Request for Proposal

Selection of Service Provider for Design, Development & Implementation and Operation of Online Recruitment Management System (ORMS) for Odisha Staff Selection Commission (OSSC), Government of Odisha

RFP No.: OCAC-SEGP-SPD-0029-2024-25048

Vol-II Terms of Reference

ODISHA COMPUTER APPLICATION CENTRE

[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]

OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India

W: www.ocac.in | **T**: 0674-2567295/2567283 | **F**: 0674-2567842

Table of Contents

1 Background

The **Online Recruitment Management System (ORMS)** project is an initiative by the **Odisha Staff Selection Commission (OSSC)** to digitize and streamline the recruitment process for Group-C & Group-B posts in the state. The project, developed by the **Odisha Computer Application Centre (OCAC)**, aims to enhance transparency, efficiency, and security in recruitment activities.

The ORMS will provide a **centralized, automated, and technology-driven** platform for job requisition management, candidate registration, application processing, exam scheduling, admit card generation, result compilation, grievance redressal, and legal case management. It integrates **Aadhaar authentication, DigiLocker for document verification, and AI-based security measures**, ensuring compliance with regulatory requirements.

The system will also feature **a mobile application, web portal, and multi-channel communication** (via SMS, Email, and WhatsApp) to enhance accessibility for candidates. The project is expected to significantly improve the recruitment process by reducing manual intervention, ensuring data integrity, and providing a seamless experience for applicants and administrators alike.

1.1 CURRENT CHALLENGES

1. **Manual and Paper-Based Processes:** Traditional recruitment methods relied on manual paperwork, leading to inefficiencies, delays, and increased chances of errors.
2. **Lack of Transparency:** Candidates had limited visibility into application status, exam schedules, and selection procedures, raising concerns about fairness.
3. **Time-Consuming Recruitment Cycle:** The process of job requisition, application review, and result declaration was slow, delaying government hiring.
4. **Security and Fraud Risks:** Verifying candidate identities and handling sensitive data manually increased the risk of impersonation, document forgery, and data breaches.
5. **Grievance and Legal Case Handling Issues:** The absence of a structured mechanism for addressing grievances and court cases led to delayed resolutions and administrative burden.
6. **Logistical Challenges in Exam Management:** Scheduling exams, allotting centers, and managing invigilators manually was cumbersome and prone to errors.
7. **Inefficient Communication:** Lack of real-time updates through SMS, email, or mobile apps resulted in candidates missing crucial deadlines and notifications.

To overcome these challenges, OSSC adopted the **Online Recruitment Management System (ORMS)** with the aim of modernizing the recruitment lifecycle. The transformation leverages **automation, AI-based verification, Aadhaar integration, DigiLocker, and real-time communication** to ensure a **seamless, transparent, and efficient** process.

Key Benefits of Digital Transformation:

1. **Faster and More Efficient Recruitment:** Automating workflows reduces processing time for applications, exams, and results.
2. **Enhanced Transparency and Fairness:** Candidates can track their application status, exam schedules, and selection processes in real time.
3. **Improved Security:** Aadhaar authentication, DigiLocker integration, and AI-powered fraud detection ensure data integrity and authenticity.
4. **Seamless Grievance and Legal Case Management:** A dedicated system for handling candidate complaints and court cases ensures timely resolution.
5. **Better Exam Coordination:** Automated venue allocation, digital admit cards, and AI-driven attendance tracking streamline exam day operations.
6. **Real-Time Communication:** Candidates receive instant updates via **SMS, email, and WhatsApp**, reducing missed notifications and confusion.
7. **Scalability and Cost Savings:** Reducing paperwork and manual intervention lowers administrative costs while making the system adaptable for future recruitment needs.

1.2 SCOPE OF WORK

The primary objective of this project aims to revolutionize recruitment processes by providing a comprehensive and interconnected set of modules. These modules collectively contribute to creating a transparent, efficient, and user-centric recruitment experience for both organizations and candidates. The use of advanced technologies ensures accuracy, security, and compliance with legal and ethical standards throughout the recruitment lifecycle. The proposed system will provide the following broad items.

