Ministry of Finance, Planning and Economic Development

Department of State Accounts

PROCUREMENT DOCUMENT

(Two Envelope System: Single-Stage Two Envelope Bidding Procedure)

Volume II

Schedule of Requirements (SOR)

Procurement of Design, Development and Implementation of a Payroll System for Government Organizations

IFB No: DSA/PROC/NCB/2026/01

Employer:

Director General
Department of State Accounts
Room Number 101, 1st Floor,
The Secretariat, Colombo 01.

29 March 2026

Table of Content

1. Background

1.1 Introduction

The Department of State Accounts, functioning under the Ministry of Finance, Planning and Economic Development (MOFPED), plays a critical role in advancing public financial reporting in Sri Lanka. As a key institutional body within the Public Financial Management (PFM) framework, the department is entrusted with formulating and supporting policies that promote sound, transparent, and accountable financial practices across government entities. It provides technical guidance and oversight to ensure the accuracy, integrity, and compliance of public financial reporting in alignment with national and international standards.

In line with this mandate, the Department originally implemented the Government Payroll System (GPS) in 1996. Since its inception, the GPS has been utilized by a broad range of public sector institutions, including government ministries, departments, special spending units, provincial councils, local authorities, and select statutory bodies. However, despite its long-standing utility, the GPS has become technologically obsolete and is no longer capable of supporting modern operational demands or adapting to evolving information security requirements.

The limitations of the existing system are multifaceted. Its outdated architecture prevents further enhancement, and its weak security protocols expose it to risks of manipulation and payroll-related fraud, undermining the credibility and efficiency of government financial operations. Furthermore, the current system lacks the flexibility and scalability required to function as an integrated human resource and payroll management platform, thereby impeding institutional productivity and efficiency.

In light of these challenges, the Department of State Accounts (DSA) recognizes the urgent need to transition to a technologically advanced, secure, and integrated payroll processing system. This modernization initiative will be guided by global best practices and emerging trends in information and communication technology.

1.2 Key Functions

I. Employee Information Management

- Maintain employee profiles including personal details, job titles, departments, salary grades, and bank information.
- Track employment status (e.g., probation, confirmed, resigned, retired).

II. Salary Structure and Pay Components Configuration

- Define multiple salary structures based on designation, grade, or department.
- Configure earnings (basic salary, allowances, incentives) and deductions (taxes, loans, pension).

III. Automated Payroll Calculations

- Calculate gross earnings, statutory/non-statutory deductions, and net pay.
- Handle prorated salaries, overtime, arrears, and adjustments.

IV. Leave and Attendance Integration

- Integrate with leave and attendance to adjust payroll based on absenteeism, holidays, or approved leave.

V. Loan and Advance Management

- Administer employee loans, including eligibility, instalment scheduling, EMI recovery, and outstanding balance tracking.

VI. Payslip Generation and Distribution

- Generate itemized payslips and tax certificates.
- Allow online access via Employee Self-Service (ESS) portal or email delivery.

VII. Statutory Compliance and Reporting

- Deduct and report taxes, social security, provident fund, and pension contributions in compliance with local laws.
- Generate regulatory reports for auditors and finance departments.

VIII. Employee Self-Service (ESS) Portal

- Enable employees to access payslips, apply for loans, view tax statements, and update personal information.

IX. Payroll Processing and Approval Workflow

- Define multi-level approvals for payroll processing and exception handling.
- Batch-wise processing by departments or entities.

X. Audit Trail and Change History

- Maintain detailed logs of all changes to payroll data and system configurations.
- Ensure accountability and traceability for audits.

XI. Bank Transfer and Payment Processing

- Generate bank files for salary disbursement.
- Interface with Treasury or ERP systems for fund transfers.

XII. Reporting and Dashboards

- Provide standard and custom reports (e.g., salary register, headcount, variance, T10, T9).
- Support data export for Excel.

XIII. Security and Access Control

- Role-based access to functions and data (admin, HR, finance, auditor).
- Use of authentication, encryption, and user activity monitoring.

XIV. Retroactive and Arrear Calculations

- Support backdated salary changes and automatic arrears computation.

