Aspire to Innovate (a2i)

Government of the People's Republic of Bangladesh

ICT Division

Agargaon, Dhaka

Terms of Reference

For

"Hiring a Firm for Enhancement and Maintenance of Doptor"

1. Background

The Government of Bangladesh is committed to modernizing its administrative ecosystem through the strategic use of information and communication technology (ICT) to enhance efficiency, transparency, accountability, and citizen-centric service delivery across public institutions. In alignment with this vision, the Doptor Platform is undergoing enhancement, support, and maintenance to address evolving institutional needs and to strengthen its role as a core enabler of effective e-Governance.

The platform is adopting necessary technological transformations, including secure audit services, application performance monitoring (APM), site reliability engineering (SRE) practices, e-Sign Gateway integration, secure identity and access control, and streamlined information-sharing mechanisms—aimed at enhancing operational efficiency, system reliability, and data-driven decision-making across government offices.

Secure identity management ensures that only authorized users can access information, protecting data integrity and confidentiality. In addition, the information mediator simplifies data exchange and communication across departments, reducing friction in day-to-day operations.

The successful rollout of this enhancement will significantly elevate the Doptor Platform's functionality and contribute to the broader e-Government transformation — enabling more efficient, responsive, and citizen-oriented public administration. In essence, this evolution marks a decisive step toward a modern, connected, and performance-driven government.

2. Review of the Existing System

2.1 About the Organization

Aspire to Innovate (a2i), a whole-of-government programme of ICT Division, supported by Cabinet Division and UNDP, that catalyzes citizen-friendly public service innovations, simplifying government and bringing it closer to people. It supports the government to be on the forefront of integrating new, whole-of-society approaches to achieve the society. The objective of the project is to increase transparency, improve governance, and reduce the time, difficulty and costs of obtaining government services for under-served communities of Bangladesh. This is to be achieved by the following 3 major components of the project:

Component 1: Institutionalizing Public Service Innovation and Improving Accountability

Component 2: Catalyzing Digital Financial Services and Fintech Innovations

Component 3: Incubating Private Sector-enabled Public Service Innovation

2.2 Review of the existing system

2.2.1 Overview of Doptor Platform

Doptor provide a wide range of data related to Bangladesh's geography and administrative information. This data is accessible to not only Bangladeshi citizens but also individuals and organizations both within and outside Bangladesh, including development partners and other

interested parties. By using this data anyone from Bangladesh all outside Bangladesh and development partners and other interested parties can get benefited they can get an insight about Bangladesh. They can get data from this platform such as Bangladesh GEO location, divisions, districts, upazilas, post offices, municipalities, city corporations, and thanas data within the platform. Furthermore, government employee information, including employee names in both Bengali and English. Also, Doptor facilitates the sharing of office-related data. The office data includes information such as office names in both Bengali and English, office IDs, ministry names, office layers, office unit names, officer unit organograms, and office designations.

2.2.2 How many services are offered by Doptor Platform?

Doptor serves the most authentic government officer information as well as their profile information such as employee name in Bangla, employee name in English, employee date of birth, employee NID, employee blood group, employee gender, employee phone number , employee alternative phone number, employee email address, employee fathers name in Bangla, employee fathers name in English, employee mothers name in Bangla, employee mothers name in English, employee joining date, employee batch id , employee cadre id , employee non cadre id , employee designation. employee signature, employee profile picture. for this data external application integrated with Doptor and Doptor serve the data with Doptor standard data sharing model.

Doptor platform also share the Offices data such as Office name in Bangla, office name in English, office id, office ministry name , office layer, office unit name, officer unit organogram , office designation and so on this data shared from Doptor platform to external application using Doptor standard data sharing model.

For SSO integration application, Doptor Platform provides the customizable login page to enhance user accessibility.

2.3.3 Doptor Ecosystem

Doptor Platform represents the actual application structure Doptor platform. In this diagram Doptor application is connected with SSO and SLO with WSO2 standard and the external applications have the only way to communicate with entire Doptor platform. Doptor API layer is connected through an industry standard API Gateway which ensures seamless communication at Doptor API Realtime data consumption from external application changes. The API gateway is monitoring the data flow as expected or not.

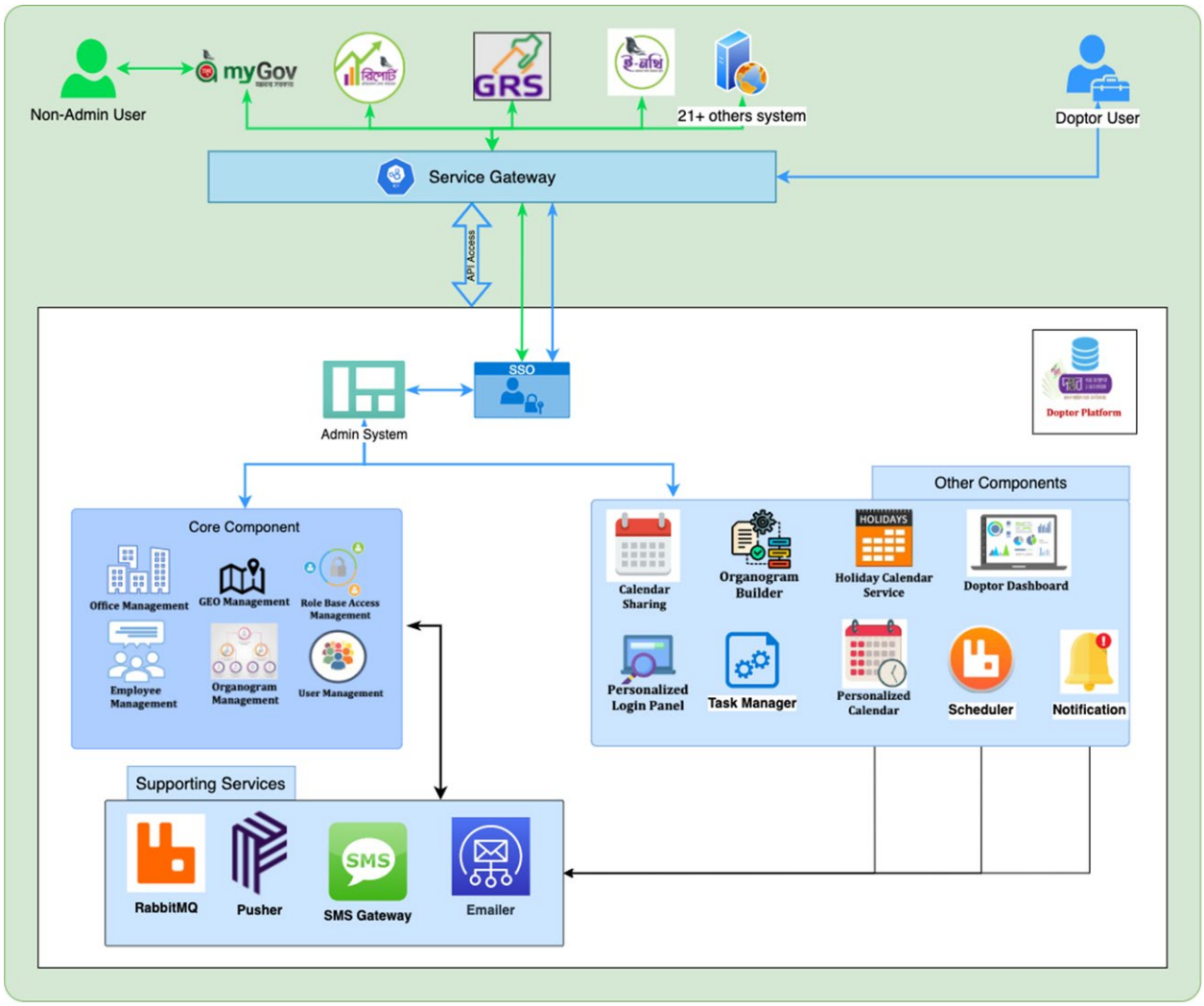


Figure 1: Doptor Ecosystem

2.3 Technology Platform of existing system

The existing Doptor Platform is a foundational e-Governance solution with established Core and Shared Components, including a Doptor SSO service for user authentication and access management.