1. Pre-Exam Activity
2. Exam Day Activity
3. Post Exam Activity
4. Court Case Management System
5. Mobile Application for iOS and Android
6. Unified Recruitment Web Portal
7. Grievance Management System
8. Objection Management System

Project Scope in brief

The broad scope of work of this project includes the following details;

1. Design & development of Pre-Examination activity Modules
    a) Requisition by Departments
    b) Creation of Online Application Form (Including option/preference)
    c) Candidate One-Time Registration (OTR) System with Aadhaar-Based Authentication
    d) Filling of Job Applications by Registered Candidates
    e) Exam Venue Allotment
    f) Admit Card Generation
    g) Mobile App (Candidate Interface)
2. Design & development of Exam Day Activity Modules
    a) Attendance Management System
    b) Verification of Candidates
3. Design & Development of Post Exam Day Activity Modules
    a) Certificate Verification System for Candidates
4. Design & Development of Unified Recruitment Web Portal
5. Design & Development of Grievance Management System
6. Design & Development of Court Case Management System Module
7. Design & Development of Objection Management System

The bidder has to furnish approach and Methodology including platform details for software applications as well as hosting requirements in Technical Bid

2 Detailed Scope of Work

2.1 Design & Development of Pre-Examination Activity Modules

2.1.1 Requisition by departments

Job Requisition: This sub-module is used to create a new job requisition, which includes information about the open position such as job title, job description, and required qualifications, vacancy and reservation details, pay scale, service rules, etc.
Approval: Upon completion of new job requisition, the job requisition moves to the approval stage. Depending on the organization's hierarchy and policies, approval may be required from multiple levels, including department heads, HR managers, and executive leadership.

2.1.2 Creation of Online Application form

Form Builder: This sub-module allows the user to create an online application form, set up validation rules by dragging and dropping fields such as name, address, educational qualifications, experience, etc. into the form. The form builder should be easy to use and provide a range of customization options to fit the job notification.

Custom Fields: This sub-module allows the user to add custom fields to the online application form to collect specific information relevant to the job. For example, if the job requires the candidate to have a driving license, the custom field could ask the applicant if they have a driving license and the type of vehicle they can drive.

Form Preview: This sub-module allows the user to preview the online application form and make any necessary changes before publishing it. This will help to ensure that the form is clear, concise and easy to user.

Form Mapping: This sub-module allows the user to map the fields on the online application form to the job notification. This will help to ensure that the information collected on the form is relevant to the job and can be used to assess the applicant's suitability for the position.

Integration: This module enables the government department to integrate the online application form with their web portal. This is typically done by embedding the form's HTML code into the portal's web page or using a web page builder tool to add the form.

Customization: This module enables the OSSC to customize the design and layout of the online application form to fit their web portal's branding and style. This includes setting up a color scheme, adding a logo or banner, and adjusting the font and layout of the form.

Accessibility: This module ensures that the online application form is accessible and user-friendly. This includes optimizing the form for mobile devices, ensuring that the form is easy to navigate, and the questions are clear and concise.

Publication: This module enables the OSSC to publish the online application form on their web portal. This is typically done by creating a dedicated page on the portal for the job advertisement and linking the online application form to this page.

2.1.3 Candidate One Time Registration with Aadhaar-Based Authentication

Aadhaar Authentication: This module is responsible for verifying the candidate’s identity through Aadhaar authentication. The system will authenticate the candidate’s identity by sending a request to the UIDAI (Unique Identification Authority of India) server and retrieving the Aadhaar information and populate the same in the appropriate fields in the registration page.

- **Aadhaar Authentication**
    - Choose between:
        - OTP-based eKYC (most common)
        - Biometric (for in-person)
    - Redirect to UIDAI's Aadhaar gateway
    - Enter Aadhaar number → OTP sent to Aadhaar-linked mobile

- **Fetch Aadhaar Data**
    - Upon successful verification, fetch:
        - Name
        - DOB
        - Gender
        - Address (optional)
    - Autofill and lock these fields

Personal Details: Details captured through Aadhaar such as name, DOB, photograph cannot be modified by the candidates. System to allow modification of other fields receiving during Aadhaar authentication.

Education Qualification and Verification from Digi locker: This module captures the candidate’s educational qualifications, such as the name of the institution, the degree/diploma/certificate earned, and the year of passing. System to have provision for retrieving the educational details from digi locker account of the candidate. In case of the non-availability of verification from digi locker, system to enable manual entry of such details.

Work Experience: This module captures the candidate’s work experience, such as the name of the organization, the designation, the duration of employment, and the job responsibilities.
Upload Documents: This module enables the candidate to upload scanned copies of their educational certificates, experience certificates, and other relevant documents. System to have the provision to directly retrieve the document from candidates digi locker account and store the same.

