push-notification options where higher assurance is required.• Standard protocols (SAML 2.0, OpenID Connect 1.0, OAuth 2.0) are preferred; the Supplier MUST support multiple IdP protocols to accommodate federal and provincial arrangements.Technical documentation, sandbox environment and credentials are arranged by the Purchaser during Inception (Sec.No1.3.6.3 integration modes). The Supplier builds the technical integration.
206	**The RFP specifies seven distinct datastores including a primary relational database, document store, search index, analytics warehouse, BPMN repository, vector database, and immutable audit store. Are all seven expected to be separate dedicated database instances, or can some be co-hosted?**	The PRR MUST implement seven (7) distinct, purpose-specific datastores per Section VII Sec.No1.3.3.1 (p.189): (i) **Primary Registry Database** — relational transactional store for all RLCO records and metadata, workflow states, consultation submissions, user roles, publication states. High availability, replication, encryption at rest, point-in-time recovery (PITR). [e.g., PostgreSQL, Oracle DB, MS SQL Server] (ii) **Document and Artifact Store** — encrypted object storage for Acts, Rules, SROs, Notifications, attachments, exported reform packs, consultation reports, AI diagnostic artifacts. Integrity hashing and lifecycle policies. [e.g., S3-compatible object storage, MinIO, Ceph] (iii) **Search Index** — full-text and faceted search index optimised for fast public and internal RLCO discovery. Urdu language analyser integrated per Sec.No3.0.1. [e.g., Elasticsearch, OpenSearch, Solr] (iv) **Analytics Warehouse or Mart** — separate reporting store for management dashboards and KPI reporting, isolated from the transactional

		database. 'No dashboard or reporting workload MUST directly query the primary transactional database.' Near-real-time or scheduled ETL acceptable (see S#228/row 231). (v) **BPMN Repository** — workflow diagram storage and versioning. Synchronised with structured workflow data model and PDF rendering per Sec.No1.2.5.1. (vi) **Vector Database** — for AI-assisted semantic similarity, conflict detection, and regulatory knowledge graph queries (Sec.No1.2.10.6). Self-hosted within GoP-controlled hosting per Sec.No1.6.9 (see S#227/row 230). (vii) **Immutable Audit Store** — tamper-evident log store for all critical system events. 7-year retention per Sec.No1.1.4. Tamper-evidence via cryptographic hash chaining and/or write-once (WORM) object storage (see S#225/row 228). All datastores operate within the GoP-provided infrastructure (Sec.No3.0.2) and are within the Protected Data Zone (Sec.No1.3.4.1). All data encrypted at rest with HSM-managed keys (Sec.No1.3.4.4, Sec.No1.6.3); backup vaults encrypted and stored in a separate geographic zone (Sec.No1.3.5.3). The Supplier proposes specific technologies in the Deployment Architecture document under Sec.No2.6.2.
207	**The immutable audit store is described as tamper-evident. What technical mechanism is expected to prove tamper-evidence — append-only storage, cryptographic hash chaining, write-once object storage, or a distributed ledger approach?**	Tamper-evidence of the Immutable Audit Store (Section VII Sec.No1.3.3.1 datastore (vii), Sec.No1.1.4 retention, Sec.No1.3.4.6 centralised logging) may be achieved through any combination of the following technical mechanisms — the Supplier proposes the design in the Architecture document under Sec.No2.6.2: • **Cryptographic hash chaining**: each audit record is hashed and chained to the previous record's hash (Merkle-tree or simple chain); periodic anchor hashes published / archived; any tampering with a record invalidates the subsequent chain. • **Write-Once-Read-Many (WORM) object storage**: object-storage tier configured with object-lock / immutability / retention policies preventing deletion or modification within the retention period. • **Append-only log infrastructure**: write-only append-only log files with cryptographic signature on each segment; rotated and sealed segments archived to WORM storage. • **Cryptographic timestamping**: trusted-timestamp service signs audit batches at scheduled intervals; tampering detectable via timestamp verification. • **Periodic integrity verification**: scheduled job verifies hash chain integrity; alerts on detected breaks. A distributed ledger (blockchain) is NOT mandated (see S#92/row 95). The above conventional approaches meet the Sec.No1.1.4 mandate ('Audit logs MUST be protected against alteration or deletion'). Audit data is encrypted at rest with HSM-managed keys per Sec.No1.3.4.4 and stored within the Protected Data Zone per Sec.No1.3.4.1. The 7-year retention applies (Sec.No1.1.4).
208	**Section 1.3.3.4 requires every field in the RLCO data model to carry a four-tier data classification tag. Is this classification enforced at the database column level through row-level security or column-level encryption, or is it enforced at the application layer only?**	Per Section VII Sec.No1.3.3.4 (p.192), every field in the RLCO data model MUST carry a four-tier data classification tag:(1) Public — published on the portal(2) Government Restricted — accessible to agencies only(3) Internal — accessible to BOI/AKTU only(4) Confidential — encrypted at rest and HSM-protectedThe classification MUST be enforced through appropriate technical controls as designed by the Supplier:• Application-layer: RBAC-driven access control (Sec.No1.6.2, p.203) with role-to-classification mappings; classification metadata attached to each field; API response filtering based on caller's role and field classification; UI

		rendering controls that suppress restricted/internal/confidential fields for unauthorised roles.• Database-layer: row-level security and/or column-level access controls for restricted tiers (typically tiers 2–4); column-level or field-level encryption for tier 4 with keys held in the HSM-based KMS (Sec.No1.3.4.4); audit logging of all access to tiers 2–4 (Sec.No1.6.7).• Storage-layer: tier 4 confidential fields stored with envelope encryption using HSM-protected master keys.• Audit-layer: every access and export event for tiers 2–4 logged in the Immutable Audit Store (Sec.No1.3.4.6, Sec.No1.6.7).The Supplier MUST design the layered enforcement mechanism in the Architecture document under Sec.No2.6.2 and validate it during OAT-2 (Security Controls and Access Management, Sec.No4.3.2).
209	**The vector database for AI semantic similarity is listed as a mandatory separate datastore. Does the Purchaser have a preference or requirement for a specific vector database technology particularly given data residency constraints and the requirement for government-hosted deployment?**	No specific vector database product is mandated. The Supplier may propose any vector database that meets the architectural and operational requirements: • **In-country data residency**: hosted within Pakistan within GoP-provided infrastructure (Section VII Sec.No3.0.2, p.222; Sec.No1.1.1.4 Data Protection Legislation). • **Self-hosted / government-controlled operation**: no transmission of PRR data to external AI platforms, model APIs or cloud-based AI services without explicit prior written Purchaser approval (Sec.No1.6.9, p.204). • **Performance**: meeting the Sec.No1.5 performance targets — interactive similarity-search queries aligned with workflow state transition targets (≤ 5 s P95 per Table 1.5-A) for the registry growing to tens of thousands of RLCOs (see S#231/row 234). • **No vendor lock-in** (Sec.NoG.3.1, Sec.NoG.3.7): full source code transfer for PRR-specific custom development; operational independence per Sec.NoG.3.8. • **IP regime** (Sec.NoG.3.4, Sec.NoG.3.5; SCC GCC 15.4): open-source disclosure with no viral/copyleft licences; pre-existing proprietary components declared, perpetual government-use licensed and escrow-deposited per Sec.NoG.3.6. • **Encryption at rest** with HSM-managed keys (Sec.No1.3.4.4, Sec.No1.6.3). Acceptable approaches include open-source options (e.g., Milvus, Qdrant, Weaviate, pgvector on PostgreSQL, OpenSearch k-NN), or commercial alternatives subject to declaration and escrow. The Supplier proposes the vector database, indexing strategy (e.g., HNSW, IVF), sharding/partitioning, and sizing in the Architecture document under Sec.No2.6.2 / AI Layer Architecture (Section VII Figure 14). The vector database is one of the 7 mandated datastores (Sec.No1.3.3.1, p.189 — datastore (vi)).

210	**The analytics warehouse must be isolated from the transactional database. Is real-time or near-real-time replication expected between the transactional database and the analytics warehouse, or is a daily ETL batch acceptable for dashboard data freshness?**	The Analytics Warehouse MUST be isolated from the transactional database (Primary Registry Database) per Section VII Sec.No1.3.3.1 (p.189): 'No dashboard or reporting workload MUST directly query the primary transactional database.' Either near-real-time replication or scheduled ETL is acceptable, subject to the reporting/analytics SLAs and the isolation requirement. Design options the Supplier may propose: • **Near-real-time replication** (Change Data Capture / log-based replication / event streaming): supports operational dashboards with low data latency (typically minutes); higher infrastructure overhead. Suitable where SLAs require real-time/near-real-time operational metrics. • **Scheduled ETL** (batch extraction at defined intervals — e.g., hourly, daily): simpler architecture, lower overhead, deterministic load windows. Suitable for periodic management dashboards and KPI reporting where slight data latency is acceptable. • **Hybrid approach**: near-real-time for high-priority operational metrics (e.g., workflow SLA breaches, active consultations) + scheduled ETL for historical analytical workloads. Mandatory regardless of approach: • Isolation from the primary transactional database — no dashboard/reporting workload queries the primary DB directly (Sec.No1.3.3.1). • Encryption at rest with HSM-managed keys (Sec.No1.3.4.4, Sec.No1.6.3). • Within the Protected Data Zone (Sec.No1.3.4.1) with controlled access (Sec.No1.6.2 RBAC). • Backups configured per Sec.No1.3.5.3 (RTO ≤ 4 h, RPO ≤ 1 h applies to the analytics warehouse as appropriate to its criticality). • Audit logging of access for tiers 2–4 data classification (Sec.No1.3.3.4). The Supplier proposes the specific approach with target data freshness SLAs in the Architecture document under Sec.No2.6.2; finalised in the Agreed Project Plan during Inception.
211	**The RFP requires the search index to support semantic search in Urdu using an Urdu language analyzer.Which Urdu language analyzer is expected — a custom-trained model, an open-source Urdu NLP library,or a standard ICU tokenizer with Urdu locale configuration? The difference in accuracy and build effortis substantial.**	Per Section VII Sec.No3.0.1 (p.222), the System MUST include 'a Urdu language analyser integrated into the search index to support Urdu-language RLCO discovery.' The RFP does not mandate a specific Urdu analyser implementation — the Supplier is free to propose an approach that meets the search-quality requirements and operates within government-controlled hosting (Sec.No1.6.9, Sec.No1.2.10.1). Acceptable approaches include:• Open-source Urdu NLP library (e.g., libraries supporting Urdu tokenisation, stemming, lemmatisation) integrated into the search engine.• ICU-based tokenisation with Urdu locale configuration plus custom stop-word and stemming rules.• Custom-trained Urdu language model or domain-tuned Urdu embedding model (subject to the AI governance regime — operating within GoP-controlled hosting per Sec.No1.6.9, with model versioning and provenance logging).• Hybrid approach combining lexical analysis (BM25/lexical search with Urdu morphology) and semantic/vector search using Urdu embeddings (subject to the Sec.No1.6.9 prohibition on external embedding APIs without Purchaser approval — see S#233/row 236).Requirements regardless of approach:• Full Unicode NFC normalisation for Urdu text storage and retrieval (Sec.No3.0.1).• Jameel Noori Nastaleeq or equivalent web-safe Urdu font for rendering (Sec.No3.0.1).• Locale-aware tokenisation handling Urdu Nastaleeq script characteristics.• Search performance meeting the P95 targets in Table 1.5-A (search/browse ≤ 2 s).The Supplier proposes the Urdu analyser strategy

		in the Technical Proposal and documents the design in the Architecture document under Sec.No2.6.2.
212	**Section 1.3.3.5 requires future-dated regulatory changes and automatic deactivation upon expiry. Does this require a scheduled job that runs at midnight to transition record states, or must the system evaluate effective dates in real time on every query, including for public API responses?**	Per Section VII Sec.No1.3.3.5 (p.192) — Version Control and Time-Aware Design: 'The System MUST support effective date tracking for all RLCO records, historical snapshot retrieval, future-dated regulatory changes, and automatic deactivation upon expiry. Regulatory time-state MUST be machine-readable and queryable via API, enabling comparison between current, historical, and future versions of any RLCO.' The clause requires reliable, timely and fully audited state transitions; the implementation mechanism is the Supplier's design choice. Acceptable approaches include: • Scheduled jobs that run at configurable cadence (e.g., midnight Pakistan Standard Time) to transition record states (activate future-dated changes, deactivate expired records), with logged execution and exception handling. • Effective-date evaluation in real-time on every query — including for public API responses — using server-side date filtering against the effective and expiry dates stored on the record. Each public/API response returns only records currently in effect on the query date/timestamp. • Hybrid approach — scheduled jobs maintain the canonical state transitions and write audit-trail events, while real-time effective-date filtering ensures correct visibility even between scheduled job runs (recommended for high-volume public access). Mandatory non-functional requirements regardless of mechanism: • Reliability: state transitions MUST occur within the agreed precision (typically same-day) without manual intervention. • Audit: every state transition (activation/deactivation) MUST be logged in the Immutable Audit Store with timestamp, source effective-date trigger, and resulting state per Sec.No1.1.4 (p.151). • Time-zone consistency: Pakistan Standard Time (PKT, UTC+05:00) as the canonical regulatory time-zone. • Public API: time-aware responses with effective-date parameters for historical and future versions (Sec.No1.3.3.5). The Supplier documents the chosen mechanism in the Architecture document under Sec.No2.6.2; the approach is validated during OAT-1 (Performance) and OAT-2 (Security/Access).
213	**The AI Feature 5 requires a vector database for similarity and conflict detection across the full RLCO registry. As the registry grows to tens of thousands of RLCOs, what is the expected maximum acceptable latency for a similarity search query to return results to the reviewer interface?**	Per Section VII Sec.No1.2.10.6 (p.177) — AI Feature 5 Similarity and Conflict Detection — the System MUST include a vector database or semantic search mechanism for detecting potential duplication, overlap or conflict between new/proposed RLCOs and existing entries; flagged similarities/conflicts MUST be surfaced as advisory flags requiring human review and a documented resolution decision. The mandatory P95 response targets for the platform (Section VII Table 1.5-A, p.201) apply to user-interactive functions: • Public search/browse ≤ 2 s; RLCO detail retrieval ≤ 3 s; workflow state transition ≤ 5 s; record save/create ≤ 3 s. Vector similarity search invoked interactively from the reviewer interface MUST meet the interactive-response target appropriate to its workflow point — typically aligning with workflow state transition (≤ 5 s P95). For non-interactive batch similarity checks (e.g., periodic full-registry scans), the Supplier proposes appropriate target SLAs in the Agreed Project Plan. As the registry grows to tens of thousands of RLCOs, the platform MUST remain horizontally scalable per Sec.No1.5.3 (p.198). The Supplier MUST propose the vector database technology, indexing strategy (e.g., HNSW, IVF), sharding/partitioning approach, hardware sizing (vector dimensions