Platform	Web Application
Programming Language	PHP, Laravel 8
Client-Side Script	JavaScript, JQuery
Style Sheet	CSS, CSS3, HTML5 & Bootstrap
Other	AJAX (Asynchronous JavaScript XML) JSON (JavaScript Object Notation) XML (Extensible Mark-up Language)
Object Oriented Programming	PHP
Framework	Laravel & CakePHP
Database	MySQL 5.7 (Percona cluster)
Cache Server	Redis
Load Balancer	NGINX, HAPROXY
Operating System	Debian, Ubuntu
Security Tools	Burp Suite
API Manager	Kong 3.3.0
Queue Manager	Laravel Queue
Monitoring Tools	iTOP, LibreNMS

2.4 Problems and Challenges

The current system requires comprehensive modernization to ensure long-term scalability, interoperability, and sustainability against future technological advancements. Specific challenges include the need to:

- Performance and data consistency challenges in the existing core services, where slow response times and data mismatches indicate architectural, database, and API inefficiencies that must be resolved without disrupting live government operations.
- Significant architectural transformation risk, as the platform must transition from a monolithic PHP-based system to microservices, containerized (Docker/K8s), and partially serverless (FaaS/PaaS) architecture.
- Identity and Access Management (IAM) complexity, including SSO, SLO, MFA, trusted devices, biometric login, and session management across web and mobile platforms, which increases security, usability, and integration challenges.
- Operational readiness gap for SRE adoption, since SRE practices (SLIs, SLOs, error budgets, incident response, postmortems) require cultural change, mature monitoring, and automation beyond traditional DevOps setups.
- High integration dependency risk, as Doptor acts as a centralized data provider for many external systems, requiring APIs to be standard-compliant, backward-compatible, secure, and high-performing at scale.
- Organogram and administrative change management complexity, where dynamic merge/split of offices and automatic transfer of responsibilities must preserve historical data integrity and avoid workflow disruption.
- Sustained support and maintenance challenge, involving multi-layer (L1–L3) support, continuous security patching, VAPT remediation, capacity planning, and CI/CD upkeep over the contract period.

3. Proposed System/ services

3.1 Objective

The overall objectives are to transform and sustain the Doptor platform by:

- To enhance, modernize, and sustain the Doptor Platform as a core national digital governance system supporting government operations.
- To ensure long-term scalability, reliability, interoperability, and sustainability of the Doptor Platform in line with evolving technological and institutional requirements.
- To position Doptor as a centralized and authoritative data provider for government office, employees, and organizational information across the public sector.
- To integrate and consolidate existing digital platforms, services, and shared components in order to deliver a unified, consistent, and seamless user experience for government officials.
- To improve system performance, availability, and resilience through architecture optimization, SRE practices, and modern DevOps approaches.
- To strengthen security, identity management, and access control mechanisms to protect sensitive government data and ensure trusted system usage.
- To establish a structured upgrade, support, and maintenance cycle that ensures smooth, uninterrupted, and standards-compliant operation of the platform.
- To enable future expansion and innovation by adopting modern, standard-based technologies and best practices, ensuring adaptability to emerging e-Government needs.

3.2 Scope

The selected firm shall be responsible for enhancing, maintaining, and undertaking new development of the Doptor platform in accordance with a recognized Software Development Life Cycle (SDLC) methodology, with the objective of ensuring the platform's standardization, stability, and long-term sustainability. The ultimate scope includes the development, enhancement, support, and maintenance of all functional and non-functional requirements detailed below.

3.3 Functional Requirements

3.3.1 Functions and Features

The assignment involves enhancement and maintenance of existing components as well as development of some new functionalities.

3.3.1.1 Development, Enhancement, Support and Maintenance Requirements

1. New Development Items

The following items represent new modules, frameworks, or significant additions to the platform's ecosystem:

- **Secure Audit Service:** A centralized, immutable audit and logging service designed to capture application logs, security events, user activities, and system access trails, with support for log normalization, encryption at rest and in transit, retention policies and compliance reporting tools.
- **SRE (Site Reliability Engineering) Implementation:**

    1. **SRE Framework Establishment**

        - Define SRE principles, objectives, and practices tailored for Doptor operations.
        - Establish Service Level Indicators (SLIs), Service Level Objectives (SLOs), and Error Budgets for core functionalities.

    2. **Monitoring and Observability**

        - Deploy comprehensive monitoring tools for infrastructure, application, database, and storage layers.
        - Implement logging, tracing, and metrics collection for end-to-end observability.
        - Build real-time dashboards for system health and performance tracking.

    3. **Incident Management and Response**

        - Establish incident detection, classification, and escalation workflows.
        - Implement automated alerting and notification mechanisms.
        - Define Incident Response Playbooks to ensure quick recovery during outages.

4. **Performance and Reliability Engineering**

    - Conduct load testing, stress testing, and capacity planning exercises.
    - Optimize system architecture to minimize downtime and latency.
    - Introduce caching, replication, and failover strategies for high availability.

5. **Automation and Tooling**

    - Automate deployment pipelines (CI/CD) for faster and safer releases.
    - Dockerization of all components of the Doptor system.
    - K8S deployment of all components of Doptor systems.
    - Automate routine maintenance tasks such as scaling, backups, and monitoring checks.

6. **Change and Release Management**

    - Define safe release practices with canary deployments and rollback mechanisms.
    - Introduce automated testing and validation pipelines before production rollout.
    - Monitor release impact in real time to minimize risks.

7. **Security and Compliance**

    - Integrate security monitoring and vulnerability scanning into SRE workflows.
    - Ensure compliance with government data protection and operational standards.
    - Implement role-based access and audit logging for critical operations.

8. **Disaster Recovery and Business Continuity**

    - Design and implement disaster recovery plans, backup strategies, and failover systems.
    - Conduct periodic DR drills to validate readiness.
    - Ensure zero data loss and minimal downtime during failovers.

9. **Continuous Improvement and Postmortems**

    - Perform root cause analysis (RCA) for major incidents.
    - Conduct blameless postmortems and document lessons learned.
    - Continuously refine SLOs, SLIs, and reliability practices based on insights.

10. SRE Dashboard

    - Develop and implement SRE Dashboard to visualize, monitor the progress of SLOs, SLIs, Error Budget, etc.
    - The Dashboard prompts the SRE team for adequate action.

2. List of Enhancement Items

The following table outlines existing features and their corresponding enhancement areas as defined in the ToR:

Existing Features	Existing Key Area Description	Enhancement Area
Core Service Framework	Currently it serves as the foundational middleware providing office-related common services (GEO, Office, Organogram, Employee Profile) for over 17,000 offices. It is primarily built on PHP (7.4) with a Maria DB 10 database.	Technology stack upgrade (Java, Python, PHP), migration to microservices, and performance optimization.
	At present, the Doptor system is experiencing comparatively slow response times and, in some cases, is displaying data inconsistencies or inaccurate information.	Performance Optimization: Conduct thorough code review and profiling to identify and eliminate performance bottlenecks, focusing on optimizing data access patterns and enhancing API response times.
Core and Shared Service Monitoring	Currently no APM (Application Performance Monitoring) is implemented in Doptor.	Service Health Monitoring: Implement APM (Application Performance Monitoring) and distribute tracing tools to provide real-time visibility, health, performance, and inter-service dependencies of all core and shared services.
Keycloak (IAM)	Currently uses a basic version of Keycloak for Unified Identity Management and Single Sign-On (SSO). It supports Multi-Factor Authentication (MFA) using Soft OTP.	Upgrade to the latest stable version, adoption of MFA/passwordless flows (e.g., WebAuth), and high-availability configuration. High-Availability Configuration: Ensure the Keycloak infrastructure is configured for full cluster mode with geo-redundancy to provide continuous availability and disaster recovery capabilities for the entire

		platform's authentication backbone.
Doptor Calendar	It's essentially a centralized scheduling and event management module that helps government offices plan, track, and manage tasks, events, and important dates.	The consulting firm shall review the existing Doptor Calendar functionalities and enhance them to ensure the system is error-free, efficient, user-friendly, and fully functional.
Event Management	It's designed to centrally manage and disseminate official events, notices, and time-bound activities across government offices and officials using Doptor's authoritative organizational and employee data.	Support for setting up Single and Recurring Events with mandatory notification mechanisms. This includes a robust Calendar Sharing Mechanism to facilitate meeting/event scheduling and sharing with internal teams, office colleagues, and external offices.
Task Management Integration	It allows government offices to assign, track, and monitor tasks for officials based on their roles and offices. It provides real-time status updates and accountability tracking across workflows.	Integration with a Task/Subtask List to allow users to manage their regular tasks and view a consolidated task list on the Calendar Dashboard.
eSign	Provides a shared service for digital signature validation used by integrated applications to avoid redundant development efforts.	Implementation of batch/bulk signing.
Common Features (GEO, Office, Organogram)	Provides core government data (administrative units, office hierarchies, and designations) via 29+ APIs. Includes a change log for tracking historical data.	Enhancing the APIs to make them standards-compliant, error-free, high-performance, and secure, ensuring reliable interoperability, scalability, and long-term sustainability of the platform.
API Manager	The system has implemented Kong 3.3.0 API Manager.	Review the API Manager and implement it optimally to achieve maximum performance across the platform.
Queue Manager	The system has been implemented by Laravel Queue Manager.	Review the Queue Manager and implement it optimally to achieve maximum performance across the platform.