Upload Documents: This module enables the candidate to upload scanned copies of their educational certificates, experience certificates, and other relevant documents. System to have the provision to directly retrieve the document from candidates digi locker account and store the same.

Declaration: This module requires the candidate to provide a declaration certifying that the information provided in the registration form is true and correct.

Verification: This module verifies the candidate's registration details by sending a verification code to their registered mobile number or email address. The candidate needs to enter the verification code in the system to complete the registration process. This module uses AI to verify the authenticity of the photo ID submitted by the candidates. The system can use OCR technology to read the information on the ID and verify its authenticity from the ID service provider.

Dashboard: This module provides the candidate with a dashboard where they can view their registration details, update their profile, and apply for job notifications.

2.1.4 Filling of Job Applications by Registered Candidates

Application Form: This module presents the application form to the candidate, which contains fields to enter the candidate's personal details, educational qualifications, work experience, and other relevant information.

Eligibility Check: This module verifies the candidate's eligibility for the job vacancy based on the criteria mentioned in the job description.

Document Upload: This module enables the candidate to upload scanned copies or fetched from digi locker (if available) of the required documents, such as educational certificates, experience certificates, and other relevant documents.

Candidate Exam Venue Preference: This sub-module allows candidates to select their preferred exam centres from the available options, based on their convenience and proximity to their location.

Application Review: This module allows candidates to review the application form and the documents uploaded before submitting the application.

Application Submission: This module enables candidates to submit the application form and the document uploaded to apply for the job vacancy.

Application Status: This module displays the status of the candidate's job application, including whether the application has been received, processed, or rejected.

2.1.5 Exam Venue Allotment

Exam Centre Creation: This module is responsible for creating new exam centres and updating the details of existing exam centres, including location, number of rooms, capacity of each room, and availability. The system to also captures the list of invigilators available in the centre.

Exam Centre Matching: This module is responsible for matching the candidate's preferences with the available exam centres, taking into account factors such as proximity, capacity, and suitability.

Exam Centre Allotment: This module is responsible for allotting the exam centres to the candidates based on their preferences and availability of the exam centres.

Room Allocation: This module is responsible for allocating exam rooms to the candidates; the system can allocate rooms based on the capacity of the room and the number of candidates assigned to each room.

Invigilator Management: This module is responsible for managing the invigilators assigned to each exam room. The system can assign invigilators based on their availability, experience, and location.

Scheduling: This module is responsible for scheduling the invigilators for the exam. The system can schedule the invigilators based on the exam schedule and their availability.

Communication: This module is responsible for communicating the room allocation and invigilator details to the candidates and the invigilators. The system can send automated emails or SMS messages to notify them of the details.

Communication Management: This module is responsible for communicating with the candidates regarding their exam centre allotment, including the exam centre address, date, and time, and any other relevant information.

2.1.6 Admit Card Generation

Admit Card Data Management: This module is responsible for managing the data related to admit card generation, including candidate details, test date, time, venue, and other relevant information.

QR Code Generation: Initially, relevant candidate and exam information would be encoded into a QR code format. This includes details such as candidate name, registration number, photograph, exam date, time, and venue.

Admit Card Design: This module is responsible for designing the admit card format, including the layout, color, font, and the QR codes are strategically integrated into the design layout of the admit cards. A dedicated section or space is allocated on the admit card for embedding the QR code, ensuring visibility and accessibility.

Admit Card Delivery: This module is responsible for making the admit card available in the candidate's dashboard for download, either through a website or mobile application. the admit card can be made available after verifying the authenticity of the candidate and can be protected by a secure login and password.

Admit Card Verification: This module is responsible for verifying the authenticity of the admit cards, to ensure that the candidate presenting the admit card is the same as the one who registered for the test.

2.1.7 Mobile Application (Android & iOS)

Candidate Interface: Candidate can view the registration details, download admit card or access e-Admit card, view results and can receive notifications related to exam.

2.2 Design & Development of Exam Day Activity Modules

2.2.1 Attendance Management System

Candidate Check-In: This module is responsible for checking in the candidates once they arrive at the exam centre. The system can verify the identity of the candidate as described above, and mark their attendance once they are cleared.

Candidate Check-Out: This module is responsible for checking out the candidates once they complete the exam. The invigilator marks the check-out time of the candidate in the system.

Record Keeping: This module is responsible for keeping a record of the attendance of the candidates. The system can generate a report that lists the attendance of each candidate, along with their identity verification details.