		× index size × QPS), and document the design in the AI Layer Architecture (referenced in Figure 14 of Section VII).
214	**The RFP requires all AI outputs to be stored with input parameters, model version, and generationtimestamp for reproducibility. Does reproducibility mean the system must be able to re-run the identicalAI job and produce bit-identical output, or is it sufficient to store the inputs and version metadata suchthat a human auditor can understand what was generated and why?**	Reproducibility of AI outputs (Section VII Sec.No1.2.10.x and Sec.No1.6.9, p.204) means the System stores sufficient inputs, model artefacts and metadata so that an AI output can be **traced, audited, and re-derived for the same inputs and model version** — NOT that future invocations of the same model produce bit-identical outputs in all cases (which is generally infeasible for non-deterministic models such as LLMs with sampling).Mandatory artefact retention for each AI output:• **Input parameters**: the full input prompt/payload, including any context windows, retrieved documents, configuration parameters.• **Model version**: model identifier, version/hash, training data version (if applicable).• **Prompt template version** for LLM-based components.• **Generation timestamp** and execution environment.• **Model output**: the raw AI-generated content with associated confidence/score where applicable.• **Provenance chain**: link to the source RLCO record / workflow artifact / consultation submission that triggered the AI invocation.• **Human review decision** where the AI output is acted upon (Sec.No1.6.9 human-in-the-loop).All retained in the Immutable Audit Store (Sec.No1.1.4 — 7-year retention) or linked stores (Document/Artifact Store, Vector Database) within GoP-controlled hosting.Bit-identical reproducibility is NOT required where the underlying model is non-deterministic; deterministic re-derivation is required for the rule-based components (scoring engines, classification rules, validation rules) under fixed parameters. The Supplier MUST design the AI governance framework documenting reproducibility expectations per component (see S#256/row 256 for AI governance framework).
215	**Section 1.2.10.1 prohibits AI modules from transmitting data to external AI platforms without written Purchaser approval. Does this prohibition extend to using cloud-based embedding APIs — for example to generate vector embeddings for the similarity search — or only to sending full document content to external generative AI services?**	The prohibition in Section VII Sec.No1.2.10.1 (p.175) and Sec.No1.6.9 (p.204) on transmitting PRR data to external AI platforms without prior written Purchaser approval EXTENDS to cloud-based embedding/inference APIs. The clause Sec.No1.6.9 states verbatim that 'AI Assist Module MUST operate exclusively within government-controlled hosting and MUST NOT transmit PRR data to external AI platforms, model APIs, or cloud-based AI services unless explicitly approved in writing by the Purchaser.' Accordingly: • Embedding generation, vectorisation, and indexing of PRR/RLCO content MUST be performed within GoP-controlled hosting using self-hosted embedding models, unless the Purchaser grants prior written approval for external API use. • Similarity-search inference, NLU classification, sentiment analysis, and any other AI processing involving PRR data is governed by the same rule. • Where the Supplier proposes to use an external embedding API for a specific function, this requires prior written approval supported by documented data-protection safeguards (data minimisation, retention controls, no model-training-on-data clauses, contractual protections). • Any approved external API usage cost assigned to the Supplier MUST be reflected in the Recurrent Cost Sub-Table with explicit assumptions stated. The default expectation is self-hosted embeddings using open-source or licensed embedding models running on GoP-provided GPU/compute infrastructure documented in the Deployment Architecture document (Sec.No2.6.2).

216	**The AI consultation analysis must perform thematic clustering, sentiment analysis, and salience scoring on potentially thousands of submitted comments. Is there a minimum accuracy or precision threshold defined for these AI outputs, and how will accuracy be measured and accepted during OAT?**	Section VII Sec.No1.2.10 (p.174–177) defines the AI Assist Module functional requirements; Sec.No1.2.10.6 (AI Feature 5) covers similarity/conflict detection; thematic clustering, sentiment analysis and salience scoring of consultation submissions are part of the consultation analytics scope. Per Section VII Sec.No1.6.9 (p.204), AI outputs are advisory and subject to human review with documented resolution decision. Minimum accuracy/precision thresholds for AI consultation analytics outputs are NOT fixed at proposal stage in the RFP — these analytics are decision-support tools for BOI/AKTU reviewers, not autonomous decision-makers. The Supplier MUST propose: • A quality measurement framework — precision, recall, F1 score on a labelled validation set; inter-rater agreement metrics; coverage metrics; bias assessment. • A validation approach using a curated test set of representative consultation submissions in English and Urdu. • A confidence-scoring mechanism — every AI output flagged with a confidence band; low-confidence outputs routed to mandatory human review. • An ongoing-monitoring approach — sampling-based human verification of AI outputs in production with drift detection. OAT acceptance for the AI Assist Module (Sec.No4.2.10 Subsystem 10) validates: AI governance controls in place; human approval gates configured; AI output provenance/reproducibility logging; advisory-only operation. Specific quality acceptance thresholds are agreed in the Agreed Project Plan (Sec.No2.6.2) during Inception. The Annex Tech-I Standard Scoring Basis applies to evaluate Proposer methodology at proposal stage.
217	**The Addendum specifies a conversational AI regulatory chatbot with multi-turn context management anda regulatory knowledge graph. Is the knowledge graph expected to be a formal Resource DescriptionFramework (RDF) or property graph structure with explicit relationship modelling, or is an embeddingbased retrieval approach over the RLCO dataset sufficient to satisfy this requirement?**	The regulatory knowledge graph for the conversational AI chatbot (referenced in the AI Assist Module Sec.No1.2.10) may be implemented as a formal RDF/SPARQL graph database OR as a property graph (e.g., Neo4j, Amazon Neptune-compatible, JanusGraph) OR as a hybrid combining graph structures with embedding-based retrieval — at the Supplier's design proposal, provided it meets the functional and architectural requirements:• Operates entirely within GoP-controlled hosting (Sec.No1.2.10.1, p.175; Sec.No1.6.9, p.204).• Multi-turn conversation context management for the regulatory chatbot.• Explicit relationship modelling between RLCOs, agencies, jurisdictions, ISIC sectors, legal instruments, workflows, fees, and applicable conditions — sufficient for accurate question-answering and traceability.• Source provenance — every chatbot answer MUST link to the source RLCO record(s), workflow artefact(s) and legal basis reference. AI outputs are advisory per Sec.No1.6.9 and subject to human-in-the-loop where business actions are involved.• Multilingual support (English + Urdu) per Sec.No3.0.1 (p.222).• Performance targets aligned to interactive use — P95 response within reasonable interactive bounds (the Supplier proposes specific SLA in the Agreed Project Plan).• AI governance regime — model versioning, prompt template versioning, evaluation logs, retention/deletion controls (per AI governance framework, Sec.No1.2.10.1; see S#256/row 256).Where embedding-based retrieval is used for query/answer matching, the prohibition on external embedding APIs without Purchaser approval applies (Sec.No1.6.9; see S#233/row 236). The Supplier documents the knowledge-graph design and embedding strategy in the AI Layer Architecture (Section VII Figure 14).

218	**The API Gateway must enforce request schema validation for all API calls. Is schema validation expected to run synchronously in the request path — adding latency to every API call — or is asynchronous validation with error reporting acceptable for non-critical endpoints?**	API Gateway request schema validation MUST run synchronously in the request path for enforcement. Per Section VII Sec.No1.3.6.1 (p.194), all services MUST be exposed through a centralised API Gateway with OpenAPI-compliant documentation, canonical data exchange formats, and versioned APIs. Schema validation is a security and integrity control that MUST gate request processing. Synchronous validation design (Supplier proposes in Architecture document under Sec.No2.6.2): • **OpenAPI-based validation**: request payloads validated against the published OpenAPI/JSON Schema specification at the gateway layer. • **Latency budget**: validation overhead included in the per-request latency budget; the platform overall must meet the Sec.No1.5 performance targets (Table 1.5-A: workflow state transition ≤ 5 s P95; save/create ≤ 3 s P95; etc.). • **Performance optimisation**: schema validation typically adds sub-millisecond to low-millisecond overhead with optimised parsers and cached schemas — well within the latency budget for the mandatory targets. • **Reject invalid requests** at the gateway with structured error responses; do not propagate invalid requests to backend services. • **Validation observability**: log validation rejections to SIEM (Sec.No1.3.4.6) for security monitoring and abuse detection. Non-blocking / asynchronous post-validation MAY supplement synchronous validation (e.g., deep semantic validation, business-rule checks, ML-based anomaly detection) BUT may not REPLACE synchronous schema enforcement. Bypassing synchronous schema validation would not meet the Sec.No1.3.6.1 enforcement mandate or the Sec.No1.6.x security controls (input validation against OWASP A03:2021 Injection).
219	**The system must generate AI-assisted draft BPMN from structured RLCO data. What level of BPMN fidelityis expected from this AI generation — a simple linear flow with tasks and decision points, or a fullyannotated BPMN 2.0 diagram with swim lanes, data objects, boundary events, and message flows?**	Per Section VII Sec.No1.2.5.2 (p.163), the System MUST support 'both system-assisted draft generation from structured RLCO data and manual authoring via a web-based BPMN editor or import and export of BPMN 2.0 XML.' AI-assisted draft generation produces a BPMN starting artifact for expert refinement; final approved BPMN workflows MUST capture the full Section VII Sec.No1.2.5.1 (p.163) structured workflow model.Expected AI-generated draft fidelity:• Sequence flow with tasks (user tasks, service tasks, manual tasks) and start/end events.• Exclusive and parallel gateways for the principal decision points and parallel paths.• Initial swimlanes (actors/roles) where extractable from the structured RLCO data.• Linkage to the source RLCO record per Sec.No1.2.5.1.• Clear labelling as 'Draft' per Sec.No1.2.5.2 — 'System-generated draft workflows MUST be clearly labelled as drafts and MUST require human verification and approval before being treated as official outputs.'Final approved BPMN workflows (after human review/refinement under the Sec.No1.2.5.3 approval workflow) MUST achieve full Sec.No1.2.5.1 fidelity:• Process steps, actors and swimlanes, decision points, inputs/outputs.• Required documents and data objects.• Applicable fees and time bands.• Service channels and inter-agency handoffs.• Boundary events, message flows, and rework loops as needed for accurate process representation (per S#11/row 13).AI outputs are advisory per Sec.No1.6.9 (p.204); the BPR Module's approval workflow (Sec.No1.2.5.3) requires human verification and approval before BPMN artifacts are treated as official.

