



RFP | Contracts and Litigation Management System

Annexure A - Contracts and Litigation Management System

U Microfinance Bank Limited (Ubank)

Contents

1.	Objectives and Purpose	2
2.	Scope of Work.....	3
3.	Functional Requirements	9
3.1 -	Contract Management Solution	9
3.2 -	Litigation Management Solution	14
3.3 -	Reporting Requirements.....	16
3.4 -	General Requirements – Applied to both, Contract and Litigation Management Modules.....	17
4.	Non-Functional Requirements	19
4.1 -	Performance & Scalability	19
4.2 -	Security.....	19
4.3 -	Reliability & Availability	20
4.4 -	Compatibility.....	20
5.	Technology and Information Security Requirements	21
6.	Service Level Agreement (SLA)	28

1. Objectives and Purpose

The Bank seeks to implement the System(s) in order to achieve the following objectives:

- **Establish centralized platform(s).** Bring all contracts and all litigation and legal matters onto one system (or integrated systems or modules), so that the Bank has searchable and authoritative sources of its contractual commitments and legal proceedings.
- **Digitize and standardize the contract lifecycle.** Move contract drafting, review, approval and execution onto a defined end-to-end workflow, using standard templates drafted and locked by the Legal Department, with mandatory Legal sign-off and turnaround time tracking at each stage.
- **Enable legally valid electronic execution.** Execute contracts electronically, with electronic signatures recognized under the law of Pakistan and with security procedures sufficient to establish the integrity and authenticity of executed documents, thereby reducing execution time and physical handling.
- **Prevent missed obligations, expiries and renewals.** Track contractual obligations and covenants, auto-renewal triggers and termination notice periods, and generate timely alerts so that renewals and obligations are actioned on time rather than through manual follow-up.
- **Strengthen control over contractual risk.** Maintain a deviation register recording negotiated clauses against original clauses, apply contract risk scoring, enforce validation against the delegation of authority, and require legal due diligence on counterparties prior to execution.
- **Introducing AI-assisted drafting and review.** Use artificial intelligence to suggest approved clauses, flag missing, ambiguous or non-standard clauses and deviations, compare counterparty drafts against the Bank's templates, and summarize key terms and obligations, in each case subject to review and final sign-off by the Legal Department.
- **Centralize litigation and dispute management.** Manage cases end from pre-litigation through filing, trial, appeal and disposal, together with court and jurisdiction mapping, hearing schedules, adjournments, limitation periods and the associated case documents and evidence.
- **Make legal and financial exposure visible.** Record claim amounts, decretal amounts, contingent liabilities, provisioning status, settlements and recoveries on a case-wise basis, and present the Bank's aggregate litigation exposure for management and Board oversight.
- **Manage legal matters and external counsel.** Route all legal requests through a central intake with defined service levels, and manage the approved panel of external counsel, including case allocation, performance and outcome tracking, fee structures, budgets and invoice approval.

- **Retain institutional knowledge and deliver management reporting.** Preserve precedents, legal opinions, judgments and counterparty history notwithstanding employee movement, and provide real-time dashboards and management information for the Legal Department, senior management, the Board and its committees, and for regulators and auditors.

2. Scope of Work

The successful Bidder will be responsible for the end-to-end delivery of its proposed Contracts and Litigation Management System (the "System") or (the "System(s)" in case separate solutions are proposed), comprising an electronic Contract Management module/solution and a Litigation and Dispute Management module/solution, together with the supporting legal matter management, knowledge management, reporting, mobile and AI capabilities set out in this annexure.

This RFP requires solutions for (02) modules:

1. Contracts Management System / Module
2. Litigation and Dispute Management System / Module

It is preferred that both modules are part of the same / single solution system; or, may be deployed as two independent (and integrated) systems. This includes, but is not limited to, the following key areas:

1. Through Requirement Gathering and Analysis:

- a. Complete due diligence of the Bank's existing contract and litigation recording mechanism, repositories and working files, to ensure that all current records, processes and functionality (in addition to all the requirements of this RFP) are carried forward and migrated to the new System.
- b. Complete due diligence of the Legal Department's current workflows, Standard Operating Procedures (SOPs), delegation of authority, approval hierarchies and method of working, and of the interfaces between the Legal Department and the initiating/user departments.
- c. Prepare and submit a detailed requirement/solution design document, including workflow designs, integration design and configuration decisions.

2. Solution Supply:

- a. Supply, deployment, configuration and provisioning as per the requirements of this RFP and this annexure, including all required licenses, software, support services and warranties.
- b. Supply, on-premises deployment, configuration and provisioning of a complete end-to-end for the Primary Site (with High Availability) and the Disaster Recovery (DR) site to ensure that the SLA mentioned in this document is fully complied with.

- The solution(s) should support and is to be deployed / configured for auto-failover in case of PR site failure.
- c. The bidder must submit **a complete unpriced BOQ of the solution** within their technical proposal, with clear depiction of all offered line items, aligning with their associated details such as SKU, Model Number, Quantity, Item Descriptions etc.
 - The hardware requirements for implementing the proposed solution(s) – for both modules, must be clearly mentioned in the BOQ.
- d. The bidder **must submit complete detailed hardware sizing (segregated for all proposed environments) for the implementing the solution**, with clear specifications and counts, inclusive of all underlying software (such as but not limited to: Hypervisors, OS, DB licenses etc.)
 - Vendors must propose hardware sizing for all proposed environments (PR, DR and Staging), that must be sufficient for at least 5 years after the complete (not partial) production cutover of the implementation.
- e. Supply of the contract management capability, covering the template and clause library, contract initiation and drafting, review and approval workflow, electronic execution and signing, contract repository, obligation and renewal tracking, and deviation and contract risk management, as specified in this Annexure.
- f. Supply of the litigation and dispute management capability, covering case lifecycle management, party and court mapping, hearing and calendar management, document and evidence management, financial exposure and provisioning, and litigation risk analytics, as specified in this Annexure.
- g. Supply of the supporting legal functions, covering legal matter intake and management, external/panel counsel management, notices and deadlines management, and knowledge management, as specified in this Annexure.
- h. Supply of the electronic execution capability, including electronic signatures recognized under the law of Pakistan, issued and supported by an accredited certification service provider, and the security procedures necessary to establish the integrity and authenticity of executed electronic documents.
- i. Implementation of the AI-assisted capabilities described in Annexure-A, including clause suggestion, deviation and risk flagging, draft comparison, contract and judgment summarization and precedent search, in each case operating within a secure, access-controlled environment and subject to final sign-off by the Legal Department.
- j. The Solution must offer an intuitive UI/UX design for web (and responsive mobile) interfaces, including role-based dashboards, work queues and navigation/workflows.

