Bidding Document

FOR THE DEVELOPMENT AND IMPLEMENTATION OF A COMPLAINT MANAGEMENT SYSTEM (CMS)

Issued By: Secretariat Provincial Ombudsman (Mohtasib) Sindh

RFB Issuance Date: 11th November, 2024

Proposal Submission Deadline: 27th November, 2024

Contact Information: Provincial Ombudsman (Mohtasib) Sindh Secretariat, Shahrah-e-Kamal Ataturk, Karachi; Ph +021-99211025

E-Mail: sindhmohtasib@gmail.com

Website: https://mohtasibsindh.gov.pk

Contents

1 Letter of Invitation

Location: Secretariat Provincial Ombudsman (Mohtasib) Sindh, Karachi
Date: 11th November, 2024

Dear Consultant,

The **Secretariat Provincial Ombudsman (Mohtasib) Sindh** invites your organization to submit a proposal for the design, development, and implementation of a **Complaint Management System (CMS)**. The goal of this system is to streamline the complaint handling process across various internal departments, enhancing transparency, accessibility, and accountability for citizens of Sindh.

The CMS must meet high standards of security, scalability, and performance. Specific details regarding the system architecture, features, and requirements are outlined in the **Terms of Reference** (Section 9).

1.1 Objectives of the CMS

- **Simplified Complaint Submission:** Accessible through a responsive web portal for easy access across devices.
- **Real-Time Complaint Tracking:** Provides complaint status updates with automated notifications via SMS and email.
- **Departmental Integration:** Ensures smooth routing, escalation, and resolution of complaints across intra (**Head office** and **19 Regional offices**) departments.
- **Analytics and Reporting:** Offers insights through dashboards to monitor complaint volumes, performance metrics, and response times.
- **Enhanced Cybersecurity:** Implements robust data protection measures aligned with ISO 27001:2022 and ISO 27701:2019 standards to safeguard sensitive citizen information and mitigate emerging threats.

1.2 Proposal Submission Guidelines

- Proposals must follow the structure outlined in Section 2 of this RFB and include both **Technical** and **Financial** proposals.
- **The selection method will follow a Single Stage – Two Envelope Procedure under 46 (2) of SPP Rules 2010.** We look forward to receiving your proposal and thank you in advance for your participation.

Sincerely,
Secretariat Provincial Ombudsman (Mohtasib) Sindh

2 Instructions to Consultants

2.1 Proposal Format and Structure

Section	Description	Required Document
Executive Summary	High-level overview of the proposal	Executive Summary Document
Technical Proposal	System design and architecture, methodology, and approach	Forms TECH-1 to TECH-8 (Section 9)
Financial Proposal	Cost breakdown and pricing structure	Forms FIN-1 to FIN-4 (Section 9)
Company Profile	Background and relevant experience	Company Profile Document
Relevant Experience	Past projects with international experience	Case Studies
References	Client references and testimonials	References Document
Warranty & Support	Post-implementation support and warranty	Warranty & Maintenance Plan

- **Deadline for Submission:** 27th November, 2024
- **Proposal Submission Address:** Secretariat Provincial Ombudsman (Mohtasib) Sindh, Shahrah-e-Kamal Ataturk, Karachi

2.2 Selection Criteria

The selection will be conducted through **Quality and Cost-Based Selection Method** using the following weightages:

Criteria	Weightage
Technical Proposal	80%
Financial Proposal	20%

Technical Evaluation Criteria

The evaluation will follow a **Single Stage – Two Envelope Procedure** in accordance with **46 (2) of SPP Rules 2010**, with proposals evaluated based on both technical and financial criteria. The **Technical Proposal** will carry the following score:

Criteria	Maximum Score	Qualifying Score
Technical Proposal	100	80

Evaluation and Proposal Opening Process

Bids will be evaluated in accordance with the Single Stage Two Envelope Procedure prescribed under Rule 46(2) of SPP Rules 2010 (Amended to date)

46 (2) Single Stage - Two Envelope Procedure

(a) bid shall comprise a single package containing two separate envelopes. Each envelope shall contain separately the financial proposal and the technical proposal;

(b) envelopes shall be marked as "FINANCIAL PROPOSAL" and "TECHNICAL PROPOSAL" in bold and legible letters to avoid confusion;

(c) initially, only the envelope marked "TECHNICAL PROPOSAL" shall be opened;

(d) envelope marked as "FINANCIAL PROPOSAL" shall be retained in the custody of the procuring agency without being opened;

(e) procuring agency shall evaluate the technical proposal in a manner prescribed in advance, without reference to the price and reject any proposal which does not conform to the specified requirements;

(f) no amendments in the technical proposal shall be permitted during the technical evaluation;

(g) financial proposals of technically qualified bids shall be opened publicly at a time, date and venue announced and communicated to the bidders in advance;

(h) financial proposal of bids found technically non-responsive shall be returned un-opened to the respective bidders; and

(I) bid found to be [Most Advantageous Bid], or best evaluated bid shall be accepted.

The qualifying score for the technical evaluation criteria would be 80/100. The technical proposals that score below 80 would be rejected and financial proposal of such firms would be returned unopened. Financial proposals of firms scoring 80 or above in technical evaluation criteria will be opened. **The bid found to be the Most Advantageous Bid shall be accepted on the basis of highest ranked in Quality and Cost-Based Selection Method using the afore-mentioned weightage.**

2.3 Instructions for Technical Proposal

The technical proposal must focus on the system's architecture, integration capabilities, security measures, and user experience.