SGV Image as Signature	The system currently stores	
Doptor Portal	Doptor provides a dedicated integration portal for the organizations, where all available APIs are systematically documented, and the platform's core functionalities, workflows, and integration guidelines are clearly defined to facilitate seamless and secure integration.	Review the existing portal and update outdated content, as well as develop and incorporate new content where required.
Garbage Cleaning	A significant amount of historical and unnecessary data is stored in the database, consuming disk space and causing performance degradation.	It is necessary to identify unnecessary (garbage) data and establish a process to clean it periodically.
Database Backup	Currently manual backup is taken.	Need to implement automated and incremental backup of the Doptor Database.

3. List of Items Requiring Regular Support

The firm is responsible for providing multi-layered support for the following:

- **1st Layer (Helpdesk):** Addressing user queries via phone, email, and tickets; providing initial troubleshooting and guidance.
- **2nd Layer (Issue Management):** Issue investigation, categorization, prioritization, and managing Standard Operating Procedures (SoPs).
- **3rd Layer (Technical Support):** Bug fixing for core applications, databases, and infrastructure in collaboration with technology partners.
- **Knowledge Transfer:** Conducting workshops and training for government personnel to ensure system adoption.
- **Integration Support:** The Doptor platform is currently integrated with 40 applications across different ministries and departments. The consulting firm will be required to provide regular maintenance and support services for these integrations.

4. List of Items Requiring Maintenance

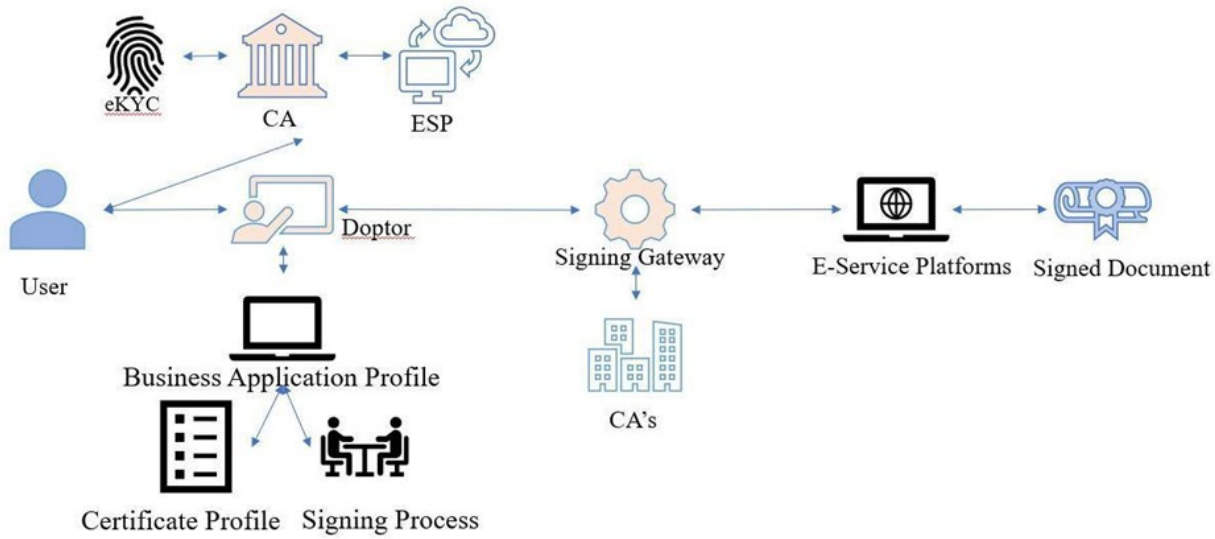
Continuous maintenance is required to ensure system stability and performance:

- **Core System Maintenance:** Regular upgrades, refactoring of source code to reduce technical debt, and managing service configurations.
- **Infrastructure & Resource Administration:** Monitoring system health, database performance, and storage utilization.

- **Security Maintenance:** VAPT (Vulnerability Assessment and Penetration Testing) issue resolution for 02 (two) times and security patching. Note that, a2i will provide the VAPT reports.
- **Capacity Planning:** Preparing proposals for computing capacity enhancement (storage, memory, node addition) based on growth trends.
- **DevOps & CI/CD:** Maintaining automated deployment pipelines, backups, and monitoring checks.
- **Database Cleaning and Backup:** Implementing file storage optimization, database cleaning and backup mechanisms.

3.3.1.2 e-Sign Gateway

The eSign Gateway is a secure, common service for integrating digital signature and verification capabilities into government workflows. Its objective is to enable paperless processing by ensuring the authenticity, integrity, and non-repudiation of all official digital documents in compliance with national legal and technical standards.



Feature	Description
Existing/Core System	A centralized API service for requesting and applying digital signatures to documents generated by other platform services.
New Development	Implement batch signing capabilities for high-volume transactions.
Deliverables	A reliable eSign API service with batch signing capabilities. Full documentation on integration standards and security protocols.

3.3.1.3 User and User Roles

The system is designed for a multi-tiered audience:

- **Government Offices**: Ministries, Directorates, departments, agencies, and entities responsible for managing and delivering government services.
- **Government Officers and Employees**: Users at different levels interacting with the platform for workflow management, decision-making, and service provisioning.
- **IT Administrators and Support Teams**: IT personnel responsible for maintaining, troubleshooting, and optimizing the platform's performance and security. Access control will be strictly managed via a Robust Role-Based Access Control (RBAC) system linked to the Uniform Identity Management module.

3.3.1.4 Identity and Access Management (IAM): SSO, SLO, and Advanced Login

The Identity and Access Management (IAM) system, based on an upgraded Keycloak instance, must be enhanced to provide robust security, improved user experience, and sophisticated session management.

Feature	Requirement Details	Deliverables
Simultaneous Session Management	The system must be able to manage multiple active user sessions across different devices (e.g., laptop, mobile). It is mandatory to implement Single Logout (SLO) functionality that allows a user to log out from all active devices simultaneously upon initiation from one device.	Fully implemented SLO functionality across all platform services.
Password Change Security	When a user initiates a password change, the system must automatically terminate all existing sessions and require re-authentication on all devices to ensure immediate security enforcement.	API and UI feature for remote session termination upon password change.
Trusted Device Management	During the multi-factor authentication (MFA) process, the system must allow users to mark a specific device (e.g., personal desktop, work mobile) as a "**Trusted Device**." Subsequent logins from a trusted device, within a defined security interval, should bypass repeated OTP/MFA challenges for a streamlined experience.	Configurable Trusted Device Registration module and Policy.
Mobile Application Login	Develop and implement native, secure login facilities for both Android and iOS mobile applications. This is essential to enable officers to manage their profiles, access services, and perform administrative duties from their mobile devices.	Secure Login components for both Android and iOS applications.
Biometric Authentication	The mobile application login system must incorporate standard Biometric Login features (e.g., Fingerprint,	Integrated Biometric Login

	Face ID) for enhanced security and convenience on supported devices.	API/SDK for mobile apps.
Comprehensive Login History	The system must maintain a detailed and auditable Login History. Records must track login events categorized by: Device Type (web, Android, iOS), Integrated Service/Application (MyGov, GRS, RMS, etc., if applicable), and Gender (for analysis and compliance).	Login History dashboard with advanced filtering and reporting capabilities.

3.3.1.5 Office Administration and Subordinate Access

The Office Administration module must be enhanced to support delegation of roles and hierarchical management access, thereby distributing the administrative workload and improving organizational efficiency.

Feature	Requirement Details	Deliverables
Delegated Administration (Sub-Admin)	Implement a Sub-Admin system that allows the primary Office Admin to delegate specific, limited administrative roles to designated users within their office. These roles must include, but not be limited to: User ID Creation, User Assignment/Release (Transfer), Change of Title and Branch Information, and Replacement Management.	Sub-Admin configuration panel and a Role-Based Access Control (RBAC) matrix for delegated administrative roles.
Hierarchical Administration	Grant specific, restricted Office Admin roles to the administrators of superior departments (e.g., Ministries, Departments) to manage their subordinate offices. These rights must include User ID Creation, Assignment, and Release (Transfer) of officers within the subordinate entities.	Documentation and implementation of the hierarchical access policy, covering all levels (Ministry/Department/ Organization/ Divisional/District/Upazila offices).
Centralized Office Admin Dashboard	Provide a consolidated dashboard for all administrators (Office Admin and Sub-Admins) to manage all delegated and assigned duties efficiently.	Dedicated Office Admin management console.

3.3.1.6 Office Organogram Builder and Management

The Office Organogram functionality must be upgraded to handle dynamic organizational changes, ensuring that the system reflects real-world administrative restructuring accurately.