3. Deployment & Configuration:

- a. Full deployment and configuration of the System(s) and all its modules to align with the Legal Department's operational requirements as per the required specifications.
- b. Configuration of the System(s) with the necessary business rules for contract routing, review stages, approvals, escalations, turnaround time targets and notifications, aligned with Ubank's SOPs and delegation of authority, and enhanced with AI where applicable.
 - i. Vendor shall disclose /clarify the following: data ownership, confidentiality and restriction on vendor/third-party use of UBank data, including prohibition on use of UBank data for AI/model training without prior approval.

c. Environment Setup and Provisioning:

- i. Vendors must provide complete infrastructure specifications (with OEM datasheets) for the proposed solution, including software, and platform architecture required for deployment and ongoing operations. Proposed solution must have these five distinct environments:
 - **Non-Production:** Development / Testing / UAT
 - **Production** (to be deployed with local High-Availability)
 - **Disaster Recovery (DR)**
- ii. The vendor must provide a complete lifecycle of the solution(s) and its components being delivered as part of the solution.
- iii. The vendor must ensure that all solution components being delivered as part of the solution **remain in full enterprise OEM support for at least 5 years post complete deployment.**
- iv. Vendor must ensure that any proposed component, software or license components **must not be declared End-of-Life (EOL) or End-of-Support (EOS)** before the first full production cutover.
- v. If any of the components are declared EOL or EOS by the OEM before the first full production cutover, the vendor shall be liable for replacing/upgrading that component with equally relevant replacement with consent of Ubank, with no cost to Ubank.
- d. Set-up of the standard contract templates and the approved clause library in conjunction with the Legal Department, including locking of clauses and configuration of deviation controls.

- e. Incorporation of all required security controls, user access roles, audit logging and compliance features (data protection, retention, Legal Hold and reporting needs) as the non-functional requirements specify.
- f. Provision and configuration of segregated Development, Testing/UAT and Production environments, with a controlled promotion path between them.

4. Disaster Recovery Site:

- a. The bidder must supply, deploy and configure a full-fledged warm Disaster Recovery (DR) site at Ubank Disaster Recovery DC to ensure seamless services, SLA compliance and automatic services shifting to DR in case any outage at primary site.
- b. The vendor must execute two full cycles of DR switch over and fall back. The DR switchover must be fully functional for at least 3 calendar days before falling back to primary site.
- c. Vendor must provide comprehensive runbook for use by Ubank DR Office, with step-by-step instructions on switching over to DR and falling back to primary site.
- d. As part of DR design, vendors must specify the RPO and RTO of the solution, based on Ubank's requirements and all involved moving parts.
- e. Vendor must qualify configuration items (CI) that need to be replicated along with replication frequency and changed based on the flow of information (primary or DR).

5. Technical Proposal:

- a. Vendors responding to this RFP must include the following information as part of their proposal:
 - Technical writeup of the solution, referencing the RFP's functional requirements.
 - Detailed solution architecture (deployment architecture for hardware setup and software, scalability approach, and infrastructure sizing assumptions).
 - High Level Diagrams
 - Implementation methodology and deployment approach
 - Integration framework and API architecture
 - Details of the hardware requirements (bidder to include an unpriced BOQ for the hardware required to run their solution for all environments, **without providing the hardware**) and software infrastructure and requirements for deployment on virtual infrastructure as a second option (i.e., complete hardware and software details in case Ubank deploys the solution on their incumbent on-premises hardware)
 - Complete infrastructure specifications:
 - Hardware requirements
 - Software architecture
 - Infrastructure sizing assumptions
 - Security architecture

- d. The Bidder will design user workflow journeys as per Ubank requirements, SOPs and guidelines determined during the discovery phase, covering contract initiation through to execution, and case initiation through to disposal.
- e. Configuration of the delegation of authority and authority matrix validation, segregation of duties, and deviation and settlement approval routing.

10. **Training Programs:**

- a. Development and delivery of comprehensive training programs for end-users (Legal Department officers, initiating/user department users and, where applicable, external/panel counsel) and for administrators on the new System.
- b. Delivery of train-the-trainer sessions to enable Ubank to conduct subsequent internal training independently.
- c. Provision of all necessary training materials.

11. **Documentation:** Provision of complete technical documentation, functional and integration design documents, user manuals, administrative guides and operations runbooks for the implemented Solution(s), updated on each major release.

12. **Ongoing and Post-Go Live Support:**

- a. Provide continuous support and maintenance for complete solution, as per the agreed Service Level Agreement (SLA).
- b. Provide on-site support as and when required.
- c. Provision of warranty & support for the 5 Year time period.
- d. Provision of a dedicated hypercare/stabilization period immediately following go-live, with on-site presence as required by Ubank.
- e. Provide on-site support (complete, for all proposed components, software and all required licenses).
- f. Provision of all product upgrades, patches and security fixes during the contract term, without overwriting or invalidating Ubank's configurations.