Key Areas to Address:

- **System Design and Scalability:** Outline a flexible, scalable architecture to support future growth and efficient load management.
- **Cybersecurity Features:** Implement robust security and privacy measures to protect sensitive citizen data, ensuring compliance with ISO 27001:2022 and ISO 27701:2019

standards, with ISO 27701:2019 extending the Information Security Management System (ISMS) to include privacy management.

- **Responsive Web-Based UI Design:** Design a responsive, accessible user interface optimized for desktops, tablets, and smartphones.
- **Integration Capabilities:** Detail seamless integration with relevant systems.
- **Cloud Hosting:** Provide a locally hosted cloud solution that ensures high availability, robust security, and optimal performance. The local hosting requirement helps maintain data sovereignty, compliance with regional regulations, and improved latency, while still delivering strong security and performance guarantees.
- **Data Backup and Restore:** Ensure regular, secure data backups and a reliable recovery process to maintain data integrity.

3 Data Sheet

Item	Details
Project Name	Development and Implementation of Complaint Management System (CMS)
Procuring Agency	Secretariat Provincial Ombudsman (Mohtasib) Sindh
Bidding Process	Single Stage – Two Envelope
Bidding Process Details	1. Proposals must include two separate envelopes marked as "Technical Proposal" and "Financial Proposal." 2. Only the Technical Proposal envelope will be opened initially and evaluated based on predefined criteria **Minimum Qualification Marks: Technical 80** 3. Proposals not meeting the specified minimum technical requirements will be rejected. Amendments to the technical proposal are not permitted during evaluation. 4. The Financial Proposal of technically qualified bids will be opened publicly at a pre-announced time, date, and venue, while financial proposals of non-compliant technical bids will be returned unopened. 5. Bid found to be Most Advantageous Bid shall be accepted.
Proposal Submission Deadline	27th November, 2024
Bid Security	**2% of the proposal amount in PKR** in the name of "DDO Secretariat, Provincial Ombudsman (Mohtasib) Sindh Karachi" in the form of either a "CDR" or "Pay Order" or "Demand Draft" or "Bank Guarantee".

Performance Security	**5% of the total contract value in PKR** in the name of "DDO Secretariat, Provincial Ombudsman (Mohtasib) Sindh Karachi" as a "Bank Guarantee".
Proposal Validity	60 days
Completion Time (Estimated)	180 days (from commencement)
Proposal Submission Address	Secretariat Provincial Ombudsman (Mohtasib) Sindh, Shahrah-e-Kamal Ataturk, Karachi
Contact for Clarification	021-99211025

4 Terms of Reference (ToR)

4.1 Objectives

The **Complaint Management System (CMS)** will be developed to manage the lifecycle of complaints submitted by citizens, from registration to resolution. The system will provide a unified platform for complaint handling, escalation, tracking, and analytics.

4.2 High-Level Scope of Work Overview

Phase/Module	Description	Workflow Actions
Complaint Submission	Users submit complaints via a responsive web portal (desktop, tablet, smartphone), with multi-lingual support (English, Urdu, Sindhi). Secretariat Provincial Ombudsman (Mohtasib) Sindh officers can create cases manually if needed. The form allows office selection, complaint categorization, location details, and includes customizable fields (e.g., dropdown values, file size limits).	- **User Action**: Citizen submits complaint. - **CMS Action**: System validates inputs, assigns unique ID, and sends acknowledgment via SMS/email.
Complaint Categorization & Assignment	Complaints are categorized by department, issue type, or other predefined criteria and assigned based on role-based access control to the relevant department or officer.	- **CMS Action**: Categorizes complaint and assigns it to the relevant department/user based on roles. - **Notification**: Assigned officer receives notification via SMS/email. - **Role-Based Assignment**: Ensures appropriate handling based on access levels.
Complaint Resolution	Authorized users (Department and Ombudsman) view and manage complaints by status (Open, In Progress, Completed, Closed). They can assign issues, adjust status or priority, add resolution details, and access uploaded documents. Feedback can be forwarded to improve the knowledge base and aid in future decisions.	- **User Action**: Officer reviews complaint, processes it, or escalates if needed. - **CMS Action**: Updates complaint status in real time; logs each step in the timeline; pushes updates to any integrated systems for cross-platform consistency.