Feature	Requirement Details	Deliverables
Organogram Merge Functionality	Develop tools to facilitate the accurate merging of multiple departments or organizational structures into a single, unified organogram structure (e.g., in cases of administrative consolidation).	UI and backend service for merging organizational units, preserving historical data.
Organogram Split Functionality	Develop tools to facilitate the splitting of a single department or office into multiple distinct organizational entities, ensuring all necessary titles and employee assignments are handled correctly.	UI and backend service for splitting organizational units.
Activity/Responsibility Transfer	When a user's title or designation is transferred within the organogram, the system must ensure the seamless and automatic transfer of all associated pending tasks, activities, and responsibilities to the new incumbent.	Enhanced transfer mechanism integrated with the Notification and Task Manager.
Visual Organogram Builder	Enhance the existing tool to allow administrators to visually create, modify, and restructure the hierarchical structure of government offices.	Interactive, visual organogram management interface.

3.3.1.7 Integration and external dependencies

The Doptor platform is currently integrated with 40 applications across different ministries and departments. The consulting firm will be required to provide regular maintenance and support services for these integrations. The list of the integrated applications is provided below:

S/L	Applications Name	Ministry Name
1	Nothi	ICT Division
2	E-License and Lease Management System	Ministry of Power, Energy and Mineral Resources
3	Paribahan Pool	Ministry of Public Administration
4	BIWTA Automation	BIWTA (Ministry of Shipping)
5	BARD ERP	BARD, LGRD

6	Integrated Hill Tracts Digital Service Delivery Platform for MoCHTA	Ministry of Chittagong Hill Tracts Affairs
7	SDG Tracker	ICT Division
8	Grievance Redress Service (GRS)	Cabinet Division
9	Digital Business Identification Platform	ICT Division
10	Integrated Digital Service Delivery Platform	Ministry of Fisheries and Livestock
11	e–Loan Management System for the weavers	Ministry of Textiles and Jute
12	General Certificate Court	ICT Division
13	Good Governance Activity Management System (NIS)	Cabinet Division
14	Integrated Digital Service Delivery Platform for Ministry of Social Welfare	Ministry of Social Welfare
15	License Management System (LMS)	ICT Division
16	Labour Inspection Management Application (LIMA)	Ministry of Labour & Employment
17	Strengthening digital processing of projects	Planning Division
18	PPS (Project Plaining system)	Planning Division
19	Integrated Digital Service Delivery Platform for Ministry of Agriculture	Ministry of Agriculture
20	Policy Guidence Unit	Cabinet Division
21	Automation Report Generating System (ARGS)	Cabinet Division
22	Mygov	ICT Division
23	NHRC	

24	ACR Management System	Cabinet Division
25	Integrated Digital Service Delivery Platform of Ministry of Science and Technology	Ministry of Science and Technology
26	ICT Policy Dashboard	Infomation and Communication Technology Division
27	Integrated Digital Service Delivery Platform (Ministry of Commerce)	Ministry of Commerce
28	Demand Note Automation Management System	Ministry of Posts, Telecommunications and Information Technology
29	EMC Court	ICT Division
30	Smart General Certificate court	ICT Division
31	Smart Executive Magistrate court	ICT Division
32	NGPIMS	Ministry of Home Affairs
33	Annual Performance Agreement Management System (APAMS)	Cabinet Division
34	BTRC LIMS	Ministry of Posts, Telecommunications and Information Technology
35	PrismERP	
36	Bangladesh Rice Research Institute	Ministry of Agriculture
37	Online Report Management System	ICT Division
38	Smart Case Management System	Cabinet Division
39	Demand Note Management System	Ministry of Posts, Telecommunications and Information Technology
40	Smart Land Service Delivery	Ministry of Housing and Public Works

In addition to the stated list, the consulting firm shall provide new integration support to external agencies that formally request a2i to integrate their digital systems with the Doptor platform.

3.4 Non-Functional Requirements

3.4.1 Sizing, Performance and Scalability Requirements

- **Scalability**: The platform must be able to scale to accommodate growing data volumes and user loads.
- **Performance**: Performance must be enhanced through code optimization and caching mechanisms.
- **Availability**: Ensure 24/7 platform access with a high uptime percentage, allowing scheduled downtime only for necessary maintenance.

3.4.2 Security and Privacy Policy

The firm must:

- Implement a Security and Privacy Policy to prevent breaches.
- Ensure Security testing of the system at regular intervals (not more than six months) by a third-party organization.
- Fix all necessary security holes identified by the third-party organization.
- Implement robust security measures, including encryption, authentication, and authorization mechanisms to protect sensitive data.
- Enforce strong password policies and secure sessions handling mechanisms.

3.4.3 Coding convention

The firm must follow the standard coding styles to produce high-quality code for further usage of the code in terms of reusability, refactoring, task automation, language factors etc. The firm should submit a standard coding convention approach, which may include different conventions like commenting, indent style, naming etc. following the best coding practices.

3.4.4 Business Continuity Plan

The system must be implemented:

- Fault Tolerance: Implement robust exception handling and recovery mechanisms to ensure system reliability and avoid irrecoverable data loss in case of transaction failures.
- Data Backup: Provide on-demand accountable consultancy support to the Data Center in terms of Data Backup Scheduling.

3.4.5 Data Ownership

The ownership of all data generated, processed, transmitted, or stored within the Doptor shall remain solely with the Government of Bangladesh (GoB). The selected firm must ensure that no data—whether in raw, processed, metadata, or derivative form—is duplicated, transferred, stored, or used outside the authorized Doptor environment without written approval from the authority. All intellectual property rights, documentation, configurations, code repositories, logs, and platform-related datasets shall be treated as government property. The firm must guarantee unrestricted administrative access and ensure that full data portability is maintained throughout the contract period and after completion of the assignment.

3.4.6 Data Security

The firm must ensure end-to-end data security for the Doptor, applying national cybersecurity guidelines, personal data protection ordinance, 2025 and internationally recognized standards such as ISO/IEC 27001, OWASP, and NIST best practices. All data at rest and in transit must be protected through strong encryption mechanisms. The firm shall implement adequate access control, identity management, security hardening, network-level protection, continuous monitoring, and vulnerability remediation. Any security breach, anomaly, or suspected threat must be immediately reported to the authority along with detailed incident analysis and mitigation actions. The firm must also ensure secure API communication, regular patching, secure coding practices, and periodic security audits.

3.4.7 Technology Handover

Upon completion or termination of the contract, the firm shall conduct a comprehensive technology handover to the authority or any nominated agency. This includes full delivery of source code, database, technical documentation, API documentation, system architecture diagrams, deployment scripts, configuration files, test cases, credentials, version control repositories, and operational manuals. The firm must ensure that all knowledge, processes, and tools required for the uninterrupted operation, maintenance, and future enhancement of the Doptor are fully transferred. A hands-on knowledge transfer session, along with detailed walkthroughs and technical demonstrations, must be conducted to ensure smooth transition without service disruption.

3.4.8 IT Compliance

The firm must ensure that the Doptor and all related services strictly comply with national ICT policies, digital security laws, data protection regulations, and government interoperability guidelines. The platform must also maintain compliance with international best practices including secure coding standards, accessibility guidelines, data privacy principles, and software licensing norms. The firm must maintain transparent audit trails, adopt proper change-management procedures, and ensure that all infrastructure, software, and operational activities adhere to IT governance, quality assurance, and documentation standards mandated by the authority.

3.4.9 Accessibility

The dashboard and all user interfaces must be designed to be intuitive, user-friendly, and inclusive—ensuring accessibility for users with varying levels of technical expertise. The solution must comply, at a minimum, with **WCAG 2.1 Level AA** accessibility standards as well as **National Web Accessibility Guideline**, with a strong preference for achieving **Level AAA** where feasible. The design should prioritize clear navigation, consistent layouts, assistive technology compatibility, and responsive elements to ensure equitable user experience across all devices and user groups.

SL.	Items to Check	Details
01.	For anything on a web page that is not text, is there any text equivalent for that item?	• Anything that does not text on a web page usually includes, but is not limited to, an image, graphic, audio clip, applets (small application running within a web browser, i.e. text chat window, etc.), tickers, or other features that conveys meaning through a picture or sound. Examples include buttons, check boxes, pictures and embedded or streaming audio or video. • Providing a text equivalent means that words are being used to describe what an item (that does not physically consist of text) is, why it is there, and any information being communicated by the use of that item or the item itself. • Check that all images have accurate and meaningful text equivalents. Images mostly use an “alt-tag” or “longdesc” attribute as part of the object. To check, mouse users can roll their cursor over an image. If a text label or window pops up, then it has a text equivalent. Screen reader users can listen to see if an image is identified and described. It is also acceptable to simply include a text description above or below the image. For example, “The picture below shows…” • Ascertain that images of text, graphical text (pictures of text), or text that is part of an image have a text equivalent. Be sure that the text equivalent correctly describes the image or communicates any information as part of the image. For example, if the image itself contains words, be sure the exact wording from the image is used within the text equivalent.