11. **Solution Sizing Parameters:**

Below is estimated sizing rationale for the solution(s). Bidder is required to explicitly explain their licensing model and size their solution(s) for optimal performance and best user experience as per the parameters (tentative) given below. **Please consider a 10% year-on-year growth to all below mentioned parameters, for the next (05) years.**

- a. Current total number of active contracts till today (approx.) = 1,200

- b. Current total number of non-active contracts till today (approx.) = 3,500
- c. Average new contracts per month (approx.) = 50
- d. Number of Concurrent Users:
 - a. Contracts Management Solution = 50
 - b. Litigation and Dispute Management Solution = 50
- e. Data retention policy = Minimum 10 years with easy archive and backup mechanism for data older than 10 years.

3. Functional Requirements

3.1 - Contract Management Solution

A. WORKFLOW FOR EXECUTION OF DOCUMENT/CONTRACTS

1. All standard contracts shall be drafted and locked by legal in collaboration with the respective department(s) for placement on the Electronic Contract Management System (“**eCMS**” or the, “**System**”).
2. Initiating/user department will determine and select the appropriate standard agreement draft, as per the services/goods required, from the list available over eCMS or will upload agreed draft over eCMS, as the case may be. The initiating/user department shall also incorporate all the relevant details of the other party i.e. legal name, legal status, address, authorized representative, term of agreement, etc. and shall also attach relevant documents, if any.
3. There needs to be a proper end-to-end flow for user access management.
4. All logs including action history will automatically be maintained by the System with view option available to admin and/or respective user/initiator.
5. Approval/signoff of legal department will be mandated for all documents/contracts to be executed through the System.
6. Initiating/User department will share finalized approved draft to the other party/customer’s authorized person for review and sign off electronically.
7. Once executed by the other party/customer, an automated intimation will be generated to the initiator/user by the system for sign-off by the UBANK authorized signatory.
8. At the time of execution of the document/contract, a summary of key terms e.g., names of all parties, subject matter/scope involved, amount, payment to be paid by or to the respective party, term, termination, expiry to be fetched from draft must appear at the top of the screen.

9. Electronic signatures as per bank policy must appear on each page of the contract including annexures etc.
10. Each activity should appear at the bottom of each page OR in separate report in relation to each page with unique identification, its number, dates, persons etc. and system reference.
11. All users should be able to generate reports for all activities in relation to integrity and authenticity of each document/contract including relating to induction, preparation of draft contract (review, view, print, comments, approvals, rejections etc.) at all times.
12. Original form of UBANK's delegation of authority and/or group authority matrix, as the case may be, should always be available under a drop down menu to all users.
13. System will retain all executed agreements which will be retrievable (along with all activity logs relating to the agreements) at any time by all users
14. The system should allow creation of any dispute memo or settlement agreement in relation to executed agreement by all the respective users of the system.
15. System should have interfaces based on best international industry practices and able to connect with other systems like system implemented by government (for e.g. for payment of stamp duty) or any group system.
16. An intimation with regard to executed contracts shall (by default) always be sent to heads/chiefs of each respective department.
17. All users or initiating/user department should be able to assign or re-assign the draft to any team members.

B. CONTRACT MANAGEMENT ENHANCEMENTS:

- Contract obligation/covenant tracking, not just expiry tracking.
- Automated tracking of payment, reporting, SLA, insurance, security, warranties and other obligations.
- Auto-renewal and termination-notice tracking.
- Contract deviation/exception register.
- Record of original clause vs negotiated clause.
- Approval of deviations based on risk/materiality.
- Contract risk scoring: Low/Medium/High/Critical.
- Counterparty legal due diligence checklist.
- Verification of authorized signatory/authority before execution.
- Automated Delegation of Authority validation rather than merely displaying the authority matrix.

- Segregation of duties between initiator, reviewer, approver and signatory.

C. AI Software/Tools: System should be supported with AI software/tools to assist the legal department across the contract review and drafting lifecycle, including but not limited to the following capabilities:

- Boiler plate clauses:** Auto-population/suggestion of standard boiler plate clauses (e.g. confidentiality, indemnity, limitation of liability, force majeure, governing law and dispute resolution, data protection/privacy, assignment, notices) appropriate to the nature and category of the contract being drafted, drawn from UBANK's approved clause library.
- Risk identification/flagging:** AI-assisted identification and flagging of missing, ambiguous, one-sided or non-standard clauses, and deviations from UBANK's approved templates/clause library, with an indicative risk rating (e.g. low/medium/high) to draw the reviewing lawyer's attention to areas of concern.
- Preferred clauses/terms and conditions:** Recommendation of preferred clauses and terms/conditions (e.g. payment terms, indemnity caps/liability thresholds, termination rights, service levels, penalties, warranties) based on the type/category of contract, nature of the counterparty, and previously negotiated/approved positions for similar transactions.
- Comparison and redlining:** AI-enabled comparison of counterparty-proposed drafts against UBANK's standard approved templates and legal playbook, highlighting clause-level deviations with supporting rationale/commentary for the reviewing lawyer.
- Clause library/precedent search:** A searchable clause library/precedent bank enabling the legal team to retrieve previously used and approved clauses/agreements for reference and re-use across similar transactions.
- Contract summarization:** Auto-generated executive summary of key contractual terms, obligations, risk exposure, and critical dates (e.g. renewal, termination, expiry) to expedite legal review.
- Human oversight:** All AI-generated content, suggestions, and risk flags shall be advisory in nature and subject to mandatory review, validation and final sign-off by an authorized member of the legal department before any contract is finalized/executed.
- Security and governance:** The AI tool(s) shall operate within a secure, access-controlled environment (with role-based permissions and complete audit logging of AI-assisted actions) and shall not result in any leakage of confidential/proprietary bank or counterparty data. Use of external/public AI tools/platforms for this purpose is not permitted unless approved by IS/Risk.

D. REQUIREMENTS IN EXECUTION OF ELECTRONIC CONTRACTS

#	LEGAL REQUIREMENTS	ACTION
1.	e-documents / contracts will be considered original where reliable assurance can be placed on the authenticity and integrity of the e-document.	Security procedures to be put in place to ensure integrity and authenticity of e-documents. See key considerations at point 6 below.