Tracking & Escalation	System tracks complaint progress and triggers escalation if processing delays exceed defined thresholds.	- **Aging Mechanism**: CMS monitors processing timelines, activating alerts if time limits are exceeded. - **Escalation Trigger**: Automatically escalates unresolved complaints to higher authorities, with notifications to the appropriate officials.
Notification System	Provides automated notifications (SMS/email) to users and staff on status updates and key actions.	- **CMS Action**: Sends notifications at each stage of the complaint lifecycle, updating relevant parties on status changes or actions required.
Analytics & Reporting	Real-time dashboards for KPIs, complaint aging, and performance metrics across departments. Department users can view personalized dashboards and reports to monitor individual and department-wide complaint resolution.	- **CMS Action**: Generates and updates reports, enabling data-driven insights into complaint handling and resolution metrics. - **User Action**: Department officers can access their own dashboards and reports to view pending complaints and performance data.
Department Officers Registration	Role-based registration and administrator approval for department officers to ensure secure and controlled access to the system.	- **CMS Action**: Approves officer registrations and assigns roles to define access permissions within the CMS.
Role-Based Access Control	System access levels based on role (e.g., administrators, department officers, citizens) for secure access and data protection.	- **CMS Action**: Restricts or grants access to system features and data based on user roles.
Testing & UAT	User Acceptance Testing (UAT) and internal testing of developed features to validate functionality and gather feedback.	- **User Action**: Assigned users test the system and provide feedback on feature performance. - **CMS Action**: Records feedback and addresses any issues before final deployment.
Final Resolution & Closure	Once complaints are resolved, they are marked as closed, with summaries provided to relevant parties.	- **User Action**: Officer marks complaint as closed and adds a resolution summary. - **CMS Action**: Generates final status report, sends closure notification to citizen, and, if necessary, escalates pending implementation actions to higher authorities. - **Audit Trail**: Logs all actions for transparency and future auditing.
		- **User Action**: Citizens are invited to provide feedback on complaint

Feedback & Archiving	Post-resolution feedback is collected from citizens; complaints are archived, and analytical data is generated for reporting.	resolution. - **CMS Action**: Records feedback, archives complaints, and compiles data for analysis to support system improvements.

4.3 Technology Stack

Layer	Technology
Frontend	**Angular** with the latest **Material Design** for a responsive, cross-device compatible UI
Backend	**Java (Spring Boot)** Microservices architecture for modular, scalable, and secure backend
Database	**PostgreSQL, MySQL** (for relational data), **MongoDB** (for unstructured data)
Security	**OAuth 2.0**, **JWT** (authentication), **AES-256 encryption** (data security)
Servers	Containerized deployment (Kubernetes / Docker)
Anti-Virus detection	Uploaded files to be scanned automatically and rejected in case of any discovery. User must be notified in real-time.
Audit Trails	Activity Logs to be stored on server, with monitoring and export options.
Project Management	Scrum framework, JIRA Issue Tracking
Version control	**Bitbucket** for source code management
Reporting and Dashboards	**Angular Material tables** with export options (CSV, Excel) and **Angular Charting Libraries** with drill-down capabilities for detailed insights

4.4 Integration Requirements

The system should integrate seamlessly with existing internal systems and third-party services, such as email, SMS, and WhatsApp, for notification purposes.

4.5 Mobile App Integration

The web-based Complaint Management System (CMS) requires integration with the existing mobile app to ensure seamless functionality across platforms. The CMS must enable data synchronization, support complaint submission, and provide status updates via both the web portal and mobile app. This integration

will involve adjustments in the mobile app to align with the CMS workflows and data structures, ensuring consistent performance and usability.

Mobile App Adjustments

To facilitate integration, necessary adjustments in the mobile app should include:

- Compatibility updates to support CMS data models and structures.
- Alignment of complaint submission, tracking, and notification features with the CMS.
- Testing and optimization to ensure smooth interaction between the mobile app and the CMS.

These adjustments will ensure that the mobile app functions seamlessly with the newly developed CMS, providing users a consistent experience across both web and mobile platforms.

4.6 System Analysis, Design, and Customization/Development Deliverables

The Consultant **must** deliver the following:

- A detailed document of system architecture, covering software and hardware components, use cases, data flow diagrams, system diagrams, and wireframes.
- Comprehensive specifications of functional, non-functional, and technical requirements, including a full requirements list, system interface details, and an updated solution model.
- A fully designed prototype of the proposed system, to be reviewed and approved before development.
- Documentation outlining the testing strategy, objectives, test cases, scenarios, resources, and schedule to validate system functionality and performance.
- An end-user manual with instructions for effective system use and troubleshooting tips.
- An operations manual for system administrators, detailing operational procedures, maintenance guidelines, and configuration instructions.
- Complete, well-documented, and structured source code for the system.

4.7 Software Customization / Development

Agile and Scrum Frameworks: Bidders must demonstrate the ability to use Agile and Scrum methodologies for iterative development. This includes adaptive planning, evolutionary development, and a capacity for rapid and flexible response to change.

4.8 Affirm The Affidavit

Before the final submission of the complaint, the complainer will be required to affirm an affidavit, which serves as a formal declaration of the truth and accuracy of the information provided in the complaint. This affidavit will contain a set of standard legal clauses designed to ensure the authenticity and seriousness of the complaint.

5 Security and Compliance Requirements

Given the sensitivity of data and the need to protect citizen information, robust security measures are crucial to the successful implementation of the CMS. The selected company must ensure compliance with international security standards and implement proactive measures against cybersecurity threats.

5.1 Data Security Requirements

- **ISO 27001 and ISO 27701 Compliance:** The system must comply with **ISO 27001:2022** standards for information security management and **ISO 27701:2019** standards to ensure robust privacy management practices, specifically for handling Personally Identifiable Information (PII).
- **AES-256 Encryption:** All data must be encrypted at rest using **AES-256 encryption** and in transit using **SSL/TLS protocols** to safeguard against unauthorized access.
- **End-to-End Encryption:** Implement **end-to-end encryption** for sensitive communications, including complaint submissions and status updates via SMS and email, ensuring data confidentiality throughout its lifecycle.
- **Zero Trust Architecture:** Adopt a **Zero Trust model**, where every user, device, and connection are continuously authenticated and authorized before access is granted to any part of the system.
- **Data Masking and Tokenization:** To protect sensitive personal data, employ **data masking and tokenization** techniques during storage and transfer, aligning with both security and privacy standards to mitigate data exposure risks.