		• Ensure any audio has a text equivalent, such as a text transcript.
02.	Is captioning, audio descriptions, or other equivalents provided for presentations that utilize both audio and video at the same time? Is captioning, descriptions, or other alternatives synchronized with the presentation?	• Determine that all audios have been captioned for the deaf and hard of hearing, and all videos have audio descriptions for the blind and visually impaired. • Ascertain that captions and audio descriptions are synchronized correctly with the audio and video. For example, synchronized captions allow someone to read captions and also watch the speaker's relevant body language. • Remember that this only applies to multimedia presentations, i.e., those presentations utilizing both audio and video at the same time. For example, the audio and video webcast of a program would need to be synchronized. An audio webcast would require a text transcript. A silent (no audio) web slide show would require a text equivalent for any images.
03.	If the color was removed, would it inhibit the use of the website?	• To check, view the page using a monochrome monitor (ex. black and white monitor, etc.) or by printing a page to a black and white printer.
04.	Is color being used to emphasize text or indicate an action?	• If so, an alternate method needs to be included so users can identify what is being emphasized using the colored text or action. • For example, if all links on a web page are blue, then underlining the links is an acceptable method for identifying blue-colored links. Another example, is if users are prompted to press a green start button, then a text label above the green button saying "press green start button" is an acceptable method.
05.	Do web pages ignore user-defined style sheets?	• Style sheets are formatting instructions on how a page should be displayed (can also include how it is printed and presented). For example, a user specifies that they want their browser to view pages with an extra-large font with white characters on a black background. These preferences are set up for all pages viewed.
06.	Does a web page override or ignore user settings?	• To check disable style sheets within the browser (Check the browser's help menu for instructions) or try changing the font size or background colors through the browser's settings.

07.	If a link is embedded in an image, is there an equivalent text link?	• Frequently, a web designer will use an image map which contains a link or set of links. • Check to see if the image has any text links or labels. In some cases, you may have to move the mouse around the image to see if different text labels appear over different portions of the image. Screen readers will announce "image map link…" when a link is detected. These text labels alert users that clicking or selecting the link in this region of the image, will retrieve a specific web page. This is an example of a client-side image map which can be quite accommodating to people with disabilities and those using assistive technology. • On the other hand, there are image maps that do not indicate to the user which specific web page will be retrieved when a particular region of the image is selected. These are called server-side image maps because the computer or server hosting the web page determines which page is sent based on a portion of the image selected. These are not accessible image maps, requiring a redundant text link on the same page retrieving the same pages as those links used in the image map.
08.	If information is displayed using a table(s), can columns and rows be identified by screen readers?	• Using a screen reader, listen to how the table is read aloud.
09.	If frames are used, are they accurately text labeled?	• Frames are used to visually separate information on a web page.
10.	Does anything on the page blink or flicker?	• Ask if the web designers can prove whether any blinking or flashing elements have a frequency greater than 2 Hz and lower than 55 Hz. This requirement is necessary because some individuals with photosensitive epilepsy can have a seizure triggered by displays that flicker or flash, particularly if the flash has a high intensity and is within certain frequency ranges.
11.	Do web sites not conforming to acceptable and approved accessibility standards offer a text only	• The World Wide Web Consortium's (W3C) Web Accessibility Initiative Guidelines and Section 508 are the two widely accepted authorities on Web accessibility and design.

	equivalent of their web site?	• Web sites that cannot adhere to the accessibility guidelines set forth by W3C and Section 508 can offer a text only equivalent to all the information displayed and all functions available.
12.	If scripting is used, such as JAVA, etc., is there a text equivalent so assistive technology, like screen readers, can read the information?	• An example of scripting could be a stock ticker on a web page that is animated, refreshing, and displaying information. Another example is using an image, that when a mouse cursor rolls over the image, additional information pops open on the screen, and then disappears when the mouse cursor rolls off.
13.	If online forms are used, can people using adaptive technology fill in and submit all the required information?	• Can a keyboard be used to access all the form fields? • Are text labels used either inside or near form fields to identify what information users should be entering? • Can a screen reader identify the form(s)? • Do the forms follow a logical order? For example, if a user hears "Last Name" is the corresponding form the area where they would enter their last name?
14.	Is there a way for users, especially those using screen readers to skip repetitive navigational links?	• Navigational links are a set of routine navigation links frequently used to move users to pages within a web site, usually located on the top or side of each web page. For example, "Help," "Contact Us," etc. links that all appear on the same page within a website in the same way and location.
15.	If users are given a certain amount of time for an action or response, is there any indication of how much time they have left or an option to request more time?	• Some web pages may expire or expire after a certain amount of time, and refresh the entire page, for example, those requesting personal information.
16.	Unicode character set for Bangla	• Use of Unicode character set for Bangla - Interspersing Bangla and English on the same page should be avoided until such time that there is a screen reader which can handle multiple languages.
17.	Accessible documents on web pages	• Where it is not possible to make a document accessible, then an alternative, accessible format should be downloadable along with the original image file.

18.	Navigation mark-up	• Use of heading level 1-6, in addition to navigation links like 'skip to main content'.
19.	HTML validation	• HTML is the simplest programming language used for website development and is accessible on all browsers — a desktop browser or a mobile browser. All web pages should have HTML validation.
	CSS validation	• Content presented with CSS errors may lead to serious problems such as overlapping of content, making it almost impossible to read. CSS errors may also prevent some users from successfully carrying out custom CSS processing to set the preference of colour and size of text and objects to suit their vision requirements.
21.	Colour adjustment option	• High contrast and font customization options should be available
22.	Labelling of Links	• Labelling links correctly rather than just 'click here'- i.e., descriptions should be accurate. • The web page has a descriptive and informative page title. • A sign language video is provided for all media content that contains audio. • The page is readable and functional when the text size is doubled. • All page functionality is available using the keyboard
23.	Accessibility plugin	• Some accessibility features such as Monochrome, Invert Colors, Big Cursor, Highlight Link, Show Headings, Reading Guide, Reset Button, Keyboard Shortcut etc. Commonly these items are named Accessibility Plugin.
24.	Accessibility Guideline	• Have to follow the WCAG 2.1 Level A Guidelines at least. To know more and details about “Digital Service and Web Designing Guideline for Inclusive Accessibility 2022” follow this website link: https://a2i.gov.bd/disability-innovation-lab/

3.4.10 Documentation Plan

The firm must deliver detailed and proper documentation throughout the project lifecycle, including:

- An extensive "**Documentation Plan**" in the technical proposal.
- Technical Document (SRS, SDD, FRS, Data dictionary, HLD, Test Report, QA Report, Technical Manual, Deployment Architecture, ER Diagram etc.).
- Updated documentation and training materials (AV and Text) for government employees and developers.

3.4.11 Standard, Tools and Technologies to be used

The solution must adhere to all applicable Technical Standards and best practices. The firm is expected to propose a modern technology stack that utilizes Function as a Service (FaaS) and PaaS for serverless components.

3.4.12 Quality Assurance and IT Audit Requirement

The Quality Assurance (QA) Management function within the Doptor Platform ensures the delivery of a reliable, high-quality system that meets defined requirements, aligns with industry standards, and delivers seamless user experience. QA encompasses the establishment of quality processes, rigorous testing, and ongoing quality control throughout the system's development and maintenance lifecycle. Standards such as ISO 9001, AS 9100, Six Sigma, or CMMI may be adopted and tailored to meet specific project needs.

Scope of Work:

1. **Quality Planning:**
    - Develop a comprehensive Quality Management Plan (QMP) defining objectives, processes, and required resources to ensure platform quality.

2. **Requirement Validation:**
    - Verify and validate system requirements to ensure completeness, accuracy, and alignment with stakeholder expectations.

3. **Test Planning and Execution:**
    - Design and execute testing activities, covering functional, performance, security, and usability aspects.
    - Employ both manual and automated testing methods to maximize platform reliability and quality.

4. **Defect Tracking and Resolution:**
    - Implement a structured defect tracking mechanism to identify, prioritize, and resolve issues efficiently.
    - Ensure timely defect resolution and continuous quality improvement.

5. **Quality Control and Process Compliance:**

- Monitor adherence to defined processes, standards, and best practices throughout development and maintenance.
- Establish quality checkpoints and controls to enforce process compliance.

6. **Documentation and Audit:**
   - Maintain thorough documentation of quality processes, test plans, test cases, and results.
   - Conduct periodic quality audits to identify gaps and implement corrective actions.

Functional Testing	Validate that all features and functionalities of the Doptor platform work as expected according to specified requirements.
Performance Testing	Evaluate the platform's responsiveness, speed, and stability under varying loads and conditions.
Security Testing	Identify vulnerabilities and weaknesses to ensure the platform is resistant to unauthorized access and data breaches.
Usability Testing	Assess the user interface, user experience, and ease of use of the platform.
Compatibility Testing	Ensure the platform works seamlessly across various devices, browsers, and operating systems.
Integration Testing	Validate the interaction and integration of different modules and components.
Regression Testing	Confirm that recent updates or changes haven't negatively impacted existing functionalities.
User Acceptance Testing (UAT)	Involve end-users to validate that the platform meets their expectations and requirements.