220	**Section 3.0.1 requires translation governance workflows within the CMS for review, approval, and versioning of translated RLCO content to prevent legal inconsistencies between Urdu and English versions.** **In the event of a legal inconsistency between the Urdu and English versions of a published RLCO, which** **language version is authoritative?**	Per Section VII Sec.No3.0.1 (p.222), the System MUST implement 'translation governance workflows within the CMS for review, approval, and versioning of translated RLCO content to prevent legal inconsistencies between Urdu and English versions.' The platform requirement establishes governance to PREVENT inconsistencies; substantive language-of-authority determination is governed by Pakistani law and the issuing authority's gazetting practice. Translation governance workflow within the CMS (Sec.No3.0.1): • Review: translated content is reviewed by an authorised translator/reviewer role. • Approval: translated versions are approved through a documented workflow (Draft → Under Review → Approved → Published states per Sec.No1.2.5.3). • Versioning: each language version is versioned with effective dates and historical retention per Sec.No1.3.3.5 (p.192). • Audit trail of all translation/approval events stored in the Immutable Audit Store (Sec.No1.1.4). Authoritative version determination: • For an RLCO whose underlying legal instrument is gazetted/notified in a specific language, that gazetted version remains the legally authoritative version under applicable law. • The PRR records both English and Urdu versions with explicit metadata identifying the source/original language of the underlying legal instrument. • Where a translation inconsistency is detected during the governance workflow, the discrepancy is escalated through the Module 9 RIS/AKTU Gating workflow for resolution prior to publication, ensuring the published versions are consistent. The detailed authoritative-version policy is confirmed during Inception in consultation with BOI/AKTU legal counsel.
221	**The search index must include an Urdu language analyzer. Is the Urdu analyzer expected to handle regional script variations, including Sindhi and Pashto text that may appear in provincial RLCO records,** **or is standard Urdu Nastaleeq the only required script variant?**	Per Section VII Sec.No3.0.1 (p.222), the System MUST provide full support for English and Urdu as the primary languages of the end-user community, including: full right-to-left (RTL) text rendering for Urdu using CSS 'direction: rtl' with bidirectional support compliant with WCAG 2.1; Unicode NFC normalisation for all Urdu text storage and retrieval; Jameel Noori Nastaleeq or an equivalent web-safe Urdu font as the standard rendering font; a Urdu language analyser integrated into the search index to support Urdu-language RLCO discovery; locale-aware rendering of dates, numbers and currency; and translation governance workflows within the CMS for review, approval and versioning of translated RLCO content. The mandatory minimum scope is English + Urdu (standard Nastaleeq). Where provincial RLCO records contain regional-language content (e.g. Sindhi, Pashto) requiring searchable indexing, the Supplier should propose an extension approach as part of the design — for example, an additional analyser, transliteration support, or content-translation governance. Such extension is beyond the Sec.No3.0.1 mandatory minimum; the specific approach will be agreed in the Agreed Project Plan during inception based on observed content needs.

222	**The RFP requires infrastructure-as-code for all environment configurations. Does the GoP data center orcloud environment support Terraform, Ansible, or equivalent IaC tooling, or are there constraints onwhich IaC tools can be used within government-managed infrastructure?**	Per Section VII Sec.No1.3.2.6 (Open Standards and Exit Strategy, p.190): 'infrastructure-as-code with documented deployment scripts' is mandatory; and per Sec.No1.3.5.1 (p.192–193), all four environments (Development, Staging/UAT, Production, Disaster Recovery) MUST be defined and managed via IaC.The GoP-provided environment is expected to support standard IaC tooling (e.g., Terraform, Ansible, Pulumi, Kubernetes manifests/Helm charts, ArgoCD/Flux for GitOps) — within the security and access constraints of the designated environment. Any environment-specific constraints (e.g., approved tooling list, security-cleared registries, network restrictions on tool-registry access) will be confirmed to the selected Supplier during Inception.Supplier responsibilities:• Propose the IaC tooling stack and patterns in the Architecture document under Sec.No2.6.2.• Deliver documented IaC scripts for all environments (DEV/UAT/PROD/DR) — versioned, tested, reproducible.• Ensure IaC scripts are GoP IP per Sec.NoG.3.1 (p.284) — full source-code transfer per Sec.NoG.3.3.• Support the operational-independence mandate — GoP MUST be able to recompile/deploy/operate the System independently per Sec.NoG.3.8 (p.284).• Integrate IaC with CI/CD pipeline (Sec.No3.4.1 and Standard Software Specifications) and configuration management to support automated environment provisioning and recovery.Where the designated environment imposes constraints not supportable by the Supplier's preferred IaC tooling, the Supplier proposes alternative tooling consistent with the constraints, documented in the Architecture document.
223	**The CI/CD pipeline must include automated schema validation and regression checks to prevent deployments that break published RLCO data or existing activity mappings. Is the schema validation expected to run against the full production RLCO dataset — which may eventually be tens of thousands of records — or against a representative test dataset maintained for this purpose?**	The CI/CD pipeline MUST include automated schema validation and regression checks to prevent deployments that break published RLCO data or existing activity mappings (per the Standard Software Specifications, Section VII Sec.No3.4 and the architecture mandates in Sec.No1.3 / Sec.No1.3.2.6 Open Standards and Exit Strategy, p.190). The validation approach is a Supplier design choice provided it reliably prevents breaking deployments. Expected design: • **Multi-tier validation strategy**: (a) Unit tests + schema validation against representative test datasets (canonical schema fixtures) within the build/test stage; (b) Integration tests against a representative production-like staging dataset in the UAT environment; (c) Pre-deployment migration dry-runs against a snapshot of the production database in a non-production environment to validate data-migration scripts against the full production data volumes (tens of thousands of records expected). • **Pre-deployment gates**: blue-green or canary deployment patterns with health checks and rollback triggers; schema compatibility checks (backward-compatible additive changes preferred; breaking schema changes require explicit migration and review). • **Production deployment validation**: post-deployment sanity checks on a sample of production records; alerting on schema-induced errors with automated rollback capability. • **Audit**: every deployment logged in the Immutable Audit Store per Sec.No1.1.4 (p.151) with deployment artifact reference, schema version, and validation report. The full production RLCO dataset does not need to be exercised in every CI run; staging dataset + production-snapshot dry-runs at deployment-gate are the standard approach. The Supplier documents the CI/CD design in the Architecture document under Sec.No2.6.2 and validates during OAT-6 (Operational Readiness, Sec.No4.3.6).

224	**For each of the priority government systems listed in section 1.3.6.2 — NADRA and government SSO platforms, government email and SMS gateways, the Pakistan Gazette and official publication systems, the e-Sign service under ETO 2002, and the BOI/National One Window — what is the current integration readiness status, specifically: does each system expose a documented, stable, and accessible API or integration interface today; is technical integration documentation, a sandbox or test environment, and sample credentials available to the Supplier from contract start; what protocol and authentication mechanism does each system use for inbound integration requests; are there per-transaction costs, rate limits, or licensing arrangements that the Supplier must account for in its architecture; and for provincial government systems and e-governance platforms listed as available where applicable, which specific provincial systems are currently in scope, which have accessible integration interfaces, and which should the Supplier treat as manual or deferred integrations for the purpose of the initial proposal — given that the answer to each of these points directly determines whether the Supplier designs a real-time automated integration, a scheduled batch exchange, a manual fallback workflow, or scopes the integration as a post-go-live activity, with material consequences for the architecture, timeline, and cost of the solution?**	Per Section VII Sec.No1.3.6.2 (p.194), the System MUST be designed and delivered to integrate with the following priority government systems: NADRA and government SSO platforms (identity verification/authentication); government email and SMS gateways (notification delivery); Pakistan Gazette and official publication systems (Gazette reference capture and linkage); e-Sign service for digital signatures under ETO 2002; BOI/National One Window (regulatory business facilitation); and Provincial government systems and e-governance platforms where available. An open, read-only API layer for published RLCO data MUST be provided for future integration with additional government portals, including the Pakistan Business Portal (PBP). Per Sec.No1.3.6.3 (p.194), integration modes supported: secure REST APIs for real-time synchronous queries; scheduled ETL pipelines for batch data exchange; CSV/Excel import staging with validation; webhook and event triggers for asynchronous notifications where supported. The current readiness status — documented APIs, sandbox/test environments, sample credentials, transaction costs, rate limits, licensing arrangements — for each integration target will be confirmed to the selected Supplier during the inception phase. The Supplier is responsible for the technical integration with Purchaser facilitation of access to the relevant agencies and integration documents. Provincial systems vary in API readiness; where APIs are unavailable for a jurisdiction, the Supplier proposes scheduled batch exchange, CSV import or manual fallback as agreed in the Agreed Project Plan.

225	**The RFP specifies that the MVP comprising Registry Core, Agency Provisioning, fullRLCO submission loop, bulk import, search indexing, and three live environments(DEV/UAT/PROD) with encryption and MFA must be delivered within ten (10) weeksof Contract Effective Date. Given that Week 2 also requires an accepted Architecture& Design Pack, the effective build window is approximately eight weeks. Could thePurchaser confirm whether the MVP scope in Section 4.2.1 is fixed and exhaustive, orwhether proposers may propose a phased MVP scope with a risk-mitigated deliverysequence, subject to BOI/AKTU written approval at inception?**	The minimum MVP scope is defined in Section VII Sec.No1.3.5.5 (p.193) verbatim as 'the minimum system capability required to enable early RLCO data entry by DFPs and early review by BOI/AKTU', to be delivered within ten (10) weeks of the Contract Effective Date. The detailed MVP capability set is reflected in SIT-1 Subsystem 1 — 'PRR MVP Core for Early Data Entry' (Section VII SIT-1, p.247). The MVP Pre-Commissioning Test acceptance criteria are set out in Section VII Sec.No4.2.1 (p.229–230).The MVP scope and Week-10 delivery date are binding minima. However, Sec.No1.3.5.5 explicitly provides for Proposer-proposed phasing within that envelope: 'The Supplier MUST submit, as part of its Technical Proposal, a Sprint Plan covering the full project timeline and clearly marking MVP scope, Phase 1, and Phase 2 deliverables. The Purchaser reserves the right to conduct user acceptance testing of each sprint deliverable and to provide structured feedback that the Supplier MUST incorporate into the Product Backlog.'Proposers may therefore propose a Sprint Plan with a risk-mitigated delivery sequence WITHIN the binding MVP scope and the Week-10 MVP delivery date, subject to BOI/AKTU written approval at inception. The full mandatory module set is integrated and accepted at Milestone M11 (Integrated System Acceptance & Operational Go-Live) at Week 40 (Section IX SCC GCC 12.1, p.386).
226	**The RFP requires that the Supplier submit a Sprint Plan as part of the Technical Proposal, clearly marking MVP scope, Phase 1, and Phase 2 deliverables. Could the Purchaser confirm the mechanism and turnaround time for BOI/AKTU review and acceptance of sprint deliverables? Specifically, if BOI/AKTU review cycles extend beyond five business days per milestone, will the corresponding downstream milestone dates be adjusted by the same duration?**	Per Section VII Sec.No1.3.5.5 (p.193), the Supplier submits a Sprint Plan as part of the Technical Proposal, marking MVP scope, Phase 1 and Phase 2 deliverables. Section VII Sec.No1.3.5.5 also provides: 'The Purchaser reserves the right to conduct user acceptance testing of each sprint deliverable and to provide structured feedback that the Supplier MUST incorporate into the Product Backlog.' The detailed BOI/AKTU review/acceptance cycle for each sprint deliverable is set in the Agreed Project Plan during Inception (Sec.No2.6.2), with target review timelines defined per deliverable type. The Purchaser will endeavour to provide review/feedback or written acceptance within the target review window. Where BOI/AKTU review of a sprint deliverable extends beyond the agreed turnaround and the downstream milestone date is impacted by that delay, the Supplier may seek schedule relief under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), through the project governance and notification process under GCC 18.2 and GCC 19. Where the relief is granted, the affected downstream milestone date is adjusted correspondingly and Liquidated Damages under GCC 28.2 do not accrue for the granted relief period. There is no automatic deemed-acceptance (see S#251 / row 251).