2.	Electronic signatures are recognized under Pakistan law.	For security procedures relating to e-signatures see key considerations at point 6 below.
3.	At present no stamp duty required for e-contracts. However provincial governments may put a procedure in place to pay stamp duties electronically.	No action required at present, however system should have capability to make stamp duty payments electronically as and when such stamp duty requirement is put in place.
4.	Advance electronic signatures are allowed for e-contracts.	Advance electronic signatures must meet the following requirements: It uniquely identifies its signatory. Private key used to create signature is under sole control of signatory. If data / contract tampered with after being signed the signature must identify this tampering. Signature should be invalidated if its accompanying data / contract has changed. Must be accredited by a reputable certification provider.
5.	e-contracts and e-signatures are admissible as evidence.	To ensure admissibility and legal validity of e-contracts and e-signatures adequate security procedures must be put in place.
6.	Security procedures	Security procedures as per best industry practices must be identified and set out. Also confirm whether these procedures are adequate. Security procedures must be updated from time to time to ensure that e-contracts and e-signatures have their integrity intact and remain authentic. Security procedure, as per law, means: a procedure which: (i) is agreed between parties; (ii) is implemented in the normal course by a business and which is reasonably secure and reliable ; or (iii) in relation to a certificate issued by a certification service provider, is specified in its certification practice statement; for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security device.

3.2 - Litigation Management Solution

1. Case Lifecycle Management

- End-to-end management of litigation from **pre-litigation, filing, trial, appeal, till final disposal**
- Centralized case repository with **unique case IDs**
- Categorization by:
 - Case type (Civil, Criminal, Recovery, Tax, Labor, Constitutional, etc.)
 - Jurisdiction (District Courts, Banking Courts, High Courts, Supreme Court, Tribunals)
 - Case status (Filed, Pending, Stayed, Decided, Executed)

2. Party & Stakeholder Management

- Database of:
 - Plaintiffs / Defendants
 - Borrowers / Customers
 - Employees / Ex-employees
 - Government Authorities (FBR, NAB, FIA, SBP, etc.)
- Linking multiple cases to the **same customer, employee, or account**
- Counsel-wise mapping (internal & external lawyers)

3. Court & Jurisdiction Mapping

- Court-wise configuration:
 - Court name & type
 - Bench / Judge details
 - Jurisdiction & territorial limits
- Case allocation to:
 - Trial Courts
 - Appellate Courts
 - Special Courts / Tribunals

4. Hearing & Calendar Management

- Automated hearing schedules
- Alerts & reminders for:
 - Hearing dates
 - Filing deadlines
 - Compliance dates
 - Limitation periods
- Integration with email/SMS notifications
- Adjournment tracking and hearing history

5. Document & Evidence Management

- Secure digital repository for:
 - Pleadings
 - Court orders
 - Notices

- FIRs
- Affidavits
- Version control and document history
- Access control based on roles

6. External Counsel Management

- Panel lawyer database
- Case assignment & workload monitoring
- Performance metrics:
 - Success ratio
 - Disposal timelines
 - Cost efficiency
- Fee structure & billing terms
- Invoice submission, verification & approval workflow

7. Financial Exposure & Provisioning

- Case-wise financial tracking:
 - Claim amount
 - Decretal amount
 - Contingent liability
 - Provisioning status
- Recovery tracking:
 - Amount recovered
 - Executions & settlements

8. Risk Assessment & Case Analytics

- Legal risk scoring (Low / Medium / High)
- Case aging analysis
- Trend analysis (increasing/decreasing litigation)
- Heat maps for:
 - Branch-wise litigation
 - Product-wise disputes
 - Employee-related cases

9. Workflow & Approval Mechanism

- Configurable workflows for:
 - Case filing approvals
 - Settlements & compromises
 - Appeals filing decisions

10. Reporting & Dashboards

- Real-time dashboards for:
 - Total cases (pending/decided)
 - Financial exposure
 - Recovery status
 - Counsel performance
- MIS reports for:

- Management
- Board & Committees
- Regulators & Auditors
- Exportable reports (Excel, PDF)

11. Knowledge Management

- Repository of:
 - Judgments
 - Legal opinions
 - Precedents
 - SOPs & legal manuals
- Searchable case law database

Litigation & Dispute Management

- End-to-end **litigation management module**.
- Unique litigation/case number and complete case profile.
- Court/tribunal, case number, jurisdiction and case type.
- Plaintiff/defendant/respondent/applicant details.
- Case value and **total financial exposure**.
- Principal, markup/profit, penalties, costs and potential liability.
- Case status, stage and ageing.
- Assigned internal lawyer and responsible business owner.
- External counsel details and case allocation.
- Hearing diary with previous and upcoming hearings.
- Automated alerts for hearing dates and required actions.
- Court orders, judgments, pleadings and evidence repository.
- Limitation-period and legal-deadline tracking.
- Appeal and execution proceedings tracking.
- Settlement workflow and settlement approval.
- Recovery following judgment/settlement.
- Case closure and closure reason.

3.3 - Reporting Requirements

- a) Comprehensive list of all active partnerships and commercial agreements
- b) Logs/reports of contract initiated/executed
- c) User level MIS of approvals/pending arrangements
- d) Report on current status of contract tenures/expiry dates
- e) Bifurcation of contracts by business unit owner, type of contract, and counterparty(ies)
- f) Listing of agreements with high risk or non-standard clauses inserted in any contracts
- g) Consolidated Listing of pricing inserted as part of any contract or annexures

3.4 - General Requirements – Applied to both, Contract and Litigation Management Modules

Legal Matter Management

- Central **Legal Request/Matter Intake** module.
- Categorization of requests: contracts, opinions, notices, litigation, regulatory, corporate, employment, recovery, etc.
- Assignment of matters to individual lawyers.
- Matter-wise SLA/TAT tracking.
- Matter ageing and escalation.
- Legal opinions/advice repository.
- Searchable legal precedents and previous advice.
- Linkage between legal advice, contracts, litigation and counterparties.