Automated Alerts: This module is responsible for sending automated alerts to the concerned authorities if a candidate does not check in or check out on time, or if there is any other unusual activity.

2.2.2 Verification of Candidates

Admit Card Details Verification: This module verifies the details of the physical admit card with the details available on the server.

ID Verification: This module uses AI to verify the authenticity of the photo ID submitted by the candidates. The system can use OCR technology to read the information on the ID and verify its authenticity from the ID service provider.

2.3 Design & Development of Post Exam Day Activity Modules

2.3.1 Certificate Verification System for Candidates

The system shall provide a digital platform for candidates to verify their examination certificates securely and efficiently. The system shall offer a user-friendly interface and intuitive system navigation to ensure ease of use for candidates during the certificate verification process. The system shall implement robust authentication mechanisms to ensure the authenticity and integrity of the certificates being verified. The system shall enable real-time verification of certificates, allowing organizations and employers to promptly validate candidates' credentials.

2.4 Design & Development of Unified Recruitment Web Portal

2.4.1 Unified Recruitment Web Portal

A unified recruitment web portal is proposed, where all the modules shall be integrated with the web portal to provide a unified and seamless user experience to candidates and other stakeholders of the ORMS applications.

2.5 Design & Development of Grievance Management System

A comprehensive end to end grievance management system proposed under ORMS to manage and provide timely resolution of grievances raised by different stakeholders of ORMS project.

2.6 Design & Development of Court Case Management System Module

Court Case Registration: This module is responsible for registering the candidates who file court cases against the exam. The system can store the details of each candidate, including their name, contact information, and the nature of the case.

Document Management: This module is responsible for managing the documents related to the court case. The system can store the court orders, legal notices, and other relevant documents related to the case.

Case Status: This module is responsible for tracking the status of the court case. The system can provide regular updates to the candidates about the status of their case.

Verification: This module is responsible for verifying the authenticity of the candidates who file court cases. The system can use an algorithm to verify the identity of the candidate and ensure that they meet the eligibility criteria specified in the job notification.

Registration Extension: This module is responsible for extending the registration deadline for the candidates who file court cases. The system can provide an interface for the candidate to submit their request for an extension, which can be reviewed by the examiners.

Communication: This module is responsible for communicating with the candidates regarding the court case and any updates related to the exam. The system can send automated emails and SMS messages to the candidates to keep them informed.

Re-Registration: This module is responsible for allowing the candidate to register again if their

application was rejected due to any discrepancies found during the verification process. The system can provide an interface for the candidate to submit their request for re-registration, which can be reviewed by the examiners.

Results Compilation: This module is responsible for compiling the results of the exam and assigning the candidates to their respective positions. The system can use an algorithm to compile the results based on the performance of the candidates in the exam.

Court Order Compliance: This module is responsible for ensuring that the court orders related to the exam are compiled with.

2.7 Design & Development of Objection Management System Module

Objection Question Map with Set: This module enables administrators to input and store information regarding question sets, including question numbers and relevant set details. It provides a centralized repository for organizing and mapping questions with set, facilitating efficient access and retrieval.

Objection by Candidate: Students can use this module to raise objections against questions they believe contain errors, inaccuracies, or ambiguities. They can submit details of the question and the nature of the objection, providing supporting evidence or reasoning where necessary. This module ensures transparency and fairness in addressing student concerns.

Track Questions: This module allows authorized users, such as administrators or instructors, to track individual questions across multiple question sets. Users can search for specific questions by question number or other criteria and view their occurrences in different sets. This functionality facilitates quality control, consistency checks, and content analysis across assessments.

2.8 Digi Locker Integration

Integrating with Digi Locker typically involves linking an online service or platform with the Digi Locker system, allowing users to access their documents and certificates stored in Digi Locker seamlessly. For the “Online Recruitment Management System” of Odisha Staff Selection Commission, integration with Digi Locker could enhance the user experience by providing a secure and centralized location for storing and sharing essential documents.

2.9 Integration with UIDAI

Integrating with the Unique Identification Authority of India (UIDAI) typically involves incorporating Aadhaar authentication services into a system or application. Aadhaar authentication allows for secure verification of an individual's identity using their Aadhaar number and biometric data. For the “Online Recruitment Management System” of Odisha Staff Selection Commission, the application needs to integrate with UIDAI to fetch details of the candidate which has been stored in the candidate’s Aadhaar.