227	**The Implementation Schedule requires ten mandatory modules to be fully operational and integrated-system-tested by Week 38, with Final Acceptance at Week 40. Could the Purchaser clarify whether the liquidated damages regime applies where milestone delays are attributable to factors within the Purchaser's control such as delayed government infrastructure provisioning, delayed stakeholder access, or delayed acceptance of Supplier deliverables?**	Liquidated Damages under GCC Clause 28.2 (Section VIII, p.342) and the SCC at Section IX GCC 28.2 (p.393) are payable only for delay in achieving Operational Acceptance that is within the Supplier's control. Where milestone delays are attributable to factors within the Purchaser's control — including delayed government infrastructure provisioning per Sec.No3.0.2, delayed stakeholder access for testing/workshops, delayed Purchaser acceptance of Supplier deliverables, or delayed counterparty integration readiness per Sec.No1.3.6.2 — the Supplier is entitled to seek schedule relief under Section VIII GCC Clause 40 (Extension of Time for Achieving Operational Acceptance, p.364). The Supplier MUST notify the cause and duration of the delay per GCC 18.2 and GCC 19, supported by documentary evidence and impact analysis on the Implementation Schedule. The Purchaser considers such EoT requests through the formal change-management process. Where an EoT is granted, the scheduled Operational Acceptance date adjusts correspondingly and LDs do not accrue for the granted relief period. The aggregate LD cap remains 10% of the relevant Activity's Contract Price excluding Recurrent Costs (Section IX SCC GCC 28.3, p.394), applied separately per Activity.
228	**Can the Purchaser clarify which MVP requirements must be production-grade at Week 10, and which may be delivered as controlled early-release functionality? In particular, should cybersecurity hardening, production-scale performance testing, full integration testing, public portal functionality, AI Assist, Gazette linkage, esignature, and provincial onboarding be excluded from MVP acceptance unless expressly listed?**	At MVP (Week 10, Milestone M2 per Section IX SCC GCC 12.1, p.385), the binding MVP functionality MUST be production-grade. Section VII Sec.No4.2.1 (p.229–230) — the MVP Pre-Commissioning Test for Subsystem 1 — requires verification of: • Template manager including draft-to-pilot-to-approved template version transitions and historical version retention • DFP RLCO submission loop (draft → submit → return → resubmit → validate → publish) • Mandatory-field validation blocking incomplete submissions per Table 1 (BIM-3 ANNEX VII-A) • Mandatory legal basis reference validation • Full versioning (create, edit with change reason, supersede, archive) with complete history • Government-controlled hosting with DEV, UAT and PROD environments operational, with documented deployment scripts, backups, and DR approach • Database encryption at rest, TLS in transit, and admin MFA all active Items NOT in the MVP scope are delivered against later milestones — full module set integration acceptance at M11 (Week 40); public portal & consultation system at M5 (Week 20); BPR/BPMN module at M6 (Week 22); AI Assist Module at M10 (Week 28); RIS/AKTU Gatekeeping at M9 (Week 28); full DR drills annually per Sec.No1.3.5.2. PSS compliance is a mandatory pre-condition for the Operational Acceptance Certificate at M11 (Sec.No1.3.4.3, p.191), not at MVP. The Sprint Plan submitted with the Technical Proposal (Sec.No1.3.5.5) elaborates the precise split of capabilities by sprint within these gates; this is finalised in the Agreed Project Plan during Inception.

229	**To maintain implementation continuity and milestone predictability, could the Purchaser confirm whether a deemed acceptance mechanism will apply where submitted deliverables remain unreviewed beyond the prescribed review period without written rejection or consolidated feedback?**	There is no automatic deemed-acceptance mechanism in the GCC/SCC. Formal Purchaser acceptance of each milestone deliverable is required before the corresponding payment is triggered (Section VIII GCC Clauses 25–27, p.337–340; Payment Release Schedule in Section IX SCC GCC 12.1, p.385–388).To prevent indefinite delay in acceptance, the framework includes:• Agreed Project Plan and governance structure (Section VII Sec.No2.6.2) — set clear review/sign-off timeframes by deliverable type during Inception.• Change Request Turnaround (Section VIII GCC 39.6, p.363–364) — BOI approves or rejects Change Requests within ten (10) business days of submission; Supplier provides impact assessment within five (5) business days.• Extension of Time (Section VIII GCC Clause 40, p.364) — where Purchaser-side review delay is beyond the Supplier's control and impacts the schedule, the Supplier may seek schedule relief through the project governance and notification process under GCC 18.2 and GCC 19.• Interest on payment delay (Section VIII GCC 12.3, p.313–314) — where Purchaser is delayed in payment beyond the period specified in the SCC, interest is payable.• Settlement of Disputes (Section VIII GCC Clause 43, p.380) — Adjudicator (SCC GCC 43.1.4: Centre for International Investment and Commercial Arbitration of Pakistan, p.395) and ICC arbitration for non-Pakistan Suppliers.The Purchaser endeavours to provide acceptance or consolidated feedback within reasonable timeframes per the Agreed Project Plan.
230	**Module 10 (AI Assist) requires self-hosted AI processing with no dependency on external model APIs unless explicitly approved in writing. The module must be operational by Week 28. Could the Purchaser confirm: (a) whether governmentcontrolled hosting infrastructure with sufficient GPU/compute capacity for LLM inference will be provisioned and accessible to the Supplier from Contract Effective Date; and (b) if not, whether the Supplier is permitted to provision and operate temporary approved compute infrastructure at its own discretion pending government infrastructure readiness, with costs recoverable as a variation?**	(a) The GoP-provided infrastructure (Section VII Sec.No3.0.2, p.222) is the designated environment for hosting the AI Assist Module (Module 10), including required GPU/compute capacity for self-hosted LLM/NLU workloads. The Supplier MUST document the required GPU sizing, architecture and auto-scaling thresholds in the Deployment Architecture document delivered under Sec.No2.6.2 early in the Contract, enabling the Purchaser to plan and provision the required capacity. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) state verbatim: 'Not Applicable — No hardware is procured under this Contract.' The AI Assist Module is required to be operational at Milestone M10 (Subsystem 9 — AI Assist modules operational) at Week 28 per Section IX SCC GCC 12.1 (p.386). (b) The Supplier is not authorised to provision and operate temporary external compute infrastructure outside GoP-controlled hosting at its own discretion; AI processing MUST occur exclusively within government-controlled hosting (Sec.No1.2.10.1, p.175; Sec.No1.6.9, p.204). Where Purchaser-side delay in GPU/compute provisioning is beyond the Supplier's control and impacts the milestone, schedule relief is available under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364). Any deviation from the GoP-hosted model requires explicit prior written approval by the Purchaser.

231	**The AI Assist Module requires consultation sentiment analysis, NLU classification, regulatory burden scoring, and workflow generation, all operating on governmenthosted infrastructure. Could the Purchaser share indicative parameters around the expected volume of RLCO records, consultation submissions, and concurrent users that the AI module will be expected to process at Week 28 operationalization? This is required to accurately size the compute and storage infrastructure in the Technical Proposal.**	Indicative parameters for the AI Assist Module workloads (Module 10) — consultation sentiment analysis, NLU classification, regulatory burden scoring, workflow generation — will be refined and confirmed during Inception, taking account of: the 100 priority economic activities across five sectors (Section VII Sec.No1.2.11.4, p.178); the mandatory concurrency targets of Section VII Table 1.5-A (p.201) — 2,000 concurrent DFP/AKTU sessions, ≥ 5,000 concurrent public users normal, ≥ 25,000 peak consultation; the public consultation window minima (Sec.No4.2.2 — minimum 30 days); and the RLCO inventory expected from the mapping waves across the six jurisdictions. For sizing purposes at proposal stage, the Supplier should propose GPU/compute architecture for the AI Assist Module based on the mandatory performance/scale targets in Section VII Sec.No1.5 (p.197–201) and Table 1.5-A. The Deployment Architecture document delivered under Sec.No2.6.2 will document the proposed GPU/compute, memory and storage architecture to enable Purchaser-side provisioning of GoP-provided infrastructure (Sec.No3.0.2; Sec.No3.1–Sec.No3.3 — 'No hardware is procured under this Contract').
232	**Given that the AI Assist Module's prompt templates, scoring logic, and feature engineering are designated as intellectual property of the Government of Pakistan, could the Purchaser clarify the contractual position on model recalibration during the AMC period specifically, whether the Supplier retains the right to use accumulated PRR RLCO data for improving model performance, or whether each recalibration cycle requires a separate written authorization? The answer materially affects AMC pricing.**	All AI workflows, scoring logic, feature engineering, prompt templates and orchestration logic developed or customised under this Contract are the intellectual property of the Government of Pakistan and vest with the Purchaser (Section VII Sec.NoG.3.5, p.284 and Sec.No1.6.9, p.204). All PRR data — including regulatory drafts, RIS submissions, consultation comments, audit logs, AI-generated artefacts, metadata and monitoring data — remains the exclusive property of the Government of Pakistan; the Supplier acts solely as Data Processor (Sec.NoG.3.2 and Sec.NoG.4.1, p.284–285). Model recalibration during the Warranty Period and the AMC Period is a Supplier obligation included in 'AI module maintenance' under the Warranty Period scope (SCC GCC 29.1, p.394) and in the mandatory Y1–Y3 AMC scope (Section VII SIT-2 Notes, p.251–252). All recalibration artefacts — re-trained model parameters, prompt updates, scoring rule updates, evaluation logs — are GoP IP and MUST be transferred with documentation. Each routine recalibration cycle does not require separate written authorisation provided it operates exclusively on PRR data within GoP-controlled hosting per Sec.No1.2.10.1 (p.175) and Sec.No1.6.9 (p.204). Transmission of PRR data to external AI platforms, model APIs or cloud-based AI services for any recalibration purpose requires explicit prior written approval by the Purchaser (Sec.No1.6.9). The Supplier MUST not re-use accumulated PRR data for any purpose outside the Contract scope.

233	**Can the Purchaser confirm whether the AI Assist Module will be evaluated as an advisory decision-support tool only, with all final clearance, publication, enforcement, and regulatory decisions remaining subject to human review and approval? This clarification is important because the RFP states that AI output must remain advisory and must not operate as final decision authority.**	CONFIRMED. The AI Assist Module is an advisory decision-support tool only. All final clearance, publication, enforcement and regulatory decisions remain subject to human review and approval by the authorised role through the configured workflow (Module 9 RIS/AKTU Gating per Sec.No1.2.9; departmental sign-off per Sec.No1.2.11.2; final approval through BOI/AKTU).This is anchored verbatim in Section VII Sec.No1.6.9 (p.204): AI outputs are advisory and subject to human review with documented resolution decision. AI MUST NOT autonomously approve, publish or take enforcement action.Specific advisory-only mechanisms:• Sec.No1.2.10.6 (AI Feature 5 — Similarity and Conflict Detection): flagged similarities/conflicts MUST be surfaced as advisory flags requiring human review and a documented resolution decision.• Sec.No1.6.9: AI outputs traceable to source data, model version, prompt template version, and processing parameters; logs retained in the Immutable Audit Store; provenance and reproducibility required (see S#232/row 235).• Module 9 RIS/AKTU Gating (Sec.No1.2.9): central gating workflow where AKTU exercises final approval before publication; AI outputs are inputs to this human review, not autonomous decisions.• Sec.NoG.4.1 (p.285): Government of Pakistan is the Data Controller; the Supplier is Data Processor; substantive regulatory authority remains with BOI/AKTU and the relevant line departments.• Departmental sign-off SOP (Sec.No1.2.11.2): formal written acceptance by the participating department / authorised signatory for each RLCO inventory.AI is never the validating authority for regulatory content (see S#201/row 204, S#207/row 210, S#270/row 270).
234	**The Al Assist Module introduces capabilities including semantic similarity, regulatory conflict detection, workflow generation, and consultation analytics. Could the Purchaser confirm whether a formal Al governance framework, model-risk management policy, and Al explainability standard already exist for the PRR programme, or whether the Supplier is expected to propose and operationalize such governance controls as part of the contract scope?**	A formal AI governance framework is REQUIRED by Section VII Sec.No1.2.10.1 (p.175) and Sec.No1.6.9 (p.204), and MUST be implemented and documented by the Supplier as part of the AI Assist Module delivery. The mandatory requirements include: • Localised processing: AI Assist Module operates exclusively within government-controlled hosting; no transmission of PRR data to external AI platforms, model APIs or cloud-based AI services without explicit prior written Purchaser approval (Sec.No1.2.10.1, Sec.No1.6.9). • Human-in-the-loop: all AI outputs are advisory; human review and a documented resolution decision are required before any AI-generated output is acted upon or progressed (Sec.No1.6.9; Sec.No1.2.10.6 for Similarity and Conflict Detection). • Output provenance and reproducibility logging: AI outputs MUST be traceable to source data, model version, prompt template version, and processing parameters; logs retained in the Immutable Audit Store. • Model version control: model and prompt versioning with rollback capability. • Bias mitigation and quality monitoring: ongoing monitoring of AI output quality with documented evaluation procedures. • Data Controller / Data Processor structure: Government of Pakistan is the Data Controller; the Supplier acts solely as Data Processor (Section VII Sec.NoG.4.1, p.285). The Supplier MUST propose and document the AI governance framework, model-risk management policy and explainability standard as part of the AI Assist Module delivery, integrated with the System's audit and immutable-record capabilities.