XV. AI Driven Payroll Process and Decision Making Support

- The proposed Government Payroll System shall leverage Artificial Intelligence (AI) technologies to enhance accuracy, efficiency, and fiscal governance across all payroll operations. AI capabilities will be utilized to automate data validation and anomaly detection, forecast payroll expenditures for improved budget planning, optimize large-scale payroll processing, detect and prevent fraudulent transactions, and support compliance monitoring. Additionally, AI-driven chatbots and analytics tools will provide self-service support to employees and decision-makers, while predictive models will enable proactive policy impact assessments and continuous system improvement. These AI integrations will ensure faster processing times, reduced errors, strengthened internal controls, and data-driven decision-making in alignment with national financial management objectives and international best practices.

1.3 Key Objectives of Payroll Implementation

The primary aim of the new payroll system is to modernize and streamline government payroll operations through the following strategic objectives:

I. Enhancing Operational Efficiency and Transparency in Payroll Processing
The system is designed to significantly improve the efficiency of payroll-related workflows by automating complex calculations, reducing manual intervention, and minimizing the risk of human error. It ensures transparency by providing traceable audit logs, clear reporting mechanisms, and real-time access to payroll records for authorized personnel. This results in faster payroll execution, greater accountability, and improved employee confidence in the payroll process.

II. Enabling Centralized Administration and Oversight Across Government Entities
The payroll platform facilitates centralized control and monitoring of payroll activities across multiple ministries, departments, and government agencies. Through a unified interface, authorized administrators can manage payroll structures, monitor disbursements, and ensure policy consistency across all entities. This centralized approach also enables standardization of procedures and easier consolidation of payroll data for national reporting and analysis.

III. Supporting Compliance with Data Protection and Information Security Requirements
In alignment with prevailing data protection regulations and government IT security standards, the system incorporates robust security features. These include role-based access controls, encrypted data transmission, secure authentication protocols, and detailed activity logs. The system ensures that sensitive employee information is handled with the highest level of confidentiality and integrity.

IV. Facilitating Digital Governance and Service Delivery

The payroll system serves as a foundational component of the government's digital transformation agenda. By digitizing payroll services, it enhances the quality and responsiveness of public sector administration. Employees gain access to self-service features such as online payslips, loan applications, and tax certificates, while administrators benefit from integrated workflows and automated approvals. This contributes to a more efficient, transparent, and citizen-focused public service delivery framework.

1.4 Scope of Work

- This section provides a brief overview of scope of work for PIP (Payroll Implementation Partner).
- This bidding document refer to the successful bidder as a PIP (Payroll Implementation Partner).

Key areas of scope of work	Summary of Scope of Work
1. Prepare and submit Project Management Plan	The Application Vendor's Project Manager is required to prepare a comprehensive Project Management Plan (PMP) that outlines how the Government Payroll System implementation will be executed, monitored, and controlled. It needs to refer to the project implementation schedule given. This plan should define key elements such as the project scope, timelines, milestones, resource allocation, risk management strategies, quality assurance measures, and communication protocols. The PMP must align with contractual obligations and reflect best practices in project governance. It should also include a detailed work breakdown structure (WBS), Gantt chart, and stakeholder engagement plan. By clearly articulating these components, the Project Manager ensures effective coordination among teams, timely delivery of deliverables, and alignment with the overall goals of the client organization. The SIP must adopt the Agile methodology for system development, as stipulated in the project framework. Under this approach, SIP is expected to execute development through two cycles of change to the product, each involving active engagement and feedback from end-users to ensure that the evolving solution meets functional and operational expectations.
2. Requirement Study	The Software Implementation Partner (SIP) shall be responsible for carrying out the following key activities to support the finalization of the Requirements Specifications for the Government Payroll System: **(a) Conducting an As-Is Study:** Undertake a comprehensive assessment of the existing functions, services, and processes related to government Payroll System management. This includes analyzing current workflows and their interfaces with external entities such as Treasury departments, line ministries, and statutory institutions. **(b) Business Process Reengineering and Definition of To -Be Processes:** Design optimized future-state (To-Be) business processes through