5.2 System Administration and Security Management

- **Dashboard Design**: Collaboratively create customized, data-driven dashboards tailored to user needs.
- **Report Configuration**: Establish standardized report formats and layouts for in-depth data analysis.
- **Automated Deployment**: Streamlined installation process for rapid system deployment.
- **Flexible Configuration**: Adaptable system settings to accommodate future integrations and evolving business requirements.
- **Change Control**: Structured change management to minimize downtime and reduce risk.
- **Role-Based Access**: Secure, role-based permissions to control system access effectively.
- **Activity Logging**: Maintain detailed user activity logs and audit trails for enhanced security and traceability.
- **Continuous Updates**: Regular security patches and updates to address potential vulnerabilities.
- **Compliance Tools**: Built-in support for compliance with industry standards and regulatory requirements.
- **Automated Backup**: Scheduled backups to safeguard against data loss.
- **Disaster Recovery and Redundancy**: Reliable recovery mechanisms and data redundancy to ensure business continuity.

5.3 System Performance and Scalability Requirements

- **High-Speed Transaction Processing**: Enables rapid, accurate database transactions, even during peak usage times.
- **Concurrent User Support**: Supports up to 100 simultaneous users with consistent performance.
- **Data Volume Handling**: Manages large data volumes efficiently while maintaining optimal performance levels.

- **Versatile Transaction Management**: Delivers reliable performance across diverse transaction types.

5.4 Data Initialization and Configuration Setup

- **Data Import and Migration**: Full data import or migration from existing datasets to the new system is outside the project scope.
- **Setup Requirements**: Only meta-data, configuration, user roles, and access permissions will be set up as part of this project.

5.5 Cloud Hosting and Network Infrastructure Requirements

- **Cloud Compliance and Infrastructure Policy:** The cloud infrastructure must fully comply with Pakistan's **National Cloud First Policy 2022** standards to meet essential requirements for data sovereignty, security, scalability, and cost-efficiency, suitable for public sector use. Key compliance elements include data residency within Pakistan, robust security aligned with **ISO 27001:2022** and **ISO 27701:2019** standards, cost-effective scalability, and interoperability to support future integrations and avoid vendor lock-in.

- **Cloud Hosting Setup:** The vendor must provide a comprehensive cloud environment, including domain setup, IP configuration, infrastructure security layers, and SSL certificates to ensure secure deployment. This setup should cover all installation, configuration, and security requirements.

- **Hosting Period:** The proposal should include an initial two-year hosting period to ensure a stable operating environment.

- **Uptime Guarantee:** Maintain a minimum of 99.98% uptime, supported by a Service Level Agreement (SLA).

- **Scalability:** The hosting solution must allow for seamless upgrades in bandwidth, storage, and computing power to accommodate evolving demands.

5.6 Technical Support and Maintenance

A two-year extended support and maintenance package, including cloud hosting, will be provided during the warranty period at no additional cost.

5.7 Privacy & Compliance

- **ISO 27701 Compliance:** The solution must adhere to **ISO 27701:2019** standards for privacy information management, along with any relevant local data protection regulations, ensuring robust privacy controls are integrated into the system.
- **Data Minimization:** Ensure that only necessary personal data is collected and processed, adhering to the principles of **data minimization** to reduce privacy risks and comply with ISO 27701 guidelines.
- **Data Deletion Requests:** Include mechanisms to facilitate users' ability to request data deletion, aligning with **ISO 27701** principles for managing personal data and responding to privacy requests.
- **Secure Data Anonymization:** Anonymize user data in non-production environments to protect privacy during testing and analytics, in compliance with **ISO 27001** and **ISO 27701** standards for data security and privacy.

5.8 Audit Logging & Monitoring

- **Comprehensive Audit Trails**: All user activities, data modifications, and system actions must be logged and accessible in real-time to authorized personnel.
- **Security Event Monitoring**: Implement real-time monitoring and alerting systems for suspicious activities, potential breaches, or security vulnerabilities, utilizing tools such as SIEM (Security Information and Event Management).
- **Immutable Logs**: Ensure audit logs are tamper-proof by using blockchain-based or other advanced logging mechanisms to maintain data integrity.

5.9 Threat Detection & Response

- **Advanced Threat Detection**: Deploy AI-driven threat detection systems that continuously monitor network traffic and user behavior to identify and respond to potential intrusions or cyberattacks.

- **Proactive Vulnerability Scanning**: Regularly perform vulnerability assessments, penetration testing, and code reviews to identify and fix weaknesses before they are exploited.

- **Multi-Factor Authentication (MFA)**: Implement MFA for all system administrators and users with access to sensitive data to ensure secure login processes.

- **Security Patching**: Regular security updates and patches must be applied promptly to all system components to minimize exposure to known vulnerabilities.

5.10 Incident Response and Business Continuity Plan

- **Incident Response Plan (IRP)**: The consultant must provide a detailed Incident Response Plan, outlining steps for identifying, managing, and mitigating security incidents. This includes communication protocols and designated teams for handling cyber threats.

- **Business Continuity & Disaster Recovery**: Implement a business continuity and disaster recovery plan to ensure that critical services remain operational in the event of a cyberattack or system failure. This includes data backup strategies, failover procedures, and recovery time objectives (RTO).