235	**The RFP mandates integration with NADRA, Government SSO, Pakistan Gazette, eSign (ETO 2002), and provincial e-governance platforms. Could the Purchaser confirm: (a) the current readiness status of sandbox/test APIs for each of these systems; and (b) whether delays in integration caused by third-party government systems including unavailability of APIs, delayed MoU execution, or system downtime will constitute excusable delays with corresponding milestone adjustments?**	(a) Per Section VII Sec.No1.3.6.2 (p.194), the mandated priority integrations are: NADRA and government SSO platforms; government email/SMS gateways; Pakistan Gazette and official publication systems; e-Sign service under ETO 2002; BOI/National One Window; and Provincial e-governance platforms where available. The current sandbox/test-API readiness for each integration target will be confirmed during the inception phase. The Supplier is responsible for the technical integration with Purchaser facilitation of access to the relevant agencies and integration documents. (b) Delays caused by third-party government systems beyond the Supplier's control — including unavailability of integration APIs, delayed MoU execution between agencies, or extended downtime of a counterparty system — qualify for relief under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364). The Supplier MUST notify the cause and duration of the delay in accordance with GCC 18.2 and GCC 19, with documentary evidence and impact analysis on the Implementation Schedule. The Purchaser will consider such EoT requests through the formal change-management process. Where the delay constitutes Force Majeure under GCC Clause 38 (Section VIII, p.358), the corresponding Force Majeure provisions apply. Operational Acceptance milestone adjustments and Liquidated Damages calculations follow from a granted EoT.
236	**The TA Workstream requires RLCO mapping across six jurisdictions, involving departmental workshops and data collection from regulatory focal points (DFPs) at federal and provincial levels. Could the Purchaser confirm the level of institutional commitment already secured from provincial governments specifically whether formal directives have been issued to provincial departments to cooperate with the Supplier's mapping activities, and what escalation mechanism exists if a provincial department declines or significantly delays its participation?**	BOI/AKTU is the central coordinating authority for the PRR programme under the Asaan Karobar Act, 2025 (Section VII Sec.No1.1.5, p.151), which mandates the establishment of the PRR as a national digital registry and the standardisation of regulatory information across all federal and provincial jurisdictions. The Act provides the legal basis for jurisdiction-wide cooperation.BOI/AKTU facilitates institutional engagement and data collection through:• Formal engagement letters / directives to provincial departments to nominate Departmental Focal Persons (DFPs) and cooperate with mapping activities (Section VII Sec.No1.2.11.1, p.177–178).• Structured stakeholder engagement sessions across all jurisdictions — physically and virtually — with a minimum of one stakeholder session per jurisdiction per mapping wave (Sec.No1.2.11.3, p.178).• Departmental sign-off SOPs for closure (Sec.No1.2.11.2).The level of formal facilitation, institutional commitment status by province, and escalation paths will be confirmed to the selected Supplier during Inception. Where a department's delay or non-cooperation impacts a Supplier milestone and is beyond the Supplier's control, schedule relief is available under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364).

237	**Where a priority government integration system is not technically ready, lacks API documentation, lacks sandbox access, or is unavailable for testing, will the Supplier be considered compliant if it delivers documented integration specifications, mock services, adapters, or interim import/export mechanisms until the relevant government system is ready?**	Where a priority government integration target (Section VII Sec.No1.3.6.2, p.194) is not technically ready — lacks API documentation, lacks sandbox access, or is unavailable for testing — through no fault of the Supplier, the Supplier is considered compliant for the relevant milestone on delivering: • A documented integration design (OpenAPI specification, data flow, sequencing, error handling, retry logic, security model) per Sec.No1.3.6.1 (p.194). • A tested adapter/integration layer ready to connect via configuration when the counterparty system becomes available. • Interim data exchange mechanisms (e.g., CSV/Excel import staging per Sec.No1.3.6.3, scheduled ETL pipelines, manual upload workflow) as a fallback where the integration mode is mandated but the live API is unavailable. • Mock services within the PRR test environment that simulate the counterparty API for system integration testing. This third-party unavailability is a delay beyond the Supplier's control and is addressed through Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), with notification under GCC 18.2 and GCC 19, supported by documentary evidence. Where the unavailability constitutes Force Majeure per GCC Clause 38 (p.358), the Force Majeure provisions apply. Once the counterparty system becomes available post-go-live, the Supplier connects the adapter under the Warranty regime (during the 2-year Warranty Period, SCC GCC 29.1, p.394) or the AMC regime (Y1–Y3 mandatory, per SIT-2 Notes) at no additional cost provided no new functionality is required.
238	**Could the Purchaser provide indicative estimates regarding the current availability and digital maturity of RLCO records across participating jurisdictions including the approximate proportion currently available in structured digital formats versus scanned documents, PDFs, or manual records?**	Indicative estimates of RLCO availability and digital maturity will be confirmed during the Inception phase. Per Section VII Sec.No2.5.1 (p.215), the Supplier MUST conduct a data quality assessment of all source data prior to ingestion, documenting completeness gaps, structural mismatches, and records requiring manual validation. The volume, type, structure, and format of existing data available will be confirmed at that time. Existing data sources span: prior mapping outputs from past initiatives, departmental RLCO lists and registers, regulatory scans, legacy database exports, scanned PDF documents and manual records. Maturity is expected to vary materially across jurisdictions and across departments within a jurisdiction. Per Sec.No2.5.2 (p.215), the Supplier MUST provide a bulk import facility supporting Excel and CSV upload with column mapping to Table 1 (ANNEX VII-A) fields, validation rules at import, a detailed import error report, and a staging area review before records are confirmed. AI-assisted extraction from documents or portals MAY be used to accelerate data structuring, BUT all AI-extracted outputs MUST be placed in a Human Verification Queue and MUST NOT be promoted to Validated status without human review and approval. Proposers should size their TA workstream effort with appropriate contingency for the data-quality variability.

239	**The RFP specifies AS-IS and To-Be documentation of 100 priority economic activities across five ISIC sectors. Could the Purchaser clarify whether this figure represents a firm ceiling i.e., the Supplier will not be required to capture additional activities beyond 100 or whether BOI/AKTU retains discretion to expand the mapping scope during contract execution? If expansion is possible, could the Purchaser confirm the contractual mechanism for pricing and authorizing such additional scope?**	The figure of one hundred (100) priority economic activities across five ISIC Rev.4 sectors is the defined scope of this engagement for AS-IS and TO-BE documentation per Section VII Sec.No1.2.11.4 (p.178), and underpins the TA workstream Implementation Schedule (Activity 2, PM-1 to PM-10 in Section IX SCC GCC 12.1).The specific 100 activities will be selected and notified through the TA deliverable 'ISIC Rev.4 Activity Selection Note' (Table 1.2.11-A row TA-D6; SIT-1 row TA-02), produced by the Supplier in consultation with BOI/AKTU during the early TA phase (per the Implementation Schedule).Expansion beyond the 100 activities is not an open-ended Supplier obligation. Where BOI/AKTU determines that additional activities should be brought into scope during contract execution, this is managed through Section VIII GCC Clause 39 — Changes to the System (p.362) read with Section IX SCC GCC 39.2.1 (p.393): changes are classified as Minor (no cost/schedule impact) or Major (subject to detailed review/approval). All changes follow a documented Change Order procedure with Change Order Forms in Section X (p.425–432). The PRR platform itself MUST remain scalable to accommodate additional activities and RLCOs over time without architectural modification (Sec.No1.1.5).
240	**Could the Purchaser clarify if the 100 economic activities have already been identified or will be identified in the future by the BOI? Is the Supplier expected to co-develop the criteria for the shortlisting of the 100 economic activities?**	The 100 priority economic activities have NOT been pre-finalised in the RFP. They are identified and notified through the Supplier-produced TA deliverable 'ISIC Rev.4 Activity Selection Note' (Table 1.2.11-A row TA-D6 / SIT-1 row TA-02, p.179–180, p.247) produced in CONSULTATION with BOI/AKTU during the early TA phase. The Supplier supports BOI/AKTU in the criteria development and methodological prioritisation, while BOI/AKTU exercises final approval. Per Section VII Sec.No1.2.11.4 (p.178), the AS-IS workflow documentation MUST be produced for a minimum of one hundred (100) priority economic activities across five (5) ISIC Rev.4 sectors. The selection is informed by: • Asaan Karobar Act 2025 priorities (Sec.No1.1.5). • PRMI Strategy framework. • Existing regulatory inventory and prior mapping work. • Stakeholder consultations with federal and provincial regulators across the six jurisdictions. • ISIC Rev.4 sector groupings. • Cross-jurisdictional balance to ensure equitable jurisdiction coverage. The Activity Selection Note is approved by BOI/AKTU and forms part of the scope baseline (see S#143/row 146). The Supplier supports BOI/AKTU through methodology, framework, evidence base, and consultation facilitation — but does NOT unilaterally select. See also S#5/row 7, S#41/row 44, S#57/row 60.
241	**The RFP requires the Supplier to provide a three-year AMC quote as a mandatory line item, covering AI module recalibration, security patches, helpdesk SLA, and minor enhancements. Could the Purchaser clarify the definition of "minor enhancements" specifically, whether this refers to configuration changes within existing module scope, or whether it could include new functional requirements arising from legislative changes to the Asaan**	The scope of the mandatory Y1–Y3 AMC is defined by Section VII Sec.No5.2 (Technical Support and Post-Deployment Engagement, p.237–238) and the AMC line items in SIT-2 (p.252). AMC scope covers: • Defect repair within the SLA regime of Table 5.1-A (p.237) • Security patches and routine vulnerability remediation per Sec.No1.6.6 (p.203) • Periodic AI model recalibration and prompt updates (Sec.No1.2.10) — minor recalibration cycles operating on PRR data within GoP-controlled hosting • Helpdesk SLA and L1/L2/L3 support per Sec.No5.2 (p.237) • Minor configuration adjustments — including parameter tuning, vocabulary updates, dashboard configuration adjustments, workflow timing adjustments, and bug-fix-level changes within existing module scope and capacity

	Karobar Act or PRMI Strategy? The distinction materially affects AMC scope and pricing.	• Routine software/licence renewals for delivered components. 'Minor enhancements' under AMC means small configuration and functional adjustments that operate WITHIN the existing scope and capacity of the delivered modules — they do NOT include new modules, new business functions, or new functional requirements arising from legislative changes (e.g., amendments to the Asaan Karobar Act, the PRMI Strategy, or other governing legislation). New functional requirements, new modules, or major scope additions are governed by Section VIII GCC Clause 39 — Changes to the System (p.362) read with SCC GCC 39.5 (15% Change Request budget ceiling, p.364). The distinction is documented in the Agreed Project Plan (Sec.No2.6.2) during Inception. Y4–Y5 AMC is optional at the Purchaser's discretion (SIT-2 column 'Year 4+ (Yn)', p.252; Sec.No5.2.3, p.238).
242	**The RFP specifies that the PRR must support government on-premises and government-controlled cloud hosting. Could the Purchaser confirm which specific hosting environment has been designated, what the provisioning timeline is postaward, and whether any infrastructure procurement including servers, storage, networking, and GPU compute for the AI module falls within the Supplier's scope of supply? If so, could the Purchaser provide indicative specifications to ensure proposals are comparably priced?**	The PRR is hosted on GoP-provided infrastructure: a national government data centre and/or a GoP-controlled/approved cloud environment, Tier-3 or higher, within Pakistan, multi-zone across at least two independent availability zones (Section VII Sec.No3.0.2, p.222; Sec.No1.1.1.7, p.149).The specific designated hosting environment and provisioning timeline will be confirmed to the selected Supplier post-award. No infrastructure procurement — servers, storage, networking, GPU compute for the AI Assist Module, or HSM hardware — falls within the Supplier's scope of supply. Section VII Sec.No3.1, Sec.No3.2 and Sec.No3.3 (p.223) state verbatim: 'Not Applicable — No hardware is procured under this Contract.'The Supplier MUST document the required infrastructure sizing and architecture in the Deployment Architecture document delivered under Sec.No2.6.2 — including compute, storage, network, GPU (for the AI Module) and HSM (for the KMS) specifications and auto-scaling thresholds. This documentation allows the Purchaser to provision the platform appropriately. Indicative platform specifications will be developed in collaboration with the selected Supplier during the inception phase.
243	**The RFP refers to a cumulative change budget ceiling to be agreed at contract award. Could the Purchaser clarify the methodology for distinguishing normal backlog refinement from formal scope change, especially where new requirements arise from legislative changes, newly identified agency workflows, additional provincial requirements, or new government digital standards?**	Distinguishing backlog refinement from formal scope change is governed by the approved scope baseline and the Change Control regime: • Scope baseline: The approved AS-IS and TO-BE workflow artefacts and supporting requirements establish the scope baseline (Section VII Sec.No1.2.5.3 Approval States and Sec.No1.2.11.2 Departmental Sign-Off, p.178). Clarifications, elaborations or implementation details consistent with the baseline are backlog refinement and are managed within the standard delivery process — they do not consume the GCC 39.5 change budget. • Formal scope change: New functionality or requirements falling outside the baseline (e.g., newly enacted legislation requiring new fields/workflows; newly identified agency workflows beyond the agreed 100 priority activities; additional provincial-specific requirements not anticipated in inception; new mandatory government digital standards) constitute changes governed by Section VIII GCC Clause 39 (p.362) read with Section IX SCC GCC 39.2.1 (p.393). • Classification (SCC GCC 39.2.1): Minor (no cost/schedule impact) or Major (subject to detailed review/approval where applicable). All changes follow a documented change-control procedure with Change Order Forms in Section X (p.425–432). • Turnaround (Section VIII GCC 39.6, p.363–364): Supplier provides written impact assessment (scope, cost, timeline) within five (5) business days of Change Request submission; BOI approves or rejects within ten (10) business days; approved CRs incorporated into the next available sprint; rejected CRs recorded in the Change Log with reasons.