External Counsel Management

- Approved panel counsel database.
- Counsel expertise/jurisdiction.
- Cases assigned to each counsel.
- Counsel performance and outcome tracking.
- Counsel fees/retainers and budgets.
- Invoice submission and approval.
- Fee vs budget monitoring.
- Counsel SLA/performance evaluation.
- Conflict-of-interest declarations.

Financial / Risk Management

- Financial exposure tracking for each litigation matter.
- Provision/accounting status.
- Recovery tracking.
- Settlement amount vs original claim.
- Amount waived, including principal/markup/costs where applicable.
- Litigation exposure dashboard.
- Materiality/risk classification.
- Escalation of high-risk/high value matters to senior management/Board.

Notices & Deadlines

- Legal notices received and issued.
- Date of receipt/service.
- Response deadline.
- Responsible lawyer/business owner.
- Automated deadline reminders.
- Escalation for overdue responses.

- Linkage of notice to relevant contract/litigation/matter.

Document & Evidence Controls

- Complete document history/version control.
- Immutable audit trail.
- Document integrity/verification.
- Download/print/access logs.
- Legal Hold functionality.
- Evidence preservation once litigation/dispute is initiated.
- Controlled retention
- Disaster recovery and backup requirements.

Reporting / MIS

- CLO dashboard.
- Litigation portfolio dashboard.
- Contract portfolio dashboard.
- Pending Legal matters and ageing.
- SLA/TAT breaches.
- Upcoming hearings/deadlines.
- Expiring/renewing contracts.
- High-risk contracts and deviations.
- Litigation exposure/provisions/recoveries.
- External counsel performance and fees.
- E& Board-level reporting for **material litigation and legal risks**.

AI Enhancements

- AI-assisted litigation/case summarization.
- Chronology generation.
- Court-order/judgment summarization.
- Identification of action items/deadlines from orders.
- Similar case/precedent search.
- Litigation risk/exposure analysis.
- Contract-to-litigation linkage.
- AI-assisted legal research, subject to Legal validation.

4. Non-Functional Requirements

4.1 - Performance & Scalability

- a) **Response Time:** The system should be highly responsive. Common operations should be instantaneous under normal and high loads. The UI should be designed to load data asynchronously where possible to avoid locking the interface. The details for response times are elaborated in the SLA section of this document.
- b) **Scalability:** The service architecture should be scalable horizontally to handle increased workload.
- c) **Batch Processing Windows:** In case of any batch jobs are run (like nightly data sync to the data lake, or model training jobs), they should be designed to complete within non-peak hours and not interfere with daytime operations. Any long-running tasks should be asynchronous and not lock user-facing functions.

4.2 - Security

This section sets out the security, audit, integrity, legal validity and resilience characteristics required of the System(s). These requirements apply to the System as a whole and to every component delivered under this RFP.

- a) **Security:** The System shall provide adequate security commensurate with the confidentiality of the contract and litigation records held.
- b) **Authentication & Authorization:** Only authorized users may be able to access the solution(s). Integration with Ubank's Single Sign-On (SSO) or Active Directory for user login is required, enforcing strong authentication with two-factor security. Role based Access Controls (RBAC) must be implemented.
- c) **Data Encryption:** Data in transit and in rest must be encrypted (HTTPS for web access, secure API calls with TLS). For storage data in rest (such as customer sensitive data (PII) in the database), it must be encrypted or hashed as appropriate.
- d) **Session Security:** User sessions should forcefully be timed out after a period of 10 minutes of inactivity (or as per Ubank policy) to prevent unauthorized use. The system should have protections against common web vulnerabilities (SQL injection, XSS, CSRF attacks, etc.). Use of a modern web framework and security testing is expected.
- e) **Audit & Compliance:** The system must maintain a detailed audit log of user activities for at least a period of 5 Years. These logs must be tamper-proof. Administrative actions (like changing an SLA or deleting a ticket) should require higher privileges and must also be logged.
- f) **Penetration Testing:** Before go-live, the system must undergo security testing (vulnerability scan and penetration testing) to ensure no critical vulnerabilities exist. Any issues found must be remediated.

- g) **Compliance Standards:** Align with any specific standards U Bank adheres to, such as PCI DSS (if card data is involved), ISO 27001 for ISMS, or SBP's IT Governance guidelines for banks. PCI compliance would be necessary.

4.3 - Reliability & Availability

- a) **Availability:** Target SLA components are mentioned in the SLA section of this annexure. Any maintenance windows should be planned in off-peak hours and communicated, and ideally zero-downtime deployment techniques are used for updates.
- b) **Failover & Redundancy:** The service provider must ensure that the system should be deployed in a redundant setup with no single point of hardware or software failure. If the primary data center fails, the service provider must use their secondary / DR (Disaster Recovery) site to restore service within the bounds of SLA defined in this document.
- c) **Disaster Recovery (DR):** Recovery Time Objective (RTO) and Recovery Point Objective (RPO) should meet Ubank's business needs as per defined SLA in this document.
- d) **Error Tolerance:** The system should handle expected error conditions gracefully. For example, if any integrated system is down, the system(s) should not crash.
- e) **Supportability:** Provide adequate logging inside the application for debugging issues. This includes logs for API calls, background job processing, etc., which can be turned on for troubleshooting. Also ensure there's a mechanism to capture user feedback or error reports if something goes wrong on the front-end (like a user can report an issue or the system sends an automatic error report).

4.4 - Compatibility

- a) **Browser Compatibility:** The web-based application(s) should support the latest versions of common browsers used in Ubank's environment (such as Chrome, Edge, Safari, Firefox etc.). It should degrade gracefully on older versions or at least clearly notify if a browser is not supported.
- b) **OS & Device Compatibility:** The proposed system must be compatible with Windows PC and Macintosh machines and their latest associated operating systems (Windows 11 and MacOS Golden Gate). However, the system must be backward compatible with older variants of these operating systems.
- c) **Screen Resolution:** Design for at least Full HD resolution while being responsive to higher resolutions (such as 4K monitors) and devices with lower resolution (such as phones and tablet screens).