6 Hardware Requirement Assessment

To ensure cost-effectiveness and avoid redundant investments, it is imperative that the assessment of hardware requirements be conducted with a comprehensive understanding of the available resources within the Head Office and the 19 Regional Offices. The assessment will focus on determining the current capabilities and limitations of existing servers, storage devices, networking equipment, and other critical hardware components. The consultant will aim to leverage the existing hardware wherever possible, ensuring that already available resources are utilized efficiently to avoid unnecessary expenditure.

The selected consultant will be responsible for assessing and recommending the hardware required to support the CMS infrastructure. This includes both on-premises and cloud-based solutions as deemed necessary for the effective operation of the system.

Detailed Hardware Resource Inventory

Head Office:

- A complete audit of the hardware resources currently available at the Head Office will be conducted. This includes evaluating server capacity, storage solutions, network equipment, and user devices to determine if they can support the new system.

- The inventory will identify any gaps where additional resources are needed and will highlight areas where existing resources are sufficient.

Regional Offices:

- A similar audit will be conducted for each of the 19 Regional Offices. The consultant will assess the hardware resources currently deployed in these locations, such as:
  - Server infrastructure (if present)
  - Local storage solutions
  - Internet bandwidth and network capabilities
- The assessment will consider the specific needs of each regional office, which may vary based on the volume of complaints and the number of users.

Tailored Hardware Recommendations

- Based on the results of the hardware assessment, the consultant will provide a detailed report with tailored recommendations for hardware acquisition.

7 Hardware and Cloud Storage Requirements

The proposed system, designed for deployment with cloud storage, should meet the following specifications to ensure optimal performance:

7.1 Server Hardware Requirements:

RAM:

- Minimum: 64 GB for basic functionality with concurrent users.
- Recommended: 128 GB for handling heavy traffic and large datasets.

Cloud Storage:

- Minimum: 500 GB SSD-equivalent cloud storage for initial data capacity.
- Recommended: 1 TB SSD-equivalent cloud storage to support long-term scalability, accommodating large files and attachments.
- Scalability: Cloud storage should support flexible, on-demand scaling to accommodate future growth without performance disruption.

CPU:

- Minimum: 4-core CPU for basic operations.
- Recommended: 8-core CPU for complex processing and multiple integrations.

Load Balancing:

- Cloud-based load balancing is required to distribute traffic evenly, ensuring high availability and rapid response times under heavy loads.
- Automatic Failover: Load balancing must support automatic failover to redirect traffic if a server instance becomes unavailable.

Monitoring and Maintenance:

- **Cloud Monitoring Tools**: Integration with suitable monitoring tools for real-time tracking of system uptime, response times, and error rates.
- **Downtime Alerts**: Automated notifications for downtime or performance issues, sent to administrators via email or SMS.
- **Maintenance Plan**: A comprehensive plan covering regular updates, security patches, and optimizations to ensure efficient and secure operations.

These server requirements, combined with scalable cloud infrastructure, will ensure the system operates efficiently under anticipated load conditions and supports future growth.

7.2 User System Requirements

To ensure optimal performance and usability for end-users accessing the system via the web portal or the existing mobile app, the following minimum system requirements are recommended:

- **Operating System:** Windows 10 or macOS 10.13+ for desktops; Android 8.0 or iOS 12+ for mobile.
- **Processor:** Dual-core, 2.0 GHz or higher (desktop).
- **RAM:** Minimum 4 GB, recommended 8 GB for optimal performance (desktop).
- **Storage:** Minimum 10 GB free disk space for cache and temporary files (desktop).
- **Web Browser:** Latest version of Chrome, Firefox, Safari, or Edge.
- **Internet Connection:** Broadband with at least 2 Mbps download speed for seamless access, especially for large files.

8 Evaluation Criteria

The evaluation of the proposal will be based on a Single Stage – Two Envelope Procedure in accordance with Rule 46(2) of SPP Rules 2010. The technical proposal will carry a maximum score of 100 points, and a minimum of 80 points is required to qualify. The evaluation criteria for the technical proposal are detailed below.

Criteria	Score	Description
Technical Proposal		The technical proposal is the primary focus, covering all aspects of system design, functionality, and compliance.
System Design and Architecture • System Analysis: **2.5** • Design Architecture: **5** • Adherence to Technology Stack: **10** • Compliance Requirements: **5** • Hosting Infrastructure: **2.5** • Network Design: **5**	**30**	**System Analysis:** Evaluates the proposed system's requirements and functionality. **Design Architecture:** Reviews the structure, components, and relationships in the system's architecture. **Adherence to Technology Stack:** Assesses the solution's alignment with the designated technology stack. **Compliance Requirements:** Verifies compliance with relevant industry standards and regulations. **Hosting Infrastructure:** Assesses stability, scalability, and security of the proposed hosting solutions. **Network Design:** Evaluates network infrastructure design, focusing on connectivity and security protocols.
Cybersecurity Measures		