		• Budget ceiling (Section VIII GCC 39.5, p.364): Up to 15% of total contract value may be allocated for Change Requests raised after MVP go-live, subject to BOI written approval for each change and World Bank no-objection for cumulative changes exceeding 10% of contract value. Changes beyond 15% require a contract amendment.
244	**Could the Purchaser clarify the mandatory multilingual requirements applicable to the PRR platform specifically whether public search, RLCO metadata, Al-assisted search, consultation workflows, and generated workflow artifacts must support Urdu and/or regional languages at launch, or whether multilingual capability may be phased post-MVP?**	The mandatory multilingual scope at launch is set in Section VII Sec.No3.0.1 (p.222) — English and Urdu, as the primary languages of the end-user community. This covers all display technologies, web interfaces, and application software, including: • Public search and Public Registry Portal — English and Urdu rendering and search. • RLCO metadata and content — English and Urdu; translation governance workflows in the CMS for review, approval and versioning of translated RLCO content to prevent legal inconsistencies between Urdu and English versions. • Urdu language analyser integrated into the search index (so Urdu-language RLCO discovery is supported in search). • Locale-aware rendering of dates, numbers and currency for both English and Urdu display contexts. For consultation workflows and AI-generated workflow artifacts (BPMN, decision packs), Section VII Sec.No3.0.1 does not explicitly mandate multilingual outputs — the AI Assist Module (Sec.No1.2.10) operates as an advisory tool with human review and approval. Operational SOPs and key user-facing training materials MUST also be available in both English and Urdu per Sec.No2.4.4 (p.213). Multilingual capability is not phaseable post-MVP for the elements specified in Sec.No3.0.1 — those are mandatory at the relevant acceptance gate.
245	**The successful delivery of both workstreams platform development and RLCO mapping requires sustained, structured engagement with BOI and AKTU representatives throughout the contract period. Could the Purchaser confirm whether dedicated focal points will be formally designated within BOI and AKTU for the duration of the contract, including their seniority level, decision-making authority, and minimum committed availability, in person-days per month, to support the Supplier's activities?**	BOI/AKTU institutional facilitation through the contract period is provided through the project governance and AKTU institutional mechanisms established under the Asaan Karobar Act 2025 (Section VII Sec.No1.1.5, p.151). Specifically:• Project governance structure with BOI as the central coordinating authority (Section VII Sec.No1.4 Systems Administration and Management; Sec.No2.6.2 Agreed Project Plan).• Departmental Focal Persons (DFPs) — each participating institution MUST be assigned a DFP as the data steward responsible for accuracy, timeliness, and verification of supporting legal documents (Sec.No1.3.3.6, p.193).• Stakeholder engagement support per Sec.No1.2.11.3 (p.178) — BOI/AKTU facilitates structured engagement sessions across all six jurisdictions, including formal engagement letters and DFP nominations.The specific designated BOI/AKTU focal points, their seniority and minimum committed availability will be confirmed to the selected Supplier post-award. Where Purchaser-side stakeholder unavailability impacts the project schedule, the Supplier is entitled to schedule relief under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), with notification under GCC 18.2 and GCC 19. The Supplier MUST propose and cost its own engagement model — including its proposed governance interface, jurisdiction-wise coordination approach, and reporting cadence — as part of the Technical Proposal.

246	**Module 9 (RIS/AKTU Gating) requires integration with AKTU's regulatory quality gate process, including public consultation portal functionality and AKTU screening workflows. Could the Purchaser confirm the current state of AKTU's internal gating process specifically, whether formal AKTU screening criteria, regulatory impact thresholds, and consultation protocols have already been documented and approved, or whether the Supplier will be required to co-develop these as part of the contract scope? If co-development is required, could the Purchaser clarify how this additional advisory scope will be reflected in the contract?**	Module 9 — RIS/AKTU Gating Module (Section VII Sec.No1.2.9) is a mandatory PRR functionality. It implements the configurable RIS submission, technical and enhanced review gates, consultation routing, Registry ID issuance, and monitoring workflows (training module reference Sec.No2.4.2(i), p.213). The platform requirements include: • Configurable RIS form builder with completeness validation. • Technical review gate and enhanced review gate (two-stage AKTU gating). • Consultation routing — public-consultation integration with Module 8 Public Portal and CMS. • Registry ID issuance upon AKTU approval. • Continuous monitoring of approved RLCOs. The current state of AKTU's internal regulatory quality-gate process, formal screening criteria, regulatory impact thresholds and consultation protocols will be confirmed to the selected Supplier during Inception. The Supplier supports BOI/AKTU in operationalising the gating process through: • Configuring Module 9 to reflect AKTU's screening criteria and impact thresholds. • TA capacity-building under Sec.No2.4.5–Sec.No2.4.8 (p.215) — including stakeholder engagement and reform facilitation training (Sec.No2.4.8) covering RIS and regulatory impact assessment process. • TA workplan deliverables (Table 1.2.11-A) — including TA Capacity Building Toolkit and stakeholder engagement workshops. Co-development of AKTU process documents that fall outside the configured Module 9 platform scope and outside the TA workstream scope is treated as new scope under Section VIII GCC Clause 39 (Change Control, p.362) with SCC GCC 39.5 budget ceiling (p.364).
247	**The contract requires formal acceptance of each deliverable by BOI/AKTU before the corresponding milestone payment is triggered. Could the Purchaser specify the maximum number of business days within which BOI/AKTU will review and either accept or provide written feedback on each submitted deliverable and confirm whether, in the absence of a written response within that period, the deliverable will be deemed accepted?**	The Contract requires formal Purchaser acceptance of each deliverable/milestone before the corresponding payment is triggered (Section VIII GCC Clauses 25–27 — Inspections and Tests; Installation; Commissioning and Operational Acceptance) read with the Payment Release Schedule in Section IX SCC GCC 12.1 (p.385–388). The maximum review/sign-off period for each deliverable type will be set in the Agreed Project Plan delivered under Section VII Sec.No2.6.2. The Purchaser will endeavour to provide acceptance or written feedback within a reasonable period — typically within fifteen (15) business days for routine deliverables and longer for complex milestone deliverables involving formal testing under Sec.No4.2 (Pre-commissioning Tests) and Sec.No4.3 (Operational Acceptance Tests). There is no automatic deemed-acceptance provision in the GCC/SCC. Where Purchaser-side delay in providing acceptance is beyond the Supplier's control, the Supplier may invoke GCC Clause 40 (Extension of Time for Achieving Operational Acceptance, Section VIII, p.364) through the project governance and notification process under GCC 18.2 and GCC 19. Operational Acceptance procedures are set out in GCC Clauses 26–27.

248	**Can the Purchaser confirm who has final authority to validate the legal basis, completeness, and publication readiness of each RLCO record: the Supplier, BOI/AKTU, the relevant line department, provincial authorities, or a joint validation committee? This should be clarified because software acceptance may otherwise become dependent on legal and data-quality determinations outside the Supplier's control.**	Final authority to validate the legal basis, completeness, and publication readiness of each RLCO record rests with BOI/AKTU and the relevant line department/provincial authority through the configured gating workflow. The Supplier provides the platform capability and TA mapping support but does NOT act as the validating authority. The validation framework is set out in Section VII Sec.No1.2.11.2 (p.178): a formal validation and closure SOP for each participating agency, including data quality and completeness checks, resolution of gaps and discrepancies until records are publishable, and formal departmental sign-off from each agency confirming that the RLCO inventory is accurate, official and complete. The Module 9 RIS/AKTU Gating Module (Sec.No1.2.9) provides the central gating workflow for AKTU Final Approval before publication. Software acceptance under the Contract (Operational Acceptance Tests in Sec.No4.3) is based on the Supplier's delivery of system functionality meeting specified requirements — NOT on the legal correctness of individual RLCO data records, which remain the responsibility of BOI/AKTU and the relevant department under the Asaan Karobar Act, 2025.
249	**The TA Workstream requires population and standardization of RLCO datasets across multiple jurisdictions and departments. Could the Purchaser clarify whether the Supplier will be responsible solely for data collection, structuring, and migration activities, or also for validating the legal correctness, completeness, and continued regulatory accuracy of RLCO content provided by participating departments?**	The Supplier's responsibility under the TA workstream is for data collection, structuring, standardisation, mapping and migration of RLCO datasets across jurisdictions (Section VII Sec.No1.2.11.1, p.177–178; Sec.No2.5.1–Sec.No2.5.3, p.215). Specifically:• Mapping support and methodology (Sec.No1.2.11.1): the Supplier deploys dedicated TA resources to provide practical mapping assistance to DFPs through remote support and in-person visits, ensuring RLCO information is accurate, complete, consistently structured, and supported by official legal references.• Closure and sign-off SOP (Sec.No1.2.11.2, p.178): the Supplier supports BOI/AKTU to implement formal validation and closure SOP, runs data quality and completeness checks, supports resolution of gaps until records are publishable, and secures formal departmental sign-off from each agency confirming the RLCO inventory is accurate, official and complete.The substantive legal correctness and continued regulatory accuracy of RLCO content remain with the relevant line department/provincial authority (the owning regulator), with BOI/AKTU as the gating authority through the Module 9 RIS/AKTU Gating workflow (Section VII Sec.No1.2.9). The Supplier is NOT the legal validating authority — see also S#270/row 270.

250	**During UAT and Operational Acceptance activities, could the Purchaser clarify the distinction between defect remediation and enhancement/change requests? Specifically, if new functional expectations emerge during stakeholder review that are not explicitly covered in the approved Architecture & Design Pack or Requirements Traceability Matrix, will such requests be managed through formal change-control procedures?**	The distinction between defect remediation (Supplier-cost) and change request (governed by GCC 39) is established by reference to the approved scope baseline: • Defect remediation: a failure of the delivered system to meet the agreed and accepted requirements set out in the Architecture & Design Pack, Requirements Traceability Matrix, applicable Section VII clauses, and the milestone-specific acceptance criteria. Defects identified during UAT, OAT, Warranty Period (Section IX SCC GCC 29.1, p.394 — TWO (2) YEARS) and the AMC Period (Y1–Y3 mandatory, Y4–Y5 optional per SIT-2 Notes, p.251–252) are remediated by the Supplier at NO additional cost, under the Warranty / Defect Repair SLA regime of Section VII Table 5.1-A (p.237). • MVP feedback under GCC 39.7 (p.364): Following MVP deployment and a 60-day live operation period, the Supplier MUST incorporate Priority 1 (critical) feedback findings within 30 days and Priority 2 (important) within 60 days, at NO additional cost — provided they do not constitute new features beyond the agreed MVP scope. • Change request: new functional expectations, new requirements, or scope additions that fall outside the approved baseline (including those emerging during stakeholder review that are not in the Architecture & Design Pack or Requirements Traceability Matrix) are managed under Section VIII GCC Clause 39 — Changes to the System (p.362), classified per SCC GCC 39.2.1 (p.393) as Minor (no cost/schedule impact) or Major (subject to review/approval), with Change Order Forms in Section X (p.425–432) and the GCC 39.6 turnaround (5 business days impact assessment / 10 business days decision). Valued within the 15% Change Request Budget Cap per SCC GCC 39.5 (p.364). The Architecture & Design Pack and Requirements Traceability Matrix are formalised through milestone acceptance and serve as the authoritative baseline for the distinction.
251	**The success of the PRR programme depends on sustained adoption by departmental focal persons across multiple jurisdictions. Could the Purchaser clarify whether formal organizational change management, user adoption campaigns, and jurisdictional onboarding coordination are fully within the Supplier's scope, or whether BOI/AKTU will separately lead these institutional transformation activities?**	Organisational change management, user-adoption activities and jurisdictional onboarding coordination are within the Supplier's scope: • Stakeholder Engagement (Section VII Sec.No1.2.11.3, p.178): the Supplier MUST design and deliver structured stakeholder engagement sessions — physically and virtually — across all six jurisdictions, with a minimum of one stakeholder session per jurisdiction per mapping wave, including validation workshops, targeted resolution sessions with key regulators, and capacity building seminars for BOI/AKTU, provincial focal points, chambers of commerce, and other key stakeholders. • Stakeholder Engagement and Reform Facilitation Training (Sec.No2.4.8, p.214): structured seminars and capacity building sessions on the PRR mandate, RLCO submission, RIS process, and reform facilitation approach — aligned to TA workstream jurisdiction onboarding waves. • Training Plan (Sec.No2.4.1, p.212): includes jurisdiction-wise DFP onboarding sessions aligned to mapping tranches, and recurring refresher clinics. • Knowledge Transfer Plan (Sec.No2.4.1, Sec.No2.4.4) and Knowledge Transfer Completion Report at project closure. BOI/AKTU provides institutional facilitation (formal engagement letters; DFP nominations; access to provincial focal points) per Sec.No1.2.11.1. The Supplier MUST propose and cost an adoption / change management plan for departmental focal persons across all six jurisdictions as part of its Technical Proposal.