Key areas of scope of work	Summary of Scope of Work
	systematic reengineering of current Payroll System workflows. These revised processes should incorporate recognized best practices in Payroll System management. The outcome shall be compiled into a "To-Be Study Report," which must be reviewed and approved by the relevant authority, such as the Department of Public Finance. **(c) Finalization of Software Requirement Specification:** The successful bidder shall engage with all key stakeholders including representatives from procuring entities, government oversight bodies, vendors, and the Department of State Account to define, document, and finalize a comprehensive Software Requirements Specification (SRS). This document must: • Clearly capture and represent the functional and non-functional requirements of the Government's Payroll System (eGPS). • Serve as the baseline reference for iterative development cycles under the Agile methodology, ensuring that all subsequent design, development, and testing activities are aligned with approved requirements. As part of this process: I. UI/UX Prototyping: • The bidder shall develop interactive UI/UX prototypes that reflect the proposed system workflows, user journeys, and visual design standards. • These prototypes must be presented to the Department of State Account for review and formal approval prior to commencing detailed development activities. II. Change Management and Updates: • Following review sessions, the bidder must incorporate all feedback and required modifications into the SRS document to ensure accuracy and completeness. • The payroll process will accommodate two rounds of revisions to the SRS, during which the bidder shall update and resubmit the document reflecting stakeholder input and DSA guidance. III. Approval and Baseline: • Once finalized, the approved SRS will act as the authoritative baseline for the system's Agile development lifecycle, guiding sprint planning, system design, and acceptance testing.
3. Supply, installation, development customization and commissioning of Payroll system	The Software Implementation Partner (SIP) shall be responsible for the design, development or customization, and successful implementation of the proposed Government Payroll System. The scope of services to be delivered by the SIP includes the following: **(a) Design, Development/Customization, and Commissioning:** The Payroll System application and all required system software components, followed by their deployment and commissioning in accordance with the approved specifications.

Key areas of scope of work	Summary of Scope of Work
	(b) System Integration and Configuration: Supply, install, configure, and commission the necessary interfaces and integration modules to enable secure and seamless data exchange between the Government Payroll System and other relevant information systems. The Software Implementation Partner (SIP) shall be responsible for preparing comprehensive and well-structured documentation covering all aspects of the Government Payroll System. This includes, but is not limited to, a detailed Technical Architecture Document outlining the system architecture, infrastructure design, integration points, configuration parameters, and security controls. Additionally, the SIP must develop thorough Operational Procedure Manuals and End-User Manuals to support system administration, troubleshooting, and routine use by various stakeholder groups. All architecture and supporting documentation shall be submitted for formal review and approval by the Department of State Accounts or by the Independent Assurer appointed by the Department. It is the responsibility of the SIP to ensure that any feedback, observations, or identified issues from the reviewing parties are promptly addressed. Corrections and clarifications must be made without undue delay, and revised versions must be resubmitted until full compliance and approval are achieved. Timely and accurate documentation is critical to ensuring system sustainability, operational readiness, and alignment with national governance standards.
4. Sizing the IT infrastructure architecture for eGPS implementation	The Software Implementation Partner (SIP) shall be responsible for designing and providing a detailed specification of the Information Technology (IT) infrastructure required for the successful implementation, deployment, and operation of the Payroll System. This includes determining the necessary computing, storage, networking, and security components based on system architecture, performance expectations, scalability requirements, and integration needs. The proposed infrastructure specification must be aligned with the deployment environment designated by the Government and next four-year operations. It is important to note that the SIP shall be fully accountable for implementing the solution within the prescribed hosting environment as public/private cloud based on the government guideline, as determined by the Department of State Accounts. The SIP must ensure that the system is configured and optimized for high availability, security compliance, disaster recovery, and efficient performance within the selected hosting infrastructure. Additionally, the SIP is expected to coordinate with relevant government IT authorities to facilitate smooth deployment and integration with existing platforms and services. The bidder is required to provide a comprehensive Bill of Materials (BOM) outlining all components, services, and resources that will be provisioned to the Department of State Accounts through the Lanka Government Cloud Solution. The BOM should include detailed