3.4.13 Functional & Non-Functional Testing

To ensure the reliability, security, and compliance of the Doptor Platform, the selected consulting firm shall carry out comprehensive testing activities as part of the Software Development Life Cycle (SDLC). The testing scope under this assignment shall primarily include **Functional Testing** and **Vulnerability Assessment & Penetration Testing (VAPT)**, as described below:

a) Functional Testing

The consulting firm shall be fully responsible for planning, executing, and managing all Functional Testing activities to verify that the developed, enhanced, and maintained features of the Doptor Platform operate correctly and in accordance with the approved functional requirements, specifications, and business rules.

Functional Testing shall include, but not be limited to:

- Verification of all core and shared services, modules, workflows, APIs, integrations, and user interfaces
- Validation of functional requirements, business logic, data integrity, and error handling
- Integration testing to ensure seamless interaction among internal modules and external systems
- Regression testing to ensure that new changes do not adversely impact existing functionalities
- Documentation of test cases, test results, and defect reports

Cost Responsibility:

All costs related to Functional Testing, including tools, environments, resources, and test execution, shall be borne entirely by the consulting firm.

Defect Resolution:

The consulting firm shall be responsible for identifying, analyzing, fixing, and retesting all bugs, defects, and issues identified during Functional Testing at no additional cost to a2i.

b) Vulnerability Assessment & Penetration Testing (VAPT)

To ensure the security and resilience of the Doptor Platform against potential cyber threats, Vulnerability Assessment & Penetration Testing (VAPT) shall be conducted by an authorized third-party security firm engaged by a2i.

Cost Responsibility:

The cost of conducting VAPT shall be borne by **a2i**.

Issue Resolution:

The consulting firm shall be fully responsible for:

- Analyzing the VAPT reports provided by a2i
- Resolving all identified vulnerabilities, security gaps, and compliance issues
- Implementing necessary fixes, mitigations, and security hardening measures
- Supporting re-testing and validation until all critical and high-risk issues are resolved

All remediation activities related to VAPT findings shall be completed within the timelines approved by a2i and shall not incur any additional cost to the authority.

3.4.14 Fault Tolerance

Implement proper exception handling and recovery mechanisms to ensure system reliability and avoid irrecoverable data loss in case of transaction failures.

- Exception Handling: Implement robust exception handling mechanisms to handle errors and exceptions gracefully.
- Transaction Recovery: Ensure the system can recover from transaction failures to prevent data loss and maintain data integrity.
- Redundancy and Failover: Introduce redundancy and failover capabilities to mitigate the impact of hardware or network failures.
- Continuous Monitoring: Implement real-time monitoring to detect and respond to faults promptly, reducing downtime.

3.4.15 Supportability

Design the Doptor platform to be modifiable, extensible, and evolvable, allowing for future additions and exploiting new technologies.

- Modular Architecture: Design the Doptor platform with a modular architecture to allow easy integration of new functionalities.
- Extensibility: Enable easy extension of existing features and capabilities to accommodate future requirements.
- API Support: Provide well-documented APIs to support integration with third-party services and applications.
- Developer-Friendly: Make the platform developer-friendly with clear documentation and guidelines for easy customization.

3.4.16 Configurability

Allow behavior control through configuration without modifying source code or redeploying packages.

- Flexible Settings: Allow users to configure various aspects of the platform, such as user interface preferences and workflow settings.
- No Source Code Modification: Ensure that configuration changes do not require modification of the source code or redeployment.
- User Role Customization: Provide options to customize user roles and permissions to align with specific organizational requirements.

- Centralized Configuration: Store all configuration settings in a centralized location for easy management and access.

3.5 Critical components in delivering the services

The following are critical components for the sustainability and strategic enhancement of the Doptor platform:

- API Manager
- IAM
- APM
- eSign gateway
- SRE Dashboard
- Secure Audit Service

3.6 Development & Approach Methodology

3.6.1 Development & Implementation Methodology

The firm is required to follow the Software Development Life Cycle (SDLC) methodology.

3.6.2 System Design & Development Plan

The platform must be designed with:

- **Supportability**: Modular, extensible architecture to ease maintenance.
- **Configurability**: Behavior control without modifying source code.
- **Serverless Architecture**: Deployment must leverage FaaS/PaaS to ensure maximum scalability and high availability.

3.6.3 Testing Plan

The testing plan must cover: Unit Testing, Integration Testing, System Testing, Load Testing, Stress Testing and Security Testing.

3.6.4 User Acceptance Test (UAT)

User Acceptance Testing (UAT) must be conducted at every phase of the project, including the provision of a dedicated Test Environment.

3.6.5 Migration of Legacy Data (If any)

A well-defined migration plan must be proposed to transition existing services and data to the upgraded framework and modern technology stack.

3.6.6 Risk Management Plan

The plan must address:

- Fault Tolerance (Data loss prevention).
- Post-Hosting Support including regular performance monitoring, database tuning, and data backup scheduling.

3.6.7 Deployment and Implementation Plan

A detailed deployment plan must be provided, including provisioning a dedicated test environment to test changes and updates before deployment to the live platform.

3.6.8 Training and Knowledge Transfer Plan

The consulting firm will be needed to conduct workshops, training programs in participation of a2i and the stakeholders. The firm will have to deploy technical resource persons during the workshops, training programs arranged by the a2i program.

- Facilitating periodic workshops with a2i teams for knowledge transfer.
- On-demand facilitation of system updates the information to a2i as the mini-training session (Quarterly and/or in case of major changes executed)
- Provide authentic access to a2i experts to source code and documentation.
- Developing technical and operational manuals to operate and manage the platform.
- Firm will prepare guideline and standard practice and will facilitate training programs, provide technical experts for system integration and further development.
- The firm will provide resource person, training material, ToT & training for capacity development in collaboration with a2i. Venue, logistics and invitation will be arranged by a2i.

All the necessary costs associated with the training sessions will be borne by a2i whereas the firm will provide the required resources persons, training materials, user manuals, presentation documents, etc.

3.6.9 Support & Maintenance Plan

A multi-layered support system must be established for continuous support and maintenance:

The vendor team needs to follow the layer-based support management system. Layer based support management is a term that refers to the IT support of the system around different levels or tiers of service. Each level or tier has a specific function and responsibility and is staffed by personnel with different skills and expertise. The purpose of layer based support management is to provide efficient, effective, and satisfactory service to customers and end users. The vendor team needs to follow a three-layer support system.

- Helpdesk Support (1st Layer Support)
- Issue Management (2nd Layer Support)
- Technical Support (3rd Layer Support)

3.6.9.1 Helpdesk Support (1st Layer Support)

The vendor team needs to provide the basic help desk resolution and service desk delivery. It is also known as first-line support for the citizens and system users. This support tier will handle basic customer issues, such as system usage help, profile management help, etc.

- Attend to user's phone calls.
- Support agents will communicate through multiple channels for example phone, email, Online Support Ticketing System etc.
- Conduct basic troubleshooting using questionnaires to find out the level of support needed.
- Create tickets for 2nd-layer support.
- Solve common queries such as username and passwords issues, office enrollment.

3.6.9.2 Issue Management (2nd Layer Support)

- Issues investigation.
- Issues Categorization, Prioritization, and Escalation.
- Basic level troubleshooting of application, database, and infrastructure.
- Collaboration and coordination among the layers.
- Collecting feedback from both service recipient and service provider end and adjusting feedback through the proper communication and coordination with the Doptor team.
- Prepare customized support reports for the management.

3.6.9.3 Technical Support (3rd Layer Support)

- Core applications, Database, and Infrastructure level bug fixing.
- Accommodating requests at Core applications, Database, and Infrastructure level
- Continuously analyze user and system logs and take necessary actions if required.
- Taking prompt preventive action solely or with the help of the core development team if any misconfiguration or anomaly is found in the Core applications, Database, and Infrastructure.
- Periodically health checking of Core applications, Databases, and Infrastructure.

3.7 Security and Privacy Policy

The system's authentication and permission system are robust to ensure the highest level of security. The following measures will be placed to prevent any kind of security breach:

- **Invalid Input:** Validating and purifying incoming data for data integrity and user access.
- **URL Restriction:** Limiting access to URLs based on user permissions and prohibiting unauthorized URL access.
- **Protected Administration Panel:** Securing the admin panel with SSL encryption and different URLs to prevent data hijacking.
- **Password Hashing:** Using one-way algorithms and random salts for password hashing.