252	**The RFP expressly permits pre-existing proprietary AI engines if they are declared in the technical proposal, licensed perpetually to the Government, and provided with sufficient transparency and documentation. Can the same treatment apply to preexisting non-AI software platforms, BPM engines, workflow tools, and reusable code bases?**	Yes — the IP and continuity treatment for pre-existing proprietary AI engines applies equivalently to pre-existing proprietary non-AI software platforms, BPM engines, workflow tools, and reusable code bases. Per Section VII Sec.NoG.3 (p.284–285) and Section IX SCC GCC 15.4 (p.390), pre-existing proprietary components may be used provided:• Declaration: each pre-existing proprietary component is explicitly declared in the Technical Proposal (Sec.NoG.3.5).• Perpetual government-use licence: irrevocable, royalty-free licence for use, modification and sharing within the Government of Pakistan, with the right to appoint third parties for maintenance/enhancement/integration (SCC GCC 15.4, p.390).• Sufficient transparency and documentation including build reproducibility for the PRR-specific configurations and customisations (Sec.NoG.3.5).• Source-code escrow at go-live, at each major version release, and annually during the maintenance period, with release conditions including Contractor insolvency, failure to provide maintenance, and material unremedied breach (Sec.NoG.3.6).• No restrictive licences or proprietary lock-in (Sec.NoG.3.3) for any PRR-specific custom development built on top.• Open-source compliance: viral/copyleft licences requiring open-sourcing of government code are NOT permitted (Sec.NoG.3.4); the Contractor indemnifies the Government against IP infringement claims arising from open-source use.For any PRR-specific custom code, configurations, workflows, BPMN artefacts, or scripts developed on top of pre-existing components: full ownership vests in GoP (Sec.NoG.3.1); full source-code transfer is mandatory (Sec.NoG.3.3, Sec.NoG.3.7). The objective is the unrestricted right of the GoP to engage third parties and to replicate/scale the System nationally without Contractor consent (Sec.NoG.3.8).
253	**Where pre-existing proprietary software is used, would a perpetual government-use license, full documentation, build reproducibility for PRR-specific components, and source-code escrow satisfy the no-lock-in and continuity requirements, without requiring unrestricted assignment of the underlying pre-existing product code?**	For pre-existing proprietary software used within the PRR, a perpetual government-use licence, full documentation, build reproducibility for PRR-specific components, and source-code escrow can satisfy the no-lock-in and continuity requirements, subject to the conditions in Section VII Sec.NoG.3 (p.284–285) and Section IX SCC GCC 15.4 (p.390). The required combination is: • Explicit declaration of each pre-existing proprietary component in the Technical Proposal (Sec.NoG.3.5, p.284). • A perpetual, irrevocable, royalty-free licence for use, modification and sharing within the Government of Pakistan, with the right to appoint third parties for maintenance, enhancement or integration (SCC GCC 15.4, p.390). • Sufficient transparency, documentation and build reproducibility for the PRR-specific configurations and customisations (Sec.NoG.3.5). • Full human-readable source-code transfer for any PRR-specific custom development built on top of the pre-existing component (Sec.NoG.3.1, Sec.NoG.3.3, Sec.NoG.3.7). • Source-code escrow deposit at go-live, at each major version release, and annually during the maintenance period (Sec.NoG.3.6). • Full disclosure of any open-source components with licences compliant with government use (SCC GCC 15.4, p.390; Sec.NoG.3.4). This combination satisfies the no-lock-in/continuity requirement without requiring unrestricted assignment of the underlying pre-existing OEM product code.

254	**Can the Purchaser confirm acceptable escrow release conditions and whether escrow is intended as an alternative to unrestricted source-code transfer for pre-existing proprietary software components? The RFP requires source-code escrow at go-live, major version releases, and annually during maintenance.**	Source-code escrow is required under Section VII Sec.NoG.3.6 (p.284). The mandatory escrow regime is: deposit of updated source code and system documentation into a Government-approved escrow mechanism at go-live, at each major version release, and annually during the maintenance period. The mandatory escrow release conditions MUST include: (i) Contractor insolvency; (ii) failure to provide maintenance; and (iii) material unremedied breach of contract (Sec.NoG.3.6). For pre-existing proprietary OEM components specifically, escrow operates as a continuity mechanism complementing the perpetual government-use licence, full documentation and build reproducibility required under Sec.NoG.3.5 and SCC GCC 15.4 (p.390). For PRR-specific custom-developed components, full source-code transfer is required under Sec.NoG.3.1 and Sec.NoG.3.3 — escrow is in addition to, not in lieu of, source-code delivery for custom-developed components.
255	**The RFP mandates containerized deployment, OpenAPI interfaces, portability, and sovereign operational independence. Could the Purchaser clarify whether the use of enterprise-supported open-source components (e.g., databases, search engines, BPM engines, vector stores, orchestration frameworks) is fully permissible, provided that all licensing obligations, supportability requirements, and escrow obligations are satisfied?**	Enterprise-supported open-source components (databases, search engines, BPM/workflow engines, vector stores, orchestration frameworks, identity providers) are fully permissible and consistent with the architectural mandates of this RFP. Section VII Sec.No3.4.1 (p.223) mandates containerised deployment of all System components (Kubernetes-based or equivalent) on GoP-controlled hosting; Sec.No1.3.6.1 (p.194) mandates OpenAPI-compliant API exposure; Sec.No1.1.1.7 (p.149) mandates cloud-agnostic operation; Sec.No1.3.1 mandates microservice decomposition (Table 1.3.1-A, p.187). Open-source use is subject to the licensing and IP regime of Section VII Sec.NoG.3.4 (p.284) and Section IX SCC GCC 15.4 (p.390): all open-source components MUST be fully disclosed with licence information; viral/copyleft licences requiring open-sourcing of government code are NOT permitted; the Contractor MUST indemnify the Government against intellectual property infringement claims arising from open-source components used in the System (Sec.NoG.3.4). For PRR-specific custom-developed code built on top of open-source components: IP vests in GoP (Sec.NoG.3.1); full source code transfer is mandatory (Sec.NoG.3.3); source code MUST be free from restrictive licences and proprietary lock-in (Sec.NoG.3.3). For pre-existing proprietary support/enterprise edition components on top of open-source: declare in Technical Proposal, perpetual government-use licence per SCC GCC 15.4, source-code escrow per Sec.NoG.3.6 (at go-live, major version releases, and annually).

256	**The RFP mandates source code escrow and full operational independence for the Government of Pakistan. Could the Purchaser clarify whether escrow obligations apply solely to custom-developed components, or also extend to deployment scripts, Al prompt templates, training pipelines, workflow models, and infrastructure-ascode artifacts?**	Source-code escrow and operational-independence obligations apply broadly to ensure full GoP operational independence (Section VII Sec.NoG.3, p.284–285). Specifically:• Custom-developed components: full source-code transfer is mandatory under Sec.NoG.3.1 and Sec.NoG.3.3 — front-end, back-end, APIs, scripts, microservices.• AI artefacts: prompt templates, scoring logic, feature engineering, orchestration logic developed or customised under the Contract are GoP IP and MUST be transferred with documentation (Sec.NoG.3.5).• Database schemas, data models, workflows and BPMN artifacts: GoP IP, vest immediately upon creation (Sec.NoG.3.1).• Deployment scripts, DevOps pipelines and infrastructure-as-code (IaC): GoP IP under Sec.NoG.3.1; delivered together with build instructions and configuration documentation under Sec.NoG.3.3.• Training pipelines and model evaluation artefacts (where AI training is performed under the Contract): GoP IP under Sec.NoG.3.5; transferred with documentation.• Declared pre-existing proprietary components: escrow plus perpetual government-use licence and sufficient transparency/documentation under Sec.NoG.3.5 and SCC GCC 15.4 (p.390); escrow covers source code and system documentation at go-live, each major version release, and annually during maintenance (Sec.NoG.3.6).The objective in all cases is the unrestricted right of the GoP to engage third parties for maintenance/enhancement, to transfer the System to provincial governments, and to replicate/scale the System nationally, without requiring further Contractor consent (Sec.NoG.3.8, p.284).
257	**Can the Purchaser confirm which cybersecurity, data residency, encryption, MFA, logging, VAPT, DR, and compliance requirements must be satisfied before MVP, before go-live, and before Final Acceptance? The RFP includes strong requirements for encryption, MFA, immutable logs, incident response, Pakistan-based hosting, and AI/data safeguards, but the delivery schedule would benefit from staged compliance gates.**	Cybersecurity, data-residency, encryption, MFA, logging, VAPT, DR and compliance requirements are mandatory and validated progressively: • MVP (Week 10) — Sec.No4.2.1 mandates the following pre-commissioning test confirmations: government-controlled hosting with DEV, UAT and PROD environments operational with documented deployment scripts, backups and DR approach; database encryption at rest; TLS in transit; admin MFA active. • Operational Go-Live (Week 40 — Milestone M11) — full security hardening per Section VII Sec.No1.6 (p.202–205) and Sec.No1.3.4 (p.190–192): OWASP Top 10 compliance (Sec.No1.6.1); mandatory MFA for all publishers, reviewers, administrators and AI reviewers (Sec.No1.6.2); full encryption regime including TLS 1.2+/1.3 in transit and at-rest encryption for all stores (Sec.No1.6.3); HSM-based KMS hosted in Pakistan (Sec.No1.3.4.4); WAF and DDoS protection (Sec.No1.6.4); centralised logging, SIEM and distributed tracing (Sec.No1.3.4.6); DR with RTO ≤4 h and RPO ≤1 h (Sec.No1.3.5.3); security incident response plan with 4-hour notification (Sec.No1.6.7). • Final Acceptance / Operational Acceptance — Sec.No1.3.4.3 (p.191) states verbatim: 'PSS compliance MUST be a mandatory pre-condition for the issuance of the Operational Acceptance Certificate.' The PSS Compliance Matrix is a mandatory deliverable. The annual third-party VAPT (Sec.No1.6.6) is required. The detailed compliance gate-by-gate checklist will be set in the Agreed Project Plan (Sec.No2.6.2).

258	**Who will select and pay for the third-party VAPT or source-code review provider, and will the Supplier have a defined cure period to remediate findings before they affect acceptance or payment?**	The annual third-party Vulnerability Assessment and Penetration Testing (VAPT), including source-code review, is mandatory per Section VII Sec.No1.6.6 (p.203). The independent security firm conducting the VAPT MUST be acceptable to the Purchaser; final selection rests with the Purchaser. The cost of the annual VAPT is the Supplier's responsibility — SIT-2 row 5.2 (p.252) 'Annual Third-Party VAPT — source code review + infrastructure penetration + remediation reporting' is a MANDATORY Recurrent Cost line item that MUST be quoted by the Proposer for Y1–Y3 (Section VII Sec.No5.2.4, p.238). Mandatory remediation timelines (Sec.No1.6.6): Critical and High severity findings MUST be remediated within thirty (30) days of identification; Medium severity findings within ninety (90) days. The Supplier MUST maintain a vulnerability register with severity classification, remediation timelines and status tracking, accessible to the Purchaser. Audit reports and remediation evidence MUST be submitted to the GoP oversight body within thirty (30) days of test completion. Where remediation is in progress within the Sec.No1.6.6 timelines and a finding is not blocking, it does not by itself bar Operational Acceptance; however, PSS compliance is a mandatory pre-condition for the issuance of the Operational Acceptance Certificate (Sec.No1.3.4.3, p.191).
259	**Can the Purchaser provide the precise performance benchmarks for Operational Acceptance, including response times, transactions per second, public search load, bulk upload volumes, consultation surge assumptions, and concurrent authenticated user expectations? The RFP references mandatory load testing of at least 2,000 concurrent authenticated users before go-live.**	The mandatory performance benchmarks for Operational Acceptance are specified in Section VII Sec.No1.5 — Performance Requirements (p.197–201) and Table 1.5-A — Summary of Mandatory Performance Targets (p.201):Response time (P95, under sustained 2,000-concurrent-user load):• Public search and browse: ≤ 2 seconds• RLCO detail retrieval: ≤ 3 seconds• Workflow state transition: ≤ 5 seconds• Record save/create: ≤ 3 seconds• Bulk-import validation for 1,000 records: ≤ 30 secondsConcurrency:• 2,000 simultaneous authenticated DFP/AKTU sessions (mandatory load testing before go-live per Sec.No1.5.3, p.198)• ≥ 5,000 simultaneous unauthenticated public portal users (normal operations, auto-scaling baseline)• ≥ 25,000 simultaneous public portal users (peak consultation surge, auto-scaling activated)Availability:• ≥ 99.9% monthly (target 99.95%)Recovery:• RTO ≤ 4 hours; RPO ≤ 1 hour (Sec.No1.3.5.3, p.193) — demonstrated in the annual DR drill.Other:• Real-User Monitoring (RUM) and Application Performance Monitoring (APM) per Sec.No1.5.6.• AI Assist Module specific processing latency for similarity/conflict detection meeting interactive-response targets (see S#231/row 234).Validated during Pre-commissioning Tests (Sec.No4.2) per subsystem and Operational Acceptance Tests (Sec.No4.3) — OAT-1 Performance and Concurrency. Annex Tech-I scoring evaluates the Proposer's design against these benchmarks (Section X, p.434+). Proposers MUST commit to these benchmarks; bidding below the mandatory minima renders the Proposal non-responsive.
260	**If performance, security, or DR testing is delayed or fails because of governmentprovided hosting constraints, third-party infrastructure limits, or unavailable test environments, will the Supplier receive corresponding schedule relief and a retest opportunity?**	Where Pre-commissioning Tests (Sec.No4.2) or Operational Acceptance Tests (Sec.No4.3) — including performance, security, multi-jurisdiction or disaster-recovery testing — are delayed or fail because of factors beyond the Supplier's control (GoP-provided hosting constraints, third-party integration unavailability, unavailable test environments, delayed Purchaser-side approvals or stakeholder access), the Supplier is entitled to: (a) a retest opportunity, and (b) corresponding schedule relief under Section VIII GCC Clause 40 — Extension of Time for Achieving Operational Acceptance (p.364), through the project governance and notification process under GCC 18.2 and GCC 19. Documentary evidence of the