Key areas of scope of work	Summary of Scope of Work
	specifications, quantities, configurations, and any associated costs to ensure full transparency and alignment with the project requirements.
5. Training of staff at DSA	The Software Implementation Partner (SIP) shall be responsible for delivering comprehensive training programs to the relevant personnel of the Department of State Accounts (DSA), as well as other designated end-users and stakeholders of the Payroll System. These training sessions must be designed to ensure that all participants gain a thorough understanding of the system's functionalities and are adequately prepared to operate and maintain it effectively. The training shall be organized as follows: **Training of Trainers (ToT):** • Provide hands-on training for business users, focusing on the day-to-day operational usage of the Payroll System. • Cover key functionalities, Payroll System processing workflows, employee data management, and report generation. • Include practical demonstrations and scenario-based exercises to ensure effective learning. • Supply user manuals and quick reference guides for post-training reference and support. **Technical Training for Department of State Account IT Staff:** • Conduct in-depth technical training sessions for system administrators and IT personnel of DSA. • Address administrative tasks, system configuration, backend management, user role and access control, and troubleshooting procedures. • Include training on routine maintenance, system health monitoring, data backup procedures, and performance optimization. • Ensure that technical staff are capable of independently managing, supporting, and maintaining the Government Payroll System post-deployment. All training materials, session plans, and schedules must be submitted for prior approval by DSA, and training shall be delivered in alignment with the overall system implementation timeline. SIP shall also provide refresher training sessions and on-demand technical assistance during the post-implementation period to ensure effective knowledge transfer and long-term sustainability of the solution.
6. Data migration	The Software Implementation Partner (SIP) shall be fully responsible for the end-to-end data migration process required for the successful implementation of the Payroll System. This includes the identification, extraction, cleansing, transformation, and loading of all relevant existing digital records. The scope of migration shall encompass all applicable employee records, Payroll System history, master data, and any other supporting datasets necessary to ensure that the system is fully functional and ready for

Key areas of scope of work	Summary of Scope of Work
	operational use by the Department of State Accounts and the respective Project Management Units (PMUs). SIP must ensure that: • All required data is accurately migrated (where not already in digital format), • Data integrity and consistency are maintained throughout the migration process, • Adequate validation checks are performed to ensure completeness and correctness, • The final data set is successfully loaded into the Payroll System prior to the official go-live. The SIP shall also be required to coordinate closely with DSA during this process and provide full documentation of the migration methodology and results. It is important to note that, following the go-live of the Payroll System, the responsibility for entering and maintaining transaction data will rest with the authorized staff of DSA. SIP's responsibility will be limited to ensuring the readiness of historical and structural data for the system to become operational from Day One.
7. Application support engineers on site.	The primary Help Desk facility for the Government Payroll System will be established and managed by the Department of State Accounts. However, the Software Implementation Partner (SIP) is required to provide dedicated support resources to ensure timely and effective resolution of user queries and technical issues during the system's rollout and operational phases. Need to align to the given Service Level Agreement (SLA) Specifically, SIP shall allocate two (2) qualified system support agents to be stationed at the MOFPED. These agents must be capable of handling inbound calls, logging issues, providing first-level support, and escalating complex technical matters as per the established support protocols. These resources must be available during standard working hours (or as agreed upon with DSA), and their performance shall be monitored as part of the broader Service Level Agreement (SLA) to ensure adherence to response and resolution timelines.
8. Third Party Testing for Security and Functionality	The Software Implementation Partner (SIP) shall be obligated to provide full support and timely resolution of all issues identified during the testing and assessment processes conducted by authorized third-party testing teams and the Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) or the Department of State Account nominated Party. This includes, but is not limited to: • Functional defects, • Non-Functional defects • Product Code and Architecture Issues • Accessibility issue • Performance Issues • Security Issues