5. Technology and Information Security Requirements

1. Information and Cyber Security Requirements:

- a. The solution must comply with all financial industry standard security requirements.
- b. Solution must adhere to Ubank's Information Security standards, attached in **Annexure-B: Compliance Sheet**, named **"Information Security"** to this RFP document.
- c. Solution must adhere to any other security guidelines by State Bank of Pakistan and / or Ubank's Information Security department, that are made public and intimated by Ubank before the sign-off of design phase.

2. Change Requests:

- a. Vendor must submit a change request (CR) man-day rate with financial proposal, that will be agreed and locked for 5 years TCO. This CR man-day rate will be used to implement change requests once the project is fully delivered.

3. Logging:

- a. The solution must provide detailed logging at all layers and components.
- b. The logging level at individual layer must be configurable based on various levels of logging (e.g. information, debug, error, critical, etc.).
- c. Logging level for each layer / component must be independently configurable.
- d. All sensitive data must be logged with strong but standard encryption techniques.
- e. A comprehensive logging solution document must be provided with details of fields being logged and other configurations.
- f. A responsive and efficient user interface must be provided for searching through logs for individual transactions (correlated at all layers) using various fields.
- g. The log searching UI must have provision of roles and privileges to be assigned to different users of the UI.
- h. The solution must be able to integrate with SIEM for centralize monitoring of application authentication and privileged accounts' activities logs.

4. Configuration Hub:

- a. Vendor's solution must have a UI based backend Configuration Hub, which will be used by backend operations teams to make changes to the items that are configuration based for the mentioned solution.
- b. No configuration item (CI) is allowed to be updated through backend data base scripts / jobs. All CIs must have a UI based configuration screen in the Configuration Hub.
- c. Vendor must propose proper hierarchy and flow of CIs in the Configuration Hub for all functional use cases implemented in the Configuration Hub.
- d. All updated CIs must be validated through the maker-checker-publisher process.

5. User Interfaces:

- a. In general, all user interfaces must be fully responsive and available for PC screens, tablets, and mobile phones.
- b. All UIs must support roles and privileges that can be assigned to various users.
- c. All UIs must use Ubank's Active Directory for authentication.
- d. All UIs must support make and checker control, for change in configuration item (CI) relevant to UI.
- e. All UIs must provide proper logging of actions being taken through that UI, for accounting and audit purposes.

6. Documentation:

- a. The vendor must provide detailed documentation on the architecture (such as, but not limited to: High Level Diagrams, Low Level Diagrams, Project Plan, Method of Procedure documents, Testing Plan, FAQs, User Manuals), and implementation of the solution.
- b. Documentation must contain details of the architecture, including logical and physical architecture, deployment architecture and integration architecture.
- c. The documentation must also carry runbooks for various activities in setting up the foundation for the solution, e.g. setting up a new platform, fine tuning and optimization guide, troubleshooting and debugging guide, etc.
- d. The solution documentation must be provided in the form of a wiki / live document, instead of static word / pdf documents.

7. Integration Architecture & Requirements:

- a. The platform must expose standard APIs and integration interfaces to support integration with Ubank's. The vendor must clearly define the integration architecture, supported protocols, and API framework within the proposed solution.
- b. Complete details of APIs offered by the bidder.
- c. The bidder shall be responsible for designing and providing custom APIs if required for integration with Ubank systems.
- d. Vendor shall be responsible for all integrations with Ubank's existing solutions via standard APIs.
- e. All integration and required transformation and translation of data must be executed through industry standard enterprise service bus.
- f. The solution must provide compatibility of integration with multiple other components and third-party applications through standard (SOAP, REST, JSON, XML, HTTP, JMS, TCP/IP, etc.) and custom integration protocols.
- g. Integration architecture must support both sync and async integration along with hybrid models.

8. Security Architecture:

- a. The solution must comply with all financial industry standard security requirements.

- b. The solution must adhere to Ubank's Information Security standards, attached in "UMBL Information Security Controls".
- c. Solution must adhere to any other security guidelines by State Bank of Pakistan and / or Ubank's Information Security department, which are made public and intimated by Ubank before the sign-off of design phase.
- d. Vendor must ensure static code review and submit results with each iteration.
- e. In case of a separate user front end (including mobile applications, web portals, etc.) must comply with standard security practices for such channels, that includes below but not limited to:
 - 1. Commercial code obfuscation
 - 2. Integrity check
 - 3. Root and Jailbreak checks
 - 4. Emulator Checks
 - 5. SSL pinning
- f. In case of full digital journey, all security checks must be implemented to ensure no spoofing / manipulation / man-in-the-middle attacks can be executed to break the system.
- g. Vendor must allow for escrow agreement, as per SBP's guidelines, for this solution.

9. Trainings:

- a. Post 1st cutover, Vendor must set up agile framework for introducing new features in the solution.
- b. The vendor must execute first two sprints of at least two months each, with Ubank's resources in shadow mode.
- c. Ubank will execute the next two sprints of at least two months each, with Vendor's resources in oversight and handholding mode.
- d. Vendor must provide a detailed training and transition plan at the start of the project, for transitioning implementation artifacts to Ubank's relevant teams and configuration / customization training of Ubank's resources. The training and transition plan should also ensure Ubank's resources are equipped with necessary skills to undertake Operations of the production platform from day-0.

10. Hyper Care Period:

- a. The bidder must provide **06 months of Hyper Care period post go-live**, where close monitoring and onsite support to Ubank shall be provided by the bidder to handle teething issues.
- b. In Hypercare period, vendor will be responsible for managed operations as well as incident management, all under Ubank's team's supervision.
- c. Vendor must agree to Hyper Care period SLA, with penalties in case of breach of SLA.
- d. Hyper Care period will start from signoff of full 1st production deployment by Ubank.