2.10 Implementation of AI and OCR Technology

Implementation of AI to verify the authenticity of photo IDs submitted by the candidate. The system can use OCR technology to read the information on the ID and verify its authenticity from
the ID service provider. The system shall implement OCR technology to extract information from the photo ID submitted by the candidate. OCR can read text, numbers, and other relevant details from the document. The system shall integrate with a document authentication service that verifies the authenticity of IDs. The system shall develop an AI verification algorithm that analyzes the extracted information from the ID. The algorithm can check for security features, validate the format of the ID, and compare the information against databases to ensure it is consistent and valid.

2.11 Communication Channel via SMS, Email & WhatsApp

A communication channel through SMS, e-mail and WhatsApp should be facilitated in the proposed system which will be communicated to all the stakeholders.

2.12 Admin Console

User & Master Management
User creation
Tagging user types with User
Creating and managing the login credentials

Roles and Rights
Provide access rights to the users
Tagging of departmental users with respect to the designation and role
User access management
Assign roles and rights to the users

Technologies

As recommended by the Ministry of IT, Government of India on IT Policy, Open-Source technology willbeused for both software development and database design for the said application as per below:

2.13 DEVELOPMENT

The Service Provider shall identify, design and develop components / functionalities for the Application Portal and Mobile App that are required to address the proposed application requirements mentioned in this RFP. The Service Provider shall provide the following documents along with the developed components:

a) Business process guides

b) Data model descriptions

c) Dashboard designs

d) Sample reports

e) Frequently asked question (FAQ) guides

f) Source Code of bespoke application, if any with proper documentation

g) Any other documentation required for usage of implemented solution

The Service Provider shall implement a system for monitoring the SLAs and ensure that the system addresses all the SLA measurement requirements and calculation of applicable penalties as indicated in the document.

2.14 TESTING

The Service Provider shall design the testing strategy including Test Cases and conduct testing of various components. Application testing shall at least include unit testing, performance testing etc. At least the following activities will be carried out by the SP.

a) Ensure the solution meets all the functional & technical requirements as per the RFP including FRS.

b) Perform the testing of the solution based on the test plan, document the results and shall fix the bugs found during the testing.

c) Ensure that the integration aspects of the solution are successfully tested.

d) Connecting with multiple data sources, databases, their seamless integration etc. should be tested and verified.

The Service Provider needs to ensure that the end product delivered meets all the requirements of the implementation specified in this bidding document.

2.15 THIRD PARTY SECURITY AUDIT

a) The Service Provider needs to ensure that the solution follows the CERT-In Security Policy and Guidelines.

b) The Service Provider shall appoint CERT-In empaneled auditor who shall be responsible for performing the security audit of the solution.

c) The cost of audit & rectification of non-compliances shall be borne by the SP.

d) Carryout security audit before go-live of application and obtain the safe-to-host certification

e) Carry out the periodic audit & certification as and when it is required as per the

OSDC policy.

f) The audit shall be performed at least on the below mentioned aspects.

  - Accessibility Testing
  - Application Security Audit
  - Vulnerability Testing

2.16 SSL CERTIFICATION

The Service Provider shall carry out SSL certification.

a) Secure connection between Client and Server through Secure protocol HTTPS

b) Encryption of Data during transmission from server to browser and vice versa

c) Encryption key assigned to it by Certification Authority (CA) in form of a Certificate.

d) SSL Security in the application server

2.17 TRAINING

a) The Service Provider is required to undertake training of the Department Users.

b) Training would be done at State Headquarter in Bhubaneswar

c) OCAC will facilitate the training logistics.

d) The Service Provider shall set up the IT infra such as computer, network, LED, etc as required for providing the training in a successful manner.

e) The schedule / training calendar and the training material for imparting training shall be developed by the Service Provider in consultation with OCAC, and department officials. The Service Provider shall submit a hardcopy of the training material to OCAC before every training session.

f) In case of modifications, either in the training plans or substitutions of the regular trainers, proper communication with OCAC and Participating Department need to be made.

g) If required, the Service Provider may conduct the training in virtual mode.