• Protocols and Standards: **10** • Access Controls: **2.5** • Threat Detection and Response: **2.5**	**15**	**Protocols and Standards:** Compliance with ISO 27001:2022 & ISO-27701:2019, industry standards for security. **Access Controls:** Strategies for managing access, including user permissions and secure authentication. **Threat Detection and Response:** Mechanisms to detect, analyze, and respond to security threats.
Integration & Interoperability • Intra Departments Integration: **10** • System Integration: **5** • Interoperability Standards: **5**	**20**	**Intra Departments Integration:** intra departmental integration functionality for smooth complaint escalation and resolution across head office and 19 regional offices. **System Integration:** Evaluates the system's capacity to integrate with third-party applications, databases, and platforms. **Interoperability Standards:** Ensures compatibility with third-party APIs and industry standards for smooth operations.
Project Management Plan • Project Timelines: **6** • Risk Management: **3** • Quality Assurance: **3** • Reporting Frequency: **3**	**15**	**Project Timelines:** Detailed timeline for each project phase, showing clear planning and progress expectations. **Risk Management:** Identification of potential risks with defined mitigation strategies. **Quality Assurance:** Measures for quality control to ensure deliverables meet standards. **Reporting Frequency:** Effective reporting frequency provides regular insights into project milestones, potential risks, and any adjustments required.
Resume/CV of proposed Team Expertise & Composition • Relevant Experience: **5** • Technical Skills: **5** • Role Allocation: **5**	**15**	**Relevant Experience:** Considers experience in similar projects to ensure relevance to the current project. **Technical Skills:** Specific skills that are directly applicable to the project scope. **Role Allocation:** Defined roles and responsibilities for each team member, aligned with project requirements.

International Exposure • Cultural Competence: **2** • Regulatory Adaptability: **3**	**5**	**Cultural Competence:** Ability to work effectively within various cultural contexts, essential for international projects. **Regulatory Adaptability:** Experience with adapting to different regulatory environments, demonstrating flexibility.
Total Score	**100**	
Qualifying Score	**80**	
Financial Proposal		Cost effectiveness and budget alignment, ensuring the proposal offers the best value for money.

9 Forms and Timelines for Submission

Timeline Template (Agile with SCRUM Framework): The following timeline outlines a 6-month project plan using Agile Scrum. Before starting Sprint 1, a thorough hardware assessment must be completed to evaluate and leverage existing resources within the Secretariat Provincial Ombudsman (Mohtasib) Sindh. This assessment ensures that all necessary infrastructure requirements are identified, supporting smooth progress throughout the project.

Sprint	Activity	Duration	Start Date	End Date
Sprint 1	Requirements Gathering & Backlog Creation. Gather and refine requirements, create the product backlog, prioritize tasks using WSJF.	1 week	[Insert Date]	[Insert Date]
Sprint 2	System Design & Architecture. Draft system architecture, technical specifications, and user stories.	1 week	[Insert Date]	[Insert Date]
Sprint 3-5	Development Iteration 1 (Core Features). Begin development of high-priority features from the backlog.	9 weeks	[Insert Date]	[Insert Date]
Sprint 6-8	Development Iteration 2 (Advanced Features). Continue development, refine backlog, build and test advanced features. Complete the intra departmental integration functionality for smooth complaint escalation and resolution across head office and 19 regional offices.	9 weeks	[Insert Date]	[Insert Date]
Sprint 9	Testing & UAT (First Release). Perform initial testing and user acceptance testing for the first set of developed features.	1 week	[Insert Date]	[Insert Date]

Sprint 10-12	Development Iteration 3 (Additional Features). Continue developing additional features based on backlog prioritization.	3 weeks	[Insert Date]	[Insert Date]
Sprint 13	Testing & UAT (Second Release). Perform testing and UAT for second set of features, fix bugs and gather feedback.	1 week	[Insert Date]	[Insert Date]
Sprint 14	Deployment & Go-Live. Final preparations, deployment of the solution, and go-live support. **User training, manuals, tutorials and an FAQ Document.**	1 week	[Insert Date]	[Insert Date]

Consultant Team Composition Form

The table below outlines the proposed team composition for this project. Each role is tailored to meet specific project requirements, with a detailed description of each team member's expertise and experience, along with their expected duration of engagement. This structure is designed to ensure comprehensive coverage across all project phases and deliverables.

Name	Role	Expertise and Experience	Duration (Months)
[Name 1]	Project Manager	8+ years in project management, specializing in cross-functional team coordination and project delivery within scope and budget.	Full Duration
[Name 2]	Lead Developer	6+ years in Java development, skilled in backend frameworks, scalable architecture, and software design patterns.	Full Duration
[Name 3]	Security Expert	5+ years in compliance and security, specializing in risk assessment and cybersecurity protocols	Security Phase
[Name 4]	UI/UX Designer	5+ years in web and application design, with expertise in user-centered design and prototyping.	Design Phase
[Name 5]	Integration Specialist	5+ years in external systems integration, proficient in API management and third-party service connections.	Integration Phase
[Name 6]	DevOps Engineer	5+ years in CI/CD processes and cloud deployment strategies, experienced with automation tools and infrastructure as code.	Deployment Phase
[Name 7]	Database Administrator	5+ years managing PostgreSQL, MySQL, and MongoDB, focused on database optimization and maintenance.	Full Duration

[Name 8]	Penetration Tester	5+ years in vulnerability assessment, skilled in penetration testing and network security analysis.	Security Phase
[Name 9]	Compliance Officer	5+ years in regulatory compliance, specializing in ISO 27701 and ISO 27001 standards.	Full Duration
[Name 10]	Business Analyst	5+ years in requirements gathering and stakeholder management, ensuring alignment with project objectives.	Initial Phase

9.1 Technical Proposal Forms

FORM TECH-1: Technical Proposal Submission Form
27th November, 2024

To: Secretariat Provincial Ombudsman (Mohtasib) Sindh

Dear Sir/Madam,

We, the undersigned, offer to provide consulting services for the development and implementation of the Complaint Management System (CMS) in accordance with your Request for Proposal (RFP). We hereby submit our technical proposal, which includes the required forms, detailed work plans, and compliance with security standards.