- **Session and Cookies:** Regenerating user sessions and cookies uniquely for improved security.
- **Disclosure of Sensitive Information:** Suppressing and logging errors to prevent sensitive information exposure.
- **CSRF Prevention:** Generating automatic tokens to prevent Cross-Site Request Forgery attacks.
- **SQL Injection Prevention:** Implementing prepared statements and proper escaping to prevent SQL and Code injections.
- **Cross-Site Scripting Prevention:** Filtering user-submitted content to prevent XSS attacks.
- **SSL Encryption:** Ensuring SSL encryption for communication between user browsers and the administration panel in Doptor.

3.8 Hosting Requirement and plan

The development must be approached using Serverless Architecture Oriented Development.

- Mandate: All new components must adopt a Serverless Architecture approach, leveraging Function as a Service (FaaS) and fully managed services (PaaS).
- Scalability: The design must ensure auto-scaling and elasticity to handle extreme fluctuations in load.
- Compliance: The Client will check the Government directives on data hosting (National Data Center / BCC) and the firm must align the serverless deployment plan accordingly.

3.9 Change Management Plan

The Change Management process ensures that all modifications to the system are planned, evaluated, implemented, and monitored in a controlled and systematic manner. The process aims to minimize disruption, optimize system performance, and enhance user satisfaction. Frameworks such as CMMI, ITIL, or other relevant standards can be tailored to guide this process.

Key Functionalities:

1. **Change Request Management:**
   - Implement a structured process for submitting, evaluating, and approving change requests.
   - Assess changes based on impact, priority, and alignment with business and organizational objectives.

2. **Change Planning and Documentation:**
   - Develop detailed change plans outlining objectives, scope, timelines, resource requirements, and associated risks.

- Maintain comprehensive documentation linking changes with Incident Management, Problem Management, and Release Management processes.

3. **Stakeholder Communication:**
   - Establish clear communication channels to keep stakeholders informed about upcoming changes, expected benefits, and potential impacts.
   - Provide regular updates, address queries, and manage concerns proactively.
4. **Training and User Support:**
   - Develop training materials and conduct sessions to familiarize users with the changes.
   - Provide ongoing support to ensure effective utilization of updated features.
5. **Change Implementation and Testing:**
   - Execute changes following a structured and controlled approach, including testing, validation, and quality assurance.
   - Minimize operational disruptions and errors during implementation.
6. **Post-Implementation Evaluation:**
   - Monitor the performance and effectiveness of implemented changes.
   - Gather stakeholder feedback and evaluate the impact on system efficiency and user satisfaction.

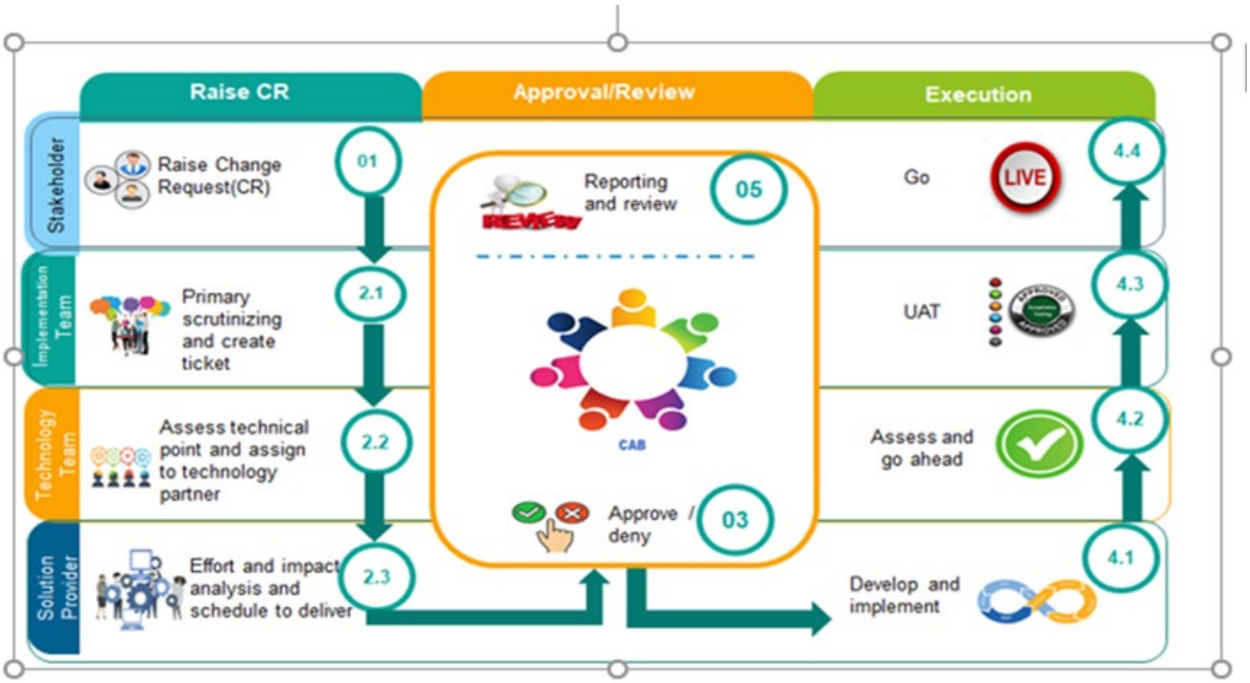


Figure: Existing change management Process

4. Duration of the Assignment

The total duration of the assignment will be nine (9) months. Both the Development & Enhancement activities and the Maintenance & Support Services shall commence from the first day of signing the contract.

5. Expected Deliverables & Deliverables Schedule

Deliverables:

Sl.	Ref. Name	Major Deliverable
1.	D-1	Project Inception Report
2.	D-2	Requirement Analysis and Finalization, Update SRS and Relevant Technical Documents.
New Development		
3.	D-3	APM (Application Performance Monitoring) Implementation
4.	D-4	Garbage cleaning process implementation
5.	D-5	Incremental database backup process implementation.
6.	D-6	Secure Audit Service Deployment
7.	D-7	SRE Dashboard Development.
8.	D-8	SRE Implementation.
Enhancement		
9.	D-9	Upgraded and Refactored Core Service Framework
10.	D-10	Latest-version Keycloak Instance
11.	D-11	Technology stake upgradation & centralized repository for service configuration

12.	D-12	Enhancement of Doptor Portal
13.	D-13	Implementation of eSign for Batch/Bulk Signing
14.	D-14	High-Performance API Gateway
15.	D-15	High-Performance Queue Manager
16.	D-16	Enhancement of Event Management, Task Management, Doptor Calendar
17.	D-17	VAPT Issue Resolution
Non-Functional Requirements		
18.	D-18	Support and Maintenance
19.	D-19	Source Code
20.	D-20	Access Credentials
21.	D-21	Technical Document Transfer
22.	D-22	Capacity Management and Knowledge Transfer
23.	D-23	Closing Report

Deliverables Schedule:

Sl.	Deliverable	Timeline
1.	D-1: Project Inception Report	End of 1st Month

2.	D-2: Requirement Analysis and Finalization, Update SRS and Relevant Technical Documents.	End of 2nd Month
3.	D-9: Upgraded and refactored Core Service Framework	End of 4th Month
4.	D-10: Latest-version Keycloak Instance	
5.	D-11: Technology stack upgradation & centralized repository for service configuration	
6.	D-3: APM (Application Performance Monitoring) Implementation	
7.	D-12: Enhancement of Doptor Portal	
8.	D-4: Garbage cleaning process implementation	End of 6th Month
9.	D-5: Incremental database backup process implementation.	
10.	D-13: Implementation of eSign for Batch/Bulk Signing	
11.	D-14: High-Performance API Gateway	
12.	D-15: High-Performance Queue Manager	
13.	D-16: Enhancement of Event Management, Task Management, Doptor Calendar	End of 9th Month
14.	D-6: Secure Audit Service Deployment	
15.	D-7: SRE Dashboard Development.	
16.	D-8: SRE Implementation.	