2.18 TIMELINE

#	Project Component	o Tentative Deliverables	Timeline
1.	Requirement Study and Documentation	o Detailed Team Structure with team members o Point of Contact o FSR/SRS Document with screen prototypes and Prototype walkthrough	T+4 Weeks
2.	Approval	o Approval letter	T+5 Weeks
3.	Software Development, Testing, Deployment, Configuration	o Source Code o System Design Document o Test Plans & Test cases o Operation manual o Configuration Manual o Administration Manual o Security Policy document o FAQs o Hosting of Application in the staging environment o Load Testing report o Performance tuning parameters for fine-tuning applications on the server	T+16 Weeks
4.	User Acceptance Test & Trial Implementation	o Preparation Test Cases by Dept. with help of bidder o Conduct of UAT	T+18 Weeks
5.	Security Audit & Go live	• Auditor’s vulnerability report • Fixing vulnerabilities found during a security audit • Submit of safe to Host certificate by bidder. o Go live of the application on Production server.	T+24 Weeks=T1

6	Operation and Maintenance (AMC)	Provide Support Report	T1 + 12 Months
7	Deployment of Hand holding Resource	Quarterly Performance and support Report	T1 + 12 Months

2.19 DEPLOYMENT and CONFIGURATION

a) The Service Provider shall deploy the application / portal over the hardware infrastructure provided by the OSDC or any other infrastructure provided by OCAC.

b) The Service Provider shall be responsible for the end-to-end management of hosting and deployment of the application.

c) The Service Provider shall ensure deployment of the application as per the policy of OSDC.

2.20 UAT and GO-LIVE

After completion of the development work for application, OCAC will conduct the technical reviews of development work performed by the Service Provider as UAT. The Service Provider shall be responsible for:

a) Preparation and submission of test strategy, test cases and test results

b) Demonstration of module-wise functionalities/ features before the OCAC in staging environment

c) Support OCAC and its designated authority for conducting the testing and provide access of the systems as required by them.

d) Rectification in the application for any issues/ bugs/ and improvements/ Enhancements / up-gradations suggested Departments (if any) during the UAT without any additional cost.

2.21 DATA MIGRATION

The Data Migration to be performed by the Service Provider shall be preceded by an appropriate Data Migration Strategy & Methodology which is to be prepared by the Service Provider and approved by OCAC.

Data Migration should be carried out as per industry practice and all care must be taken to log in each error. The Service Provider should clearly define the data migration strategy in the proposal. The following activities will be carried out as part of the Data Migration:

a) Define all the specifications that are needed to populate the data into the new system

b) Prepare the Data cleaning and migration plan and submit to concern authority for approval.

c) Prepare uniform codification of all data sets

d) Identification, configuration or development of the data upload / download programs for the Data Migration

e) Ensure minimum business downtime at the time of data cleaning and migration

f) Ensure the accuracy and completeness of the migrated data

g) Ensure migration of all data is completed by the time of Go Live

h) Database of existing system would be migrated to the newly developed system

i) The Service Provider will be expected to understand the data which has been captured and devise a template so that meaningful information can be captured and entered into the new system

j) This template should have basic sanity check to prevent entry of incorrect information. E.g. numerals should not be allowed in patient name etc.

k) The application must have a provision to upload citizen data through Excel format by respective departments too.

2.22 AUDIT

i. The software and documents prepared for this project are subject to audit. The bidder should help OCAC during preparation of compliances of audit without any additional cost.

ii. Software including source code, licenses (if any) and all technical documents/manuals shall be in favour of OCAC and all records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

2.23 POST IMPLEMENTATION SUPPORT

2.22.1 Application Support

a) Fixing the bugs identified during the period

b) The defects will be covered, which occur due to development error(s), the subject of which appears in the requirements specification.

c) Minor changes to the business process will be addressed except new table, database etc.

d) Monitor application to ensure that the application does not suspend, hang etc.

e) Ensure the desired functioning of the Interface / integration

f) Ensuring uptime of the application developed

g) Ensure periodic backup and recovery of the Data

h) Perform Performance Tuning

i) Modification / improvisation of existing MIS reports

j) New software modules are not covered in this phase.

k) Quality audit compliance (if applicable)

l) Regular database maintenance activity

2.22.2 Operational Support

The Service provider will also provide one Technical Support Executive for handholding support for a period of 12 Months. The work profile of the resource are as follows.

a) Ensure the accuracy and timeliness of data uploaded as received

b) Resolve and report the data discrepancies to the designated OCAC persons

c) Submit document on the performance of the application on a quarterly basis

d) Provide handholding support

e) Present relevant information and impart training as applicable

f) Support for high level review meeting

The desired experience and qualification of the resource are as follows.

Position	Qty	Skill
Technical Support Executive	2	B.E./B.Tech/MCA/BCA/BSc(IT/Comp. Sc.) with working experience in e-Governance projects shall be preferred with working experience of minimum 2 years in IT Industry.