		constraint and impact analysis on the Implementation Schedule are required. Liquidated Damages under GCC 28.2 (p.342) are payable only for delay within the Supplier's control. Where Operational Acceptance is delayed by Purchaser-attributable factors, the Operational Acceptance date adjusts correspondingly under GCC 27 — Commissioning and Operational Acceptance (Section VIII, p.339–340) and the Performance Security obligations track the adjusted schedule. Force Majeure events are covered by GCC Clause 38 (Section VIII, p.358). The Supplier MUST give written notice of any such impediment within the period specified in GCC 38.2.
261	**The RFP references compliance with Pakistan Security Standards (PSS), OWASP, and ISO/IEC 27001-aligned controls. Could the Purchaser clarify whether formal certification activities including penetration testing, security audits, pre-OAT compliance validation, and any third-party certification costs fall within the Supplier's contractual scope, and whether approved government security assessors will be designated for this purpose?**	Formal certification, penetration testing, security audit and pre-OAT compliance validation activities fall within the Supplier's contractual scope and MUST be priced: • Annual third-party VAPT including source-code review — SIT-2 row 5.2 (p.252) is a MANDATORY Recurrent Cost line item Y1–Y3 priced by the Proposer (Section VII Sec.No1.6.6, p.203; Sec.No5.2.4, p.238). • PSS Compliance Matrix — mandatory deliverable, prepared by the Supplier and submitted as a mandatory pre-condition for the issuance of the Operational Acceptance Certificate (Section VII Sec.No1.3.4.3, p.191; Sec.No1.6 preamble, p.202). • ISO/IEC 27001-aligned information security management controls — mandatory; ISO 27001 certification of the Supplier's delivery organisation or the System itself is PREFERRED, not mandatory (Sec.No1.6.8, p.203). Proposers are encouraged to demonstrate certification. • OWASP Top 10 compliance — mandatory across all portals and APIs (Sec.No1.6.1, p.202). • Annual security audit — covering access controls, audit log integrity, encryption key management, vulnerability remediation status and security policy compliance, with findings submitted to the Purchaser (Sec.No1.6.8). Where the Purchaser designates approved government security assessors for any audit/assessment, the Supplier coordinates with those assessors. PSS reference materials are accessed through the issuing authorities (Ministry of IT and Telecom; National Telecommunication Corporation (NTC); IGNITE); the Purchaser will facilitate access during the engagement.
262	**Could the Purchaser confirm the required Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets for the PRR platform, including the Al Assist Module, search infrastructure, and audit stores, and clarify whether disaster recovery infrastructure will be provisioned by the Purchaser or supplied by the Supplier?**	Per Section VII Sec.No1.3.5.3 (p.193), the System MUST achieve contractually binding Recovery Time Objective (RTO) of FOUR (4) HOURS or less and Recovery Point Objective (RPO) of ONE (1) HOUR or less, to be demonstrated in the annual DR drill. These targets apply across the platform — including the AI Assist Module, search infrastructure and the Immutable Audit Store. Automated backups with point-in-time recovery MUST be configured for the primary registry database. Scheduled snapshots MUST be maintained for search indices and analytics warehouses. All backup vaults MUST be encrypted and stored in a separate geographic zone. Deployment MUST be multi-zone within Pakistan across at least two independent availability zones, with multi-city redundancy across at minimum three cities preferred for critical services (Sec.No1.3.5.2). DR infrastructure forms part of GoP-provided infrastructure (Sec.No3.0.2, Sec.No3.1, Sec.No3.2, Sec.No3.3 — 'No hardware is procured under this Contract'); the Supplier architects the DR solution and documents the required sizing in the Deployment Architecture document (Sec.No2.6.2). Annual DR drills are mandatory with results submitted to the GoP oversight body within thirty (30) days (Sec.No1.3.5.2).

263	**The PRR platform is intended to operate as a national public regulatory registry with high-volume public search and browse capabilities. Could the Purchaser provide indicative assumptions regarding expected concurrent users, peak search volumes, consultation-event traffic spikes, and API transaction loads to enable accurate performance sizing and capacity planning in proposer submissions?**	The mandatory indicative assumptions for capacity planning are specified in Section VII Table 1.5-A (p.201) and Sec.No1.5.3 (p.198) — these are CONTRACTUAL MINIMA, not estimates: • Concurrent authenticated DFP/AKTU sessions: 2,000 simultaneous (national mapping campaign scenario) • Concurrent unauthenticated public portal users (normal operations): ≥ 5,000 (auto-scaling baseline) • Concurrent unauthenticated public portal users (peak consultation surge): ≥ 25,000 (auto-scaling activated) • System availability ≥ 99.9% monthly; RTO ≤ 4 h; RPO ≤ 1 h. Public consultation events: per Section VII Sec.No1.2.8.3 (Public Portal — public consultation windows), open consultation windows of minimum 30 days are supported, with significant traffic spikes expected around launch and closure of high-profile consultations — the 25,000 peak target is the sizing assumption for such surges. API transaction loads: the platform MUST be designed for horizontal auto-scaling of the public portal and search tier (Sec.No1.5.3); the open read-only API layer for PBP and other integrations (Sec.No1.3.6.2) is part of the same scale envelope. Bulk-import throughput: 1,000-record validation within ≤ 30 seconds per Table 1.5-A. Proposers should size the GoP-provided infrastructure (documented in the Deployment Architecture document under Sec.No2.6.2) to meet these binding minima with appropriate headroom for growth. The platform MUST remain horizontally scalable beyond the stated minima (Sec.No1.5.3).
264	**Could the Purchaser clarify the measurable performance benchmarks that will be used during UAT/OAT for determining acceptance of the PRR platform including response-time thresholds, search indexing latency, concurrent user benchmarks, and Al module processing performance?**	The measurable performance benchmarks for Operational Acceptance are specified in Section VII Sec.No1.5 — Performance Requirements (p.197–201), particularly Table 1.5-A — Summary of Mandatory Performance Targets (p.201). These are binding contractual minima validated during Pre-commissioning Tests (Sec.No4.2) and Operational Acceptance Tests (Sec.No4.3): Page-load / response time (P95 measured under sustained 2,000-concurrent-user load): • Public search and browse: ≤ 2 seconds • RLCO detail retrieval: ≤ 3 seconds • Workflow state transition: ≤ 5 seconds • Record save/create: ≤ 3 seconds • Bulk-import validation for 1,000 records: ≤ 30 seconds Concurrency: • 2,000 simultaneous authenticated DFP/AKTU sessions • ≥ 5,000 simultaneous unauthenticated public portal users (normal operations) • ≥ 25,000 simultaneous public portal users (peak consultation surge) Availability and recovery: • System availability ≥ 99.9% monthly (target 99.95%) • RTO ≤ 4 hours; RPO ≤ 1 hour (Sec.No1.3.5.3, p.193) AI module benchmarks: the AI Assist Module specific processing-time benchmarks (e.g., sentiment analysis latency, NLU classification throughput) are validated during Subsystem 9 Pre-commissioning Test (Sec.No4.2.10) — operational at Milestone M10 at Week 28 (Section IX SCC GCC 12.1, p.386). Where testing is delayed or fails due to Purchaser-provided hosting or third-party constraints beyond the Supplier's control, schedule relief is available under Section VIII GCC Clause 40 — Extension of Time (p.364).

265	**What information about named subcontractors, software vendors, proprietarycomponents, open-source components, and manufacturer authorizations must beincluded in the proposal to avoid later non-responsiveness?**	To avoid a finding of non-responsiveness, the Technical Proposal MUST include:• Subcontractors: identification of each proposed subcontractor and the scope subcontracted, supported by the Subcontractor's Agreement form (Section IV, p.115). Subcontractor eligibility under Section V (p.133) and ITP 4 applies.• Software vendors and proprietary OEM/commercial components: full disclosure of each pre-existing proprietary component used (per Section VII Sec.NoG.3.5, p.284), with declared licence terms (perpetual government-use, royalty-free, with rights to appoint third parties) in line with SCC GCC 15.4 (p.390).• Open-source components: full disclosure of all open-source components with licence information (per Sec.NoG.3.4, p.284 and SCC GCC 15.4, p.390). Viral/copyleft licences requiring open-sourcing of government code are NOT permitted.• Manufacturer's Authorization on the Section IV form, where applicable to commercial software/OEM components.• Conformance of Information System Materials (Section IV form).• Intellectual Property Forms (Section IV).All disclosures are subject to the operational-independence, escrow, source-code and continuity obligations of Section VII Sec.NoG.3.1 through Sec.NoG.3.8 (p.284), and the IP vesting provisions of SCC GCC 15.4 (p.390).
266	**The RFP requires the Supplier to demonstrate at least two contracts of similar nature with a value of at least 1.5 Million USD. Could the Purchaser clarify if any similar but substantially completed projects will fulfil this requirement? Secondly, will the experience of subcontractor be considered particularly for two qualifying projects of at least 1.5 Million USD?**	Per Section III Sub-Factor 1.4.2 (p.67–69), the Proposer must demonstrate at least two (2) contracts of similar nature, each of at least USD 1.5 million, successfully and substantially completed within the last five (5) years. A substantially completed similar project meeting the criteria is acceptable — the documentation field 'Status of completion' in Section III (p.69) expressly lists both 'completed' and 'substantially completed' as valid statuses (see also S#2). Subcontractor experience for the CURRENT proposal is NOT credited towards the Lead Bidder's qualifying experience under Section III Sub-Factor 1.4 unless the Evaluation Criteria expressly provide for it (see S#83). Distinct from this: in a CITED past contract, the Proposer's own past role of 'Sub-consultant' is explicitly recognised in Section III, p.69; in that case, the firm's 'Percentage of participation' in the past contract counts towards its own qualifying value. For Joint Ventures, all members' qualifying contracts are aggregated under the 'All members combined — Must meet requirements' column (Section III, p.67). Required evidence per contract: signed contract/work order, completion certificate or client reference letter, and proof of project value and scope.
267	**The RFP expressly permits use of pre-existing proprietary AI engines if declared, perpetually licensed to the Government, and sufficiently documented. Can the Purchaser confirm that the same treatment applies to pre-existing non-AI software platforms, including BPM/workflow engines and reusable low-code code bases, provided that all PRR-specific deliverables are owned by the Government, the Government receives a perpetual license for PRR use, and continuity is protected through documentation and escrow?**	The treatment afforded to pre-existing proprietary AI engines applies equally to other pre-existing/background software, including BPM/workflow engines and reusable low-code code bases, subject to the following: Declaration – such platforms must be declared in the bid, with background IP clearly distinguished from PRR-specific deliverables. Ownership – all PRR-specific configurations, customizations, and integrations vest in the Government. Perpetual license – a perpetual, irrevocable, royalty-free license for PRR use, expressly covering the right to operate, maintain, modify, and enhance the solution, including by successor contractors on the Government's behalf. Documentation & escrow – sufficient documentation for independent operation, plus source code held in escrow with defined release triggers (insolvency, cessation of support, uncured breach, or product discontinuation), with the license extending to any released materials.

268	**Technical Scoring Matrix does not clearly specify a dedicated evaluation matrix for the low-code capability. Kindly clarify how the low-code requirement will be evaluated during technical evaluation.**	The low-code requirement will be evaluated as part of the existing Technical Scoring Matrix; a separate, dedicated matrix will not be introduced. Bidders' low-code capability will be assessed under the relevant existing criteria, including [e.g., Solution Architecture & Technical Approach / Platform Capability / Methodology], based on the evidence submitted in the technical proposal.'Low Code' (10% technical weight) assesses the platform's low-code/no-code capability for rapid configuration (e.g. CMS, template manager, workflow configuration) per Section VII sub-section 1.2.x/13. Any low-code/no-code component used MUST be extensible without vendor lock-in and MUST allow full source-code export and independent deployment. Please also refer to S# 135 and 272.
269	**The Supplier’s Code of Conduct needs to be signed by all resources as part of proposal?**	The Supplier's Code of Conduct is not required to be signed by all individual resources at the proposal stage. At the time of bid submission, the Bidder is required to acknowledge and accept the Code of Conduct at the organizational level through [an authorized signatory / the prescribed undertaking .