17.	D-17: VAPT Issue Resolution	
Non-Functional Requirements		
18.	D-18: Support and Maintenance	1st Month – 9th Month
19.	D-19: Source Code	End of 9th Month
20.	D-20: Access Credentials	
21.	D-21: Technical Document Transfer	
22.	D-22: Capacity Management and Knowledge Transfer	
23.	D-23: Closing Report	

6. Work distribution & Team Composition

The technical proposal must include a detailed Work Distribution & Team Composition plan, outlining the required number of personnel, qualifications, and job descriptions for key roles such as:

SL	Position	No. of Person
1	Project Manager	1
2	Technical Documentation Expert	1
3	Solution Architect	1
4	Business Analyst	1
5	System Analyst	1
6	Senior Software Engineer	2
7	UI/UX Expert	1
8	Database Expert	1
9	Integration Engineer	1
10	DevOps Engineer	1
11	Software Engineer	4
12	Security Expert	1
13	QA Lead	1
14	QA Engineer	2
15	Infrastructure Expert	1

16	Support Engineer	2
	Total	**22**

Qualification:

SL	Position	Minimum Qualification
Project Management		
1	Project Manager	**Job Description:** • Lead overall planning, execution, monitoring, and delivery of all Doptor development, enhancement, and support activities. • Coordinate with a2i, development teams, QA teams, and stakeholders to ensure timely milestone completion. • Ensure requirement analysis, sprint planning, resource allocation, and technical decision-making. • Maintain project documentation, risk matrix, mitigation plan, and progress dashboard. • Ensure compliance with standards, security guidelines, and government procedures. **Experience, Expertise and Educational Requirement:** i) Minimum graduate in Computer Science and Engineering/ICT. ii) 10 years of progressive experience with at least 5years' experience in managing large-scale IT projects. iii) Experience in leading such an assignment, role including software design and development. iv) Relevant certification in PMP/PRINCE2/Scrum Master, or equivalent is preferable.
2	Business Analyst	**Job Description:** • Conduct requirement analysis, stakeholder discussion, and documentation of system processes. • Prepare user stories, use-case diagrams, workflows, and requirement specifications. • Assist Sr. BA in validating requirements, managing change requests, and conducting UAT. • Coordinate with UI/UX, development, and QA teams for requirement clarification. • Support functional review of developed modules. **Experience, Expertise and Educational Requirement:**

		i) Minimum Bachelors in CS/CSE/EEE or any relevant discipline from university. ii) Minimum 8 years' professional experience in IT Industry. iii) Minimum 5 years' professional experience as a business analyst.
3	Technical Documentation Expert	**Job Description:** • Prepare user manuals, system documentation, SRS, API documentation, and release notes. • Develop structured documentation for all major modules of Doptor based on inputs from BA and development teams. • Ensure version-controlled, updated, and standardized documents following government documentation guidelines. • Assist QA and support teams by preparing troubleshooting guides and FAQs. **Experience, Expertise and Educational Requirement:** i) Bachelors in English/BBA/IT or any relevant discipline. ii) 3 years of experience in technical documentation. iii) Prepared documentation for at least two platforms.
4	Solution Architect	**Job Description:** • Lead system and solution architecture design for Doptor core system and sub-modules. • Define architecture patterns, integrations, database structures, API standards, and security models. • Review system scalability, performance, load distribution, and failover strategies. • Guide development teams with best practices and ensure alignment with cloud and on-prem standards. • Evaluate new technologies for system enhancement and optimization. **Experience, Expertise and Educational Requirement:** i) Bachelor's/Master's in CSE or any relevant discipline. ii) Minimum 7 years of experience in software development, with at least 2 years in a solution architect role. iii) Relevant certification in TOGAF, AWS, Azure, Google, Oracle Solution Architect or equivalent is preferable.
5	System Analyst	**Job Description:** • Translate business requirements into technical requirements, workflows, data models, and system diagrams. • Prepare SRS, system design documents including sequence diagrams, ERD, API specifications, and module interactions.

		• Work closely with Solution Architect to finalize system logic. • Support developers by clarifying system behaviors and constraints. • Validate functional and system-level alignment before development. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 5 years of experience in analysis, with at least 2 years in system analysis and documentation.
6	Sr. Software Engineer	**Job Description:** • Develop scalable backend modules, APIs, and perform critical fixings/issue resolutions for Doptor. • Implement business logic, database queries, authentication, and third-party integrations. • Ensure coding standards, secure API design, and high-performance backend logic. • Conduct code reviews, performance tuning, and database optimization. • Support solution design and system-level enhancements. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 7 years' experience in programming using PHP, Python, RDBMS & NoSQL for medium to large scale web-based applications. iii) Experience in backend programming for 2 medium to large scale projects.
7	UI/UX Expert	**Job Description:** • Lead UI/UX design for Doptor web and mobile platforms. • Prepare wireframes, mockups, prototypes, and visual interfaces aligned with government usability guidelines. • Ensure accessibility, user experience consistency, and responsive design. • Conduct user research, usability testing, and interaction design improvements. • Collaborate with frontend and BA teams for seamless UI implementation. **Experience, Expertise and Educational Requirement:** i) Bachelor's in any relevant discipline.

		ii) Minimum 6 years of experience in UI/UX design for medium to large scale web-based applications.
8	Database Expert	**Job Description:** • Support database optimization and maintenance for all modules of Doptor. • Optimize queries, indexes, and stored procedures for performance improvement. • Manage database backups, restoration, and routine health checks. • Support DBA in migrations, tuning, and resolving DB-related issues. • Ensure database alignment with application requirements. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 8 years of experience in database design, database programming, query optimization, database backup and restoration. iii) Experience in database programing, database optimization for 2 medium to large web-based applications.
9	Integration Engineer	**Job Description:** • Plan and execute system-to-system integration using REST, SOAP, and middleware. • Develop APIs, manage integration endpoints, and handle authentication protocols. • Diagnose integration issues and ensure proper data synchronization. • Document integration flows and prepare test scripts. • Work with external government agencies for API onboarding. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 7 years of experience in software development, with at least 2 years in system integration role. iii) Experience in at least two integration projects using REST, SOAP, or middleware tools.
10	Software Engineer	**Job Description:** • Develop backend modules, REST APIs, and server-side business logic. • Perform issue fixing and resolution for the system.

		• Implement database interactions, authentication workflows, and validation rules. • Support senior backend engineers in refactoring and system improvements. • Conduct unit testing, bug fixing, and documentation of backend modules. • Ensure coding standards and security compliance. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 4 years of profound experience in backend programming and technologies. iii) Experience needs to focus on multiple development platforms including PHP.
11	Security Expert	**Job Description:** • Lead implementation of application and infrastructure security measures. • Configure security tools, firewalls, WAF, IAM, and encryption mechanisms. • Develop security guidelines and enforce secure coding practices. • Respond to security incidents and perform forensic analysis. • Support compliance with GDPR, ISO27001, and government security standards. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 7 years of experience in web security implementation. iii) Certification in CISSP, CEH, or equivalent is preferable.
12	QA Lead	**Job Description:** • Lead QA strategy, planning, and execution for all Doptor modules. • Supervise QA engineers, review test cases, and manage defect lifecycle. • Oversee functional, regression, integration, performance, and UAT testing. • Ensure quality metrics and testing standards are maintained. • Prepare QA reports, dashboards, and improvement recommendations. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) At least 10 years of progressive experience in Quality Assurance. iii) CSQA, CMSQ ISTQB Certified Tester is preferable.

13	QA Engineer	**Job Description:** • Develop test cases, perform manual/automated testing, and report defects. • Conduct functional, UI, smoke, and regression testing. • Work with BA and developers to validate requirements and fixes. • Track bugs using appropriate tools and ensure retesting. • Maintain test documentation and support UAT. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 5 years of experiences in software testing and quality assurance for medium to large scale web-based applications.
14	Infrastructure Expert	**Job Description:** • Manage server infrastructure, virtualization, storage, and deployment systems. • Troubleshoot hosting issues, performance bottlenecks, and network-related problems. • Support production environment, monitoring, and high-availability setup. • Work with DevOps, security, and DBA teams during releases. • Prepare infrastructure documentation and capacity planning. **Experience, Expertise and Educational Requirement:** i) Bachelor's in CSE or any relevant discipline. ii) Minimum 7 years of experience in infrastructure, with at least 2 years in engineering roles. Supported at least two IT environments.
15	DevOps engineer	**Job Description:** • Implement CI/CD pipelines, containerization, and automated deployment workflows. • Manage Kubernetes, Docker, Terraform, Ansible, and cloud infrastructure. • Optimize application performance through monitoring and scaling. • Coordinate with developers, QA, and hosting teams for release cycles. • Ensure secure and reliable DevOps practices. **Experience, Expertise and Educational Requirement:** i) Bachelor's degree in Computer Science, Information Technology, Software Engineering, or a related discipline.

		ii) Minimum 5 years of hands-on experience in DevOps roles supporting medium- to large-scale applications and hosting infrastructures. iii) Relevant professional certifications (e.g. AWS Certified DevOps Engineer, Kubernetes Administrator, Azure DevOps, or equivalent will be an added advantage.
16	Support Engineer	**Job Description:** • Provide first-level support to Doptor users through phone, email, and ticket system. • Log issues, perform initial troubleshooting, and escalate unresolved cases. • Guide users with system usage, basic configurations, and FAQs. • Maintain ticket records and ensure timely closure as per SLA. • Support training and awareness activities. **Experience, Expertise and Educational Requirement:** i) Minimum graduate in any subject ii) At least 2 years of experience on providing software support services

Joint Venture

Multiple Companies having technical and legal competencies for providing such services can apply jointly but they must have legal agreement among them where one company needs to be led. The joint venture company jointly needs to fulfil all conditions mentioned in this ToR. The joint-venture agreement needs to have clear identification about each responsibility matrix along with IPR. In case of JV, JV agreement as per rule 70(2), PPR 2025, Schedule 12 to be used.