2.24 PROJECT MANAGEMENT

The envisioned project is a multi-disciplinary initiative. An effective project management plan and commitment to adhere to it is a mandatory requirement. The project plan should also include the resources, task and time plan for the entire duration of the project. The Service Provider shall employ best practices in project management methodology to ensure that the envisioned project components are developed and implemented within the defined time period. A copy of the project management plan shall be handed over to the department to keep track of the progress of the project

2.25 GUIDING PRINCIPLES

The proposed solution should adhere to the following principles.

2.24.1 Standards

a) The system architecture should be based on industry standards and protocols

b) The system will be centrally deployed and globally accessed

c) The system shall be designed to be scalable and easily extensible

d) The system should be flexible to cater to changing business, industry and compliance requirements (including reporting requirements in proper formats)

2.24.2 Application

a) All applications must consider appropriate security, performance, efficiency and maintainability issues.

b) The ownership of the product licenses would be with OCAC.

c) Upgrade to new releases should not become mandatory for the next three years from the date of installation.

2.24.3 Integration

The integrated solution design should include framework for integration of both internal and external applications and services using suitable architecture.

2.24.4 Data

a) Data will be owned, shared, controlled and protected as a corporate asset of the OCAC.

b) Data should only be accessed through application / interfaces to create, update and delete. There should not be any direct access to the data layer for users.

2.24.5 Data Security

a) The Service Provider shall provide a strategy to maintain data security at the application level

b) The Service Provider shall provide a strategy to maintain data security at the database level

c) The Service Provider shall provide a strategy to maintain data security at the messaging and middleware level

d) The Service Provider shall provide security strategies when the applications are accessed from outside the network or accessing resources outside the network.

e) The Service Provider shall provide strategies of encryption and security for external transaction with partner network and systems

2.26 ADHERENCE TO STANDARDS

The system shall comply with relevant defined industry standards (their latest versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to its design, development, security, installation, and testing. The suggested architecture must be scalable and flexible for modular expansion. It should ensure ease of integration with software / applications developed using common industry standards since the solution may be linked and connected to other sources (websites, contents, portals, systems of other user departments etc.) as well as there may be loose/tight integration with backend system of other departments depending on individual service processes. The solution architecture should thus have provision to cater to the evolving requirements of the Department.

A reference list of the minimum industry standards which the system components should adhere to is mentioned below:

Component	Standards
Information Access / Transfer Protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open Standards
Portal Development	W3C Specifications
Document encryption	PKCS specification
Information Security	ISO 27001 certified System
Operation	ISO 9001 Certified
Service Management	ISO 20000 specifications or latest
Project Documentation	IEEE/ISO Specifications for documentation
Data Standards	All-important data entities should be in line with standards published by MeiTY.

2.27 SECURITY, INTEGRITY CONFIDENTIALITY

a) ***Web Services Security:*** System shall comply to all the Web services including routing, management, publication, and discovery should be carried out in a secure manner. Those who are using the Web services should be able to utilize security services such as authentication, authorization, encryption and auditing. Encryption of data shall take place at client level itself. Application server shall provide SSL security.

b) ***Data Integrity and Confidentiality:*** Data integrity techniques need to be deployed to ensure that information has not been altered, or modified during transmission without detection. Similarly, Data confidentiality features are also to be applied to ensure that the data is only accessible by the intended parties.

c) ***Transactions and Communications:*** With respect to the Data Transactions and Communications, system needs to ensure that the business process are done properly and the flow of operations are executed in correct manner.

d) ***Non Repudiation Security*****:** The application shall have the Non-repudiation security services to protect a party to a transaction against false denial of the occurrence of that transaction by another party. End-to-End Integrity and Confidentiality of Messages The integrity and confidentiality of messages must be ensured even in the presence of intermediaries.

e) ***Database Controls*****:** The database controls for online transaction processing systems like access to database directly, access to database through application, access to log files, access by the remote terminals, DBA controls, backup policy and backup procedures.

2.28 EXIT PLAN

a) The selected firm will provide systematic exit plan and conduct proper knowledge transfer process to handover operations to OCAC technical team at least three months before project closure.

b) IT resource persons of OCAC will work closely with resource persons of the Service Provider at test, staging and production environment during knowledge transfer phase.

c) All knowledge transfer should be documented and possibly recorded.

d) The Service Provider will ensure capacity building of the IT resource persons of OCAC on maintenance of software and infrastructure.