11. Warranty and Support:

- a. The bidder must share a comprehensive Support Structure plan as part of their proposal.
- b. Vendor/Bidder must **provide 5 years of Local and OEM warranty and support backed by the SLA defined this RFP document**, without any additional cost, for all proposed components (software, license, services etc.) delivered as part of the solution.
- c. Completion of 1st year's warranty period will be the last financial milestone and percentage of that cannot be any less than 10% of the total contract value (TCV).
- d. The warranty period will require SLA based incident resolution; penalties would be applicable in case of SLA breach.
- e. The successful bidder shall be required to submit performance guarantee bond, tied to a specific percentage on total contractual value (TCV).
- f. Warranty period will start at sign-off of Hyper Care period by Ubank.
- g. The commercials for warranty and support must be submitted in bifurcated form (i.e., per annum)
- h. Any / all operational and incident support services pertaining to the solution(s) offered must be provided locally and onsite (if required or deemed necessary by Ubank)

i. Lifecycle Management, Bug Fixes, & Product Roadmap Stewardship:

As part of the support services, the vendor is strictly obligated to handle all software release cycles, which must include:

1. **Continuous Improvement:** Deployment of major and minor releases and hotfixes at no cost to Ubank.
2. **Major Roadmaps:** Upgrades to all new major product versions.
3. **Bug Resolution:** Obligation to resolve any technical bugs or performance bottlenecks discovered within the solution according to severity level definitions within a defined timeframe.

12. Documentation:

- a. Vendor/Bidder must provide detailed documentation on the architecture and implementation of the solution.
- b. Documentation must contain details of the architecture, including logical and physical architecture, deployment architecture and integration architecture.
- c. The solution documentation must be provided in the form of a wiki / live document, instead of static word / pdf documents. Vendor/Bidder may choose to provide documentation in Jira Confluence or any other similar tool.

13. General Implementation Principles:

- a) Vendors must provide detailed implementation methodology, with tangible and measurable criteria for sign-off of each implementation phase.

- b) Post 1st cutover, vendor must propose an agile approach along with establishing a rapid Continuous Integration - Continuous Development (CICD) pipeline.

14. Testing Phases:

- a) Vendors must complete the standard test phases (unit testing, integration testing, user acceptance testing, performance testing, vulnerability testing and full-dress testing).
- b) All test cases must be provided on live documentation platforms such as live wiki, along with the results. No word or PDF documents of test cases will be acceptable.
- c) **Unit Testing:** Vendor must provide detailed unit testing results for all functionality, along with proper screenshots and evidence, via live documentation platforms such as live wiki.
- d) **Integration Testing:** Vendor must provide detailed integration testing results to validate the integrations. In case no test environment for a third party is available or access to third party is not possible, vendors must develop stubs / mocks for bi-directional calls. Detailed test cases for integration testing and results of integration testing along with evidence (logs, screenshots, videos, etc.) must be shared by the vendor via live documentation platforms such as live wiki.
- e) **User Acceptance Testing:** Before UAT kickoff, Ubank will provide detailed list of UAT cases via live documentation platforms such as live wiki. Vendors must execute all UAT cases before formally calling out UAT. UAT results along with evidence (logs, screenshots, videos, etc.) must be uploaded by vendor on JIRA, before formal UAT by Ubank can be started.
- f) **Performance Testing:** Vendor must execute at least 1 cycle of performance testing before production cutover. Detailed performance test cases, test results and summary outcome of performance testing cycle(s) will be provided by the vendor via live documentation platforms such as live wiki. Performance testing results must comply with the load forecast provided by Ubank as part of this RFP.
- g) **Vulnerability Assessment / Penetration Testing (VA/PT):** Vendor must execute VA/PT cycles on the solution and all integrated layers, using standard VA/PT toolset, to be arranged by the Vendor. Ubank will also execute VA/PT cycles on all components using its toolset. Vendor is responsible to close all critical, high, medium and low anomalies / vulnerabilities identified in any component of the solution, before going live.

15. Configuration Management:

- a. All source code / scripts / implementation will be property of and in the ownership of Ubank.
- b. The vendor must set up a configuration management function at the start of the implementation.
- c. All development by the vendor must be performed in the development environment, with nightly code check-in.

- d. Ubank team will build the implementation artifacts using the checked-in code, on nightly basis. Vendor must ensure that nightly build is not broken.
- e. For any new deployment on test / pre-prod or production environment, either nightly build or on-demand build prepared by Ubank's configuration management team will be deployed by Ubank's team on the relevant environment.
- f. Vendors will not have access to any environment other than development environment.

16. Change Request Framework

a. Change Request Process

1. Ubank will raise a formal BRD for the change request that needs to be implemented. BRD formal document will be raised which requires customization and / or development. No BRD will be raised for configurational changes.
2. For each BRD, Vendor will come up with detailed functional specifications document (FSD).
3. Ubank will provide sign-off on the FSD.
4. Once FSD is signed off, Vendor will provide effort estimates along with calendar schedule.
5. Ubank and Vendor will mutually agree on the effort estimates and on the calendar schedule.
6. Post this agreement, Vendor will start implementation.
7. Vendor will offer the CR for UAT along with detailed internal test cases and associated results.
8. The UAT will follow the "Acceptance Criteria" defined below.
9. Once UAT is ACCEPTED, Vendor will provide the deployment schedule, which needs to be agreed with Ubank.
10. The CR will be considered CLOSED after 45 calendar days of successful and complete post-deployment hyper care period.

b) Change Request UAT Acceptance Criteria

1. The acceptance testing of any change request is based on the UAT execution results. This will be considered successful when all 100% test cases based on change request requirements have been executed and 100% of the test cases have been marked passed by Ubank.
2. Ubank has the right to override the UAT acceptance criteria and mark it successful, even if 100% UAT test cases have not been executed or 100% UAT test cases have not passed. In this case, both Ubank and Vendor must first agree on a schedule to address all incidents observed during UAT. The schedule upon mutual agreement can go beyond the production deployment.