Key areas of scope of work	Summary of Scope of Work
	• Data Migration Issues Any other non-conformities detected during independent quality assurance and security testing phases. Upon receiving the test reports or issue logs, SIP shall be required to analyze, address, and rectify the reported issues comprehensively within a maximum of two (2) resolution cycles, unless otherwise agreed upon in writing with the Department of State Accounts. Each cycle shall include the process of issue verification, resolution, and revalidation. SIP must ensure that the system meets the required quality and security benchmarks established by both the independent testing team, internal QA team and Sri Lanka CERT, prior to system acceptance and go-live. Failure to comply with this requirement may result in delay of system certification, impact on milestone approvals, and potential enforcement of contractual remedies as outlined in the agreement. The SIP needs to align to the given Service Level Agreement (SLA) mentioned in each Sprint level certifications.
9. Warranty, operations and maintenance support for software	The Software Implementation Partner (SIP) shall be responsible for providing comprehensive warranty, operations, and maintenance (O&M) services for all components software and any other items supplied under this project. These services shall extend throughout the duration of the implementation contract and continue for a period of **four (04) years warranty and three (03) years post warranty,** during the warranty and operations & maintenance phase of the Payroll System. The scope of these services shall include, but not be limited to, the following: **(a) Defect-Free System Operations:** SIP shall ensure that all systems and components supplied by them operate in a stable and error-free manner. Any issues affecting the continuity, accuracy, or usability of the system must be promptly identified and resolved by the SIP without causing disruption to Payroll System operations. **(b) Comprehensive Application Support:** SIP shall provide full operations and maintenance support for the Government Payroll System software, which includes: • Fixing defects, errors, or failures in functionality refer to the SLA (Annexure II). • Resolving integration related issues with interfacing systems • Addressing performance degradation and optimization needs • Identifying and mitigating security vulnerabilities • Correcting any other application-level issues that arise during usage **(c) Warranty Coverage for Third-Party Components:** SIP shall provide warranty services for any third-party systems, software tools, or platforms procured and implemented as part of the Payroll System.

Key areas of scope of work	Summary of Scope of Work
	(d) Support for Product Feature Modifications: SIP shall provide technical assistance and development support for modifications or enhancements to existing product features, as may be required by the Department of State Accounts to adapt the system to evolving business needs. **(e) Technology Stack Upgrades:** SIP shall be responsible for upgrading and maintaining compatibility of the system with the latest stable versions of the operating system, development frameworks, database systems, and web servers. These upgrades must be technically feasible and aligned with industry best practices. Prior to the annual maintenance payment, a technical feasibility assessment shall be conducted to verify the relevance and readiness of the proposed upgrades. If the SIP not update the above mention area the Department of State Accounts have write to take a penalty mention in the SLA. All warranty and O&M activities must be carried out in accordance with the service-level standards defined in the contract and must be performed without any degradation to system availability, performance, or security. The Selected Implementation Partner (SIP) shall be entitled to warranty maintenance payments on a quarterly basis during the warranty period. These payments will be subject to a comprehensive review and approval process carried out by the Department of State Accounts (DSA). Before authorizing each quarterly warranty maintenance payment, the DSA will undertake a structured verification process, which includes the review and validation of the following project artifacts and technical deliverables: I. Documentation and Specifications • Software Requirements Specification (SRS): Verification that the system continues to operate in alignment with the approved SRS. • Test Cases and Test Results: Confirmation that appropriate test cases have been executed and documented, with results meeting the expected outcomes. • User Manuals and Guides: Review of the latest end-user documentation to ensure accuracy, clarity, and incorporation of any system updates. II. System Components and Technical Environment • Operating System (OS): Validation that all deployed servers are up-to-date with the latest security patches and updates. • Web Server: Confirmation that the web server is patched, optimized, and operating in compliance with security standards. • Database: Review of database updates, patches, and optimization measures to ensure security, stability, and performance. III. Compliance and Security • Ensuring that all applied patches and updates are aligned with government ICT security guidelines and industry best practices.

Key areas of scope of work	Summary of Scope of Work
	• Verification that the system remains stable and functional after each applied update or modification. Only upon satisfactory completion of this review will the quarterly warranty maintenance payment be released to the SIP.

2. Source Code

Updated source code, application deployment files, and all configuration files related to the complete solution shall be maintained and submitted as part of the project deliverables.

It shall be noted that implementation stage, and at the end of each quarterly period during the operations and maintenance phase, the System Implementation Partner (SIP) is required to submit the latest versions of all system artifacts. These include, but are not limited to, updated system design documents, technical specifications, source code, application deployment packages, configuration files, user manuals, administration manuals, training manuals, software change logs, and any other applicable deliverables listed under this section. Release of payments associated with these milestones shall be strictly subject to the receipt, verification, and acceptance of the above deliverables.