We confirm that all information contained in this proposal is accurate and that we are in full agreement with the terms and conditions outlined in the RFP.

Sincerely,
[Authorized Signature]
[Name of Signatory]
[Title]
[Name of Consultant]
[Address]
[Phone Number]
[Email Address]

FORM TECH-2: Consultant's Organization and Experience

Consultant's Organization: Provide a brief description of your company, including the year of establishment, type of organization (corporation, partnership, etc.), areas of expertise, and relevant certifications (e.g., ISO 27001, ISO 27701 compliance).

Consultant's Experience: List projects your firm has undertaken, especially in the field of complaint management systems or other high-security systems. Include project details like scope, client, and results achieved. Highlight any international projects and renowned clients.

Project Name, Client Duration, Description of Project Outcome/Results, Contact Person

FORM TECH-3: Consultant's Team and CVs of Key Personnel

Provide detailed CVs of key consultants and team members who will be directly involved in the CMS project. Each CV should include the individual's qualifications, relevant experience, certifications, and roles in previous projects related to complaint management systems or high-security environments.

FORM TECH-4: Approach, Methodology, and Work Plan

Provide a detailed description of your proposed approach and methodology for the CMS project. This should include the following:

1. **Understanding of Objectives**: Explain your understanding of the goals and objectives of the CMS project.
2. **Methodology**: Describe the overall methodology for delivering the project, including how you plan to meet the technical, security, and integration requirements.
3. **Work Plan**: Provide a work plan that outlines major activities, milestones, and timelines.

Activity, Duration (Weeks), Start Date, End Date, Remarks

FORM TECH-5: Team Composition and Task Assignments

Provide the details of the team members who will be involved in this project, including their roles and expertise.

Name, Role, Expertise and Experience, Duration on Project, Responsibilities

FORM TECH-6: Project Management Plan

Submit a project management plan, which includes:

- Roles and responsibilities
- Key deliverables
- Risk management and mitigation strategies
- Communication plan with stakeholders
- Quality assurance measures

FORM TECH-7: Cybersecurity Plan

Outline the cybersecurity measures you will take to ensure the security and integrity of the CMS, including:

- Data encryption strategies
- Access control mechanisms
- Incident response plan
- Threat detection and response capabilities
- Compliance with ISO 27001 and ISO 27701
- Regular vulnerability assessments and penetration testing

FORM TECH-8: Compliance with the Terms of Reference (ToR)
Confirm that your technical proposal fully complies with the Terms of Reference outlined in the RFP. Mention any deviations or exceptions, if applicable.

9.2 Financial Proposal Forms

FORM FIN-1: Financial Proposal Submission Form
27th November, 2024

To: Secretariat Provincial Ombudsman (Mohtasib) Sindh

Dear Sir/Madam,

We, the undersigned, offer to provide consulting services for the development and implementation of the Complaint Management System (CMS) in accordance with your Request for Proposal (RFP). We hereby submit our financial proposal, which includes all costs associated with the project, including development, training, and maintenance services.

Our total financial proposal amount is [Insert Amount] inclusive of all taxes and duties.

Sincerely,
[Authorized Signature]
[Name of Signatory]
[Title]
[Name of Consultant]
[Address]
[Phone Number]
[Email Address]

FORM FIN-2: Breakdown of Costs

A. Development Costs

Provide a detailed breakdown of the costs associated with the development phase, including design, system integration, and testing.

Description	Unit Cost	Quantity	Total Cost
Design & Architecture	[Insert Cost]	[Insert Quantity]	[Insert Total]
Development	[Insert Cost]	[Insert Quantity]	[Insert Total]
System Testing	[Insert Cost]	[Insert Quantity]	[Insert Total]
Security Implementation	[Insert Cost]	[Insert Quantity]	[Insert Total]

B. Training Costs
Provide a detailed breakdown of the costs associated with training users and administrators.

Description	Unit Cost	Quantity	Total Cost
User Training	[Insert Cost]	[Insert Quantity]	[Insert Total]
Admin Training	[Insert Cost]	[Insert Quantity]	[Insert Total]
Training Materials	[Insert Cost]	[Insert Quantity]	[Insert Total]

FORM FIN-3: Payment Schedule

Propose a payment schedule based on the following milestones:

Milestone	Payment Percentage	Amount
Hardware requirement assessment and Completion of System Design & Architecture	10%	[Insert Amount]
Deliverables: Completion of **Sprint 1** and **Sprint 2** activities: requirements gathering, backlog creation, system design and architecture.		
Completion of Core Development Phase	20%	[Insert Amount]
Deliverables: Completion of **Sprints 3-5**: Development of core features, culminating in the first prototype.		
Completion of Advanced Development & Testing Phase	30%	[Insert Amount]
Deliverables: Completion of **Sprints 6-8:** demonstrating the development of advanced features, refinement of functionalities, and alignment with project requirements to showcase feature completion. Complete the intra departmental integration functionality for smooth complaint escalation and resolution across head office and 19 regional offices.		
Completion of Testing, UAT, and Final Deployment	35%	[Insert Amount]