3. In case all test cases related to change request (and its impacted areas) are not successful, Ubank can reject the change request. Ubank also has the right to reject the change request based on quality and performance of the work delivered, provided these requirements are part of functional specifications and UAT plan. If a change requested is rejected by Ubank, the subject change request will not be moved into production.

c) Change Request Process Penalties

1. In the build delivered by the Vendor for UAT, if any of the provided UAT cases fail that were previously marked as passed during Vendor's internal QA, such failure shall be considered a breach of the Development SLA.
2. On each such verified breach, Ubank may impose penalties, the %age of which will be agreed with the Vendor in the Contract.
3. For a period of 45 days post production deployment of a change request, if an incident occurs that is solely because of the changes made by the Vendor, Ubank has the authority to impose penalties to recover the financial and/or reputation loss due to this incident.

6. Service Level Agreement (SLA)

The proposed solution must be backed by a robust Service Level Agreement (SLA) covering, but not limited to, the following aspects:

1. **Availability:** Guaranteed uptime percentage of **99.99% (or higher)**, excluding scheduled maintenance.
2. **Incident Response, Restoration & Resolution Times:** The vendor must commit to the following maximum timelines for SLA:

Incident Severity	Coverage	Response Time	Restoration Time	Resolution Time	Target Thresholds
Severity 1	24 x 7 (including public holidays)	< 30 minutes	< 4 hours	< 2 calendar days	99%
Severity 2	24 x 7 (including public holidays)	< 1 hour	< 8 hours	< 4 calendar days	97%
Severity 3	Workdays	< 1 workday	< 3 workdays	< 6 workdays	95%
Severity 4	Workdays	< 2 workdays	< 5 workdays	< 10 workdays	90%
Technical Query	Workdays	< 24 hours	Best possible effort	Not Applicable	

Table 1: SLA for Incident Support

Severity Level	Description
Severity 1 – Critical Issue	Essential Business Process or Workgroup affected – any highly critical system or service outage that result in loss of defined business processes and/or capabilities, and for which there is no workaround acceptable to Ubank (availability of workaround renders it “High”)
Severity 2 – High Issue	Part of an Essential Business Process or Workgroup affected - Degradation of system or service performance that impacts end user service quality or significantly impairs business process control or operational effectiveness, but for which there is a workaround acceptable to Ubank.
Severity 3 – Low Issue	Part of essential/Non-Essential Business Process or Workgroup or Individual affected and can be replicated with discrete steps – Minor degradation of system or service performance that does not have any impact on end user service quality.
Severity 4 – Other Issue	A low-level priority defect that cannot be replicated, is caused by corruption in data, or has other non-software related cause
Technical Query	A query regarding technical information regarding a feature implemented

Table 2: Severity Level Definitions

Time Span	Description
Response Time	Response time is defined as the elapsed time between the vendor receiving the support request and formal acknowledgement of the request by the vendor back to the Ubank.
Restoration Time	Restoration time is defined as the elapsed time between response time and successful restoration of the service, by temporary or permanent fix or workaround, as confirmed and agreed by Ubank.
Resolution Time	Resolution time is defined as the elapsed time between restoration time and successful deployment of a permanent fix for the reported incident.

Table 3: Time Span Definition

3. Vendor shall be required to immediately escalate material security incidents to UBank and provide periodic updates until closure.
4. **Performance:** Bidder to define & share metrics for system response times and UI responsiveness, report generation etc. The
5. **Disaster Recovery:** The bidder must supply, deploy and configure a full-fledged Disaster Recovery (DR) site at U Bank Disaster Recovery DC to ensure seamless services, SLA compliance and automatic services shifting to DR in case any outage at primary site.
6. **Support Channels:** Availability of 24/7 support via multiple channels (phone, email, chat, dedicated portal).
7. **Data Backup & Recovery:** Bidder to share details on backup frequency, retention policies, and disaster recovery plans with defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
8. **Security Incident Response:** Bidder to define & share the process and timelines for responding to and notifying Ubank of any security breaches or incidents.
9. **Penalties:** Penalties shall be applied in case for failure to meet agreed-upon SLA targets.
10. **Reporting:** Regular performance reports on SLA adherence.
11. **Escalation Matrix:** The vendor must provide a clear escalation matrix for all issues, incidents, and change requests related to their provided solution. This matrix should outline the contact points and escalation paths within the vendor's organization.

Escalation Level	Role/Contact Person	Contact (Email/Phone)	Method	Response Expectation	Time
Level 1	Service Desk / L1 Support				
Level 2	Team Lead / L2 Support				
Level 3	Manager / L3 Support				
Level 4	Director / Executive				

12. Service and Website performance metrics:

Metric Category	Parameter	Target Threshold	Definition
Core User Experience	Largest Contentful Paint (LCP)	< 1.0 seconds	Measures loading performance. This is the time it takes for the largest image or text block to become visible within the viewport.
	Interaction to Next Paint (INP)	< 200 milliseconds	Measures interactivity. This metric assesses the delay from when a user interacts with the page (e.g., clicks a button) until the page visually responds. It has largely replaced First Input Delay (FID).
	Cumulative Layout Shift (CLS)	< 0.1	Measures visual stability . This checks how much the content unexpectedly shifts or "jumps around" during loading. A low score is better.
Server & Network	Time to First Byte (TTFB)	< 500 milliseconds	This measures how long it takes for a user's browser to receive the very first byte of data from the server after making a request. It's a key indicator of server responsiveness.
	Uptime / Availability	> 99.99%	This is the percentage of time the service is online and operational . This is a critical Service Level Agreement (SLA) metric.
	Error Rate	Less than 0.1% of all server requests.	The percentage of server requests that result in an error (e.g., HTTP 5xx server errors).

END OF DOCUMENT