2.29 PROJECT DOCUMENTATION

The Service Provider will share below list of documents to OCAC during the project contract period.

a) Latest version of Source Code

b) System Requirement Study Documents

c) High Level Design (HLD) / Low Level Design (LLD) documents including

- Application architecture documents
- ER diagrams and other data modelling documents
- Database design
- Application component design including component deployment views, control flows, etc.
- Application flows and logic

d) Test Plans and Reports

e) Issue Logs

f) User Manual

g) Application Installation & Configuration Manual

h) Report of Security Audit & Safe-to-Host Certificate

i) Any other documents defined under Timeline & Tentative Deliverables

j) All the above documentation should be done as per IEEE/ISO/CMM Standard

2.30 Service Level & Penalty:

The Service Provider shall agree to the following service level agreement (SLA) parameters while providing Contact Centre services. These SLAs shall be tracked on a periodic basis and are envisaged to have penalty and/or liquidation damage clauses on non-adherence to any of them. The Service Provider has to provide the SLA tool which will facilitate generating the SLA reports. The SLA parameters are divided into 2 (two) types: -

1. During implementation

In case of delay in implementation of the project as per the Delivery Schedule mentioned in the RFP/ PO/ Agreement, penalties shall be imposed as mentioned below:

a) In the event of delay in execution of work, specified in this Contract /furnishing of deliverables, the Service Provider shall be liable to a penalty @ 0.25% of the value of work order for the respective component/item, for delay of 15 days or part thereof, up to a maximum of 10%, after which OCAC shall be at liberty to take action against the Service

Provider as deemed proper (such as cancellation of order forfeiting of Performance Guarantee., increase of penalty percentage etc.)

b) Penalty will not be applicable, if the delay is not attributable to the SI. However, in such cases, the Service Provider has to communicate in writing the reason of delay. The decision of the Chairman, OCAC in this regard shall be final.

2. Post Implementation

a) Solution Uptime

The solution uptime shall be based on the overall performance of the hardware, application software, system software, where the uptime represents the percentage of time the system remains operational.
The uptime shall be calculated as follows:
Total uptime in minutes*100/ Total minutes of operations in a month.

Measurement Interval	Reporting Period	Target	Penalty
Daily	Monthly	>=99.5%	Nil
		>=98.7% but <99.5%	.5% of Quarterly billed value
		>=97% but <98.7%	1.0% of Quarterly billed value
		>=95% but <97 %	1.5% of Quarterly billed value
		<95 %	2.0% of Quarterly billed value

b) Reporting Procedures of SLA

The SI's representative will prepare and distribute Service level performance reports in a mutually agreed format by the 10th working day of the completion of each month. The reports will include "actual versus target” Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports will be distributed to Purchaser management personnel as directed by Purchaser. Discrepancies in the service levels shall be monitored as per Escalation matrix given below.

Escalation Matrix for Portal

Sl#	Designation	Position in escalation matrix (L 1/L2/L3)	Escalation Time/ Period
a)	Support Executive	L1	Escalation time period in case of issue with the application

Sl#	Designation	Position in escalation matrix (L 1/L2/L3)	Escalation Time/ Period
			management, Quality Analysis & Reporting
b)	Project Manager	L2	Escalation time period after 2 days in case of issue with application, Quality Analysis and Reporting
c)	Delivery Head/CTO	L3	Escalation time period after 3 days in case of issue with application, Quality Analysis and Reporting

3 Payment Terms

SL#	CATEGORY/ACTIVITIES	PAYMENT TERM
1.	Application Design, Development, Integration and Implementation of ORMS solution for OSSC as per SOW (Including Mobile App development)	• 20% of application development cost on approval of SRS. • 40% of application development cost on approval of UAT. • 30% of application development cost after declaration of Go-Live by OCAC/User Department.. • 10% After 12 months from the date of Go-live or submission of Performance Bank Guarantee of equivalent amount.
3.	Application Support and Software Maintenance for a period of one year.	QGR Payment. To be paid in 4 Installment on submission of quarterly status report.
4.	SSL Certificate for 1 Year	100% of the cost shall be paid after configuration of SSL in the Live Web application
5.	Third Party Security Audit	100% of the cost shall be paid on submission of Safe-to-Host certificate
6.	Handholding Support	To be paid in 4 equal Installment on submission of resource quarterly attendance report due signed by user department.