Deliverables: Completion of **Sprints 9-14**: Testing (First and Second Release), additional feature development, final deployment, and go-live support, **user training, manuals, tutorials and an FAQ Document.** **Risk Management Plan:** Addressing potential risk during the project lifecycle, including but not limited to: Project Delays, Security Risks, Integration Challenges		
Post-deployment Support	5%	[Insert Amount]
Deliverables: Support and maintenance during the initial warranty period after deployment. The system must come with a 24-month warranty period, during which the consultant will provide free-of-cost support for any defects or malfunctions found in the CMS.		

FORM FIN-4: Additional Costs

Include any additional costs, such as third-party licenses, hosting fees, and compliance certifications, if applicable.

Description	Unit Cost	Quantity	Total Cost
[Insert Description]	[Insert Cost]	[Insert Quantity]	[Insert Total]

10 Deliverables and Milestones

The selected consultant is expected to deliver the following at various stages of the project. Prior to initiating Sprint 1, a comprehensive hardware assessment must be conducted to evaluate and optimize existing resources within the Secretariat Provincial Ombudsman (Mohtasib) Sindh.

Sprint	Deliverable	Description	Timeline
Sprint 1	Requirements Document	Submission of a detailed project plan, work breakdown structure, and timeline	End of Sprint 1
Sprint 2	Design Documentation	System architecture diagrams, database schema, and API specifications, reflecting the system design and technical framework	End of Sprint 2
Sprints 3-5	Prototype	A functional prototype demonstrating core system components and high-priority features	End of Sprint 5
Sprints 6-8	Advanced Development	Development of additional features and refinement of backlog based on iterative feedback. Complete the intra departmental integration functionality for smooth complaint escalation and resolution across head office and 19 regional offices.	End of Sprint 8

Sprint 9	Beta Version	Beta release for initial testing, including user acceptance testing for the first set of features.	End of Sprint 9
Sprints 10-12	Additional Feature Development	Development of additional features and continued backlog prioritization	End of Sprint 12
Sprint 13	Testing & UAT (Second Release)	Completion of second round of testing, user acceptance testing, bug fixes, and feedback gathering	End of Sprint 13
Sprint 14	Final System & Feature Completion. Deployment & Go-Live	Finalized system addressing remaining backlog items, ready for deployment preparation. Full deployment of the CMS, go-live support, **user training, manuals, tutorials and an FAQ Document.**	End of Sprint 14
Post Go-Live	Post-Implementation Support	Two years of extended support and maintenance, including cloud hosting under the warranty period, at no additional cost	Starting immediately post-deployment

11 Training and Knowledge Transfer

The consultant will be required to provide comprehensive training to both technical and non-technical staff, covering:

- **System Administration**: How to manage and configure the CMS.
- **User Training**: How to navigate and use the system for daily operations.
- **Technical Training**: For in-house IT staff to handle system maintenance, upgrades, and troubleshooting.
- **Deliverables include training manuals, video tutorials, and an FAQ document. All training sessions must be recorded and made available for future reference.**

12 Post-Implementation Support and Maintenance

- **Service Level Agreement (SLA)**: The consultant must propose an SLA to ensure timely response and resolution to any system issues post-deployment. This should include:
  - Response Time: 2 hours for critical issues, 24 hours for minor issues.
  - Resolution Time: 72 hours for critical issues, 5 days for minor issues.
  - The system must come with a 24-month warranty period, during which the consultant will provide free-of-cost support for any defects or malfunctions found in the CMS.

13 Risk Management Plan

The consultant must submit a risk management plan addressing potential risk during the project lifecycle, including but not limited to:

- **Project Delays**: Outline strategies to mitigate delays in requirements gathering, design, or development.
- **Security Risks**: Address potential data breaches, hacking attempts, and security vulnerabilities, including preventive measures.
- **Integration Challenges**: Risks related to integration with existing ERP and third-party systems, along with proposed solutions.

The risk management plan should be periodically updated as the project progresses.

14 Quality Assurance Plan

The consultant is required to submit a quality assurance (QA) plan, which should cover:

1. **Testing Strategy**: Detail unit testing, integration testing, user acceptance testing (UAT), and stress testing.
2. **Test Cases**: Provide a list of test cases covering all system modules and features.
3. **Bug Reporting**: Set up a system for reporting, tracking, and resolving bugs throughout the testing phase.
4. **Performance Metrics**: Outline metrics to ensure the system meets performance benchmarks, including load handling, response times, and uptime.

15 Intellectual Property Rights

The intellectual property (IP) for the CMS, including the source code, design documents, and other deliverables, will be owned by the Secretariat Provincial Ombudsman (Mohtasib) Sindh. The consultant will not have the right to use or share the IP without prior written consent.

16 Ethical Considerations

The consultant must ensure compliance with the following ethical standards:

- **Data Privacy**: Guarantee that all personal data is handled in accordance with the highest privacy standards.
- **No Conflict of Interest**: Consultants must declare any potential conflicts of interest in their proposal.

- **Non-Disclosure Agreement (NDA)**: The selected consultant will be required to sign an NDA to protect sensitive information shared during the project.