The MOFPED will arrange and manage the Escrow Agreement for the SIP. The SIP shall fully comply with and adhere to all procedures, obligations, and requirements defined within the Escrow Agreement, including timely submission of escrow materials in the format and frequency specified.

3. User Requirement for the System

The table below presents the current distribution of employees processed through the government payroll system. For infrastructure design and capacity planning purposes, the overall payroll workload has been segmented into a maximum of ten (10) logical segments. The bidder is required to use this table as a key reference when determining system sizing parameters, performance benchmarks, and scalability provisions. Furthermore, the proposed solution must accommodate future growth and allow for seamless expansion of capacity in line with anticipated increases in employee volumes and organizational requirements.

System Login and User Access

The proposed Government Payroll System shall be designed as a national-level platform capable of supporting a large number of employees and authorized government officers accessing the system concurrently. The solution shall provide secure login access for all government employees through the Employee Self-Service Portal, as well as for payroll administrators, HR officers, accountants, payroll users, approving authorities, auditors, and treasury officials.

The system shall be scalable to accommodate high volumes of simultaneous logins, particularly during peak payroll processing periods, salary disbursement cycles, and statutory reporting deadlines. **The vendor shall ensure that the system architecture supports future expansion in the number of employees, institutions, and operational users without performance degradation or service interruption.**

Table 3.1 - Number of users (Operational)

User Type	No. of Users
HR Admin	2,500
HR User	5,000
Accountant	2,500
Payroll User	6,000
Loan User	2,500
Other User	1,500
Total	**20,000**

Table 3.2 - Number of Employees (Employee Self Service Portal)

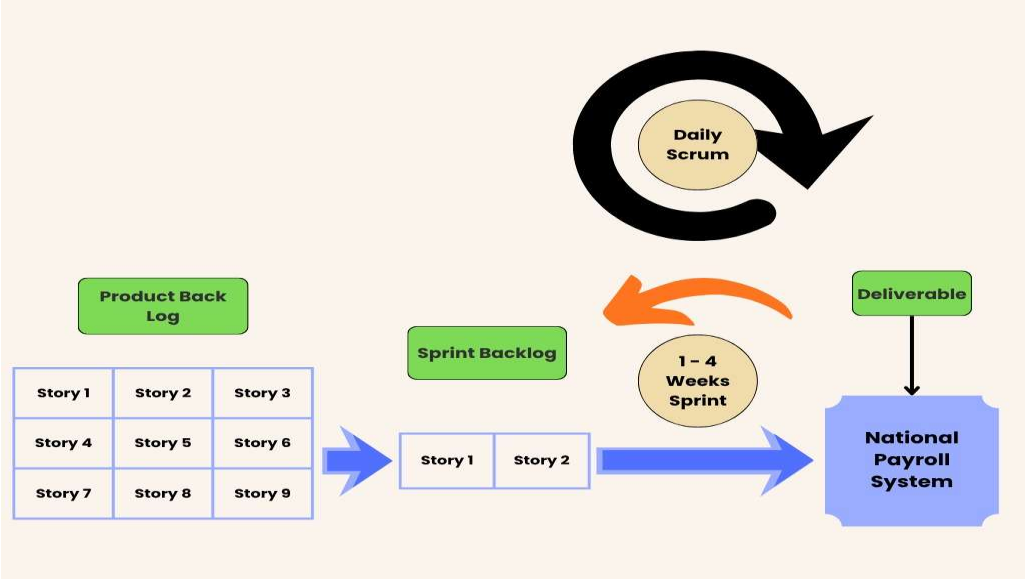
Employee Category	No. of Users
Central Government	1,000,000
Provincial Councils and Local Authorities	500,000
Total Number of Employees	**1,500,000**

4. Implementation Approach of Payroll Application

4.1 Agile Approach and Time Line

(a) The (DSA) shall place significant emphasis on ensuring the long-term sustainability of the testing process while verifying and validating the functional accuracy of the system. This shall be achieved through a phased implementation strategy guided by the principles of the Agile methodology, enabling iterative testing, continuous feedback, and timely refinements throughout the project lifecycle.

(b) The Software Implementation Partner (SIP) shall develop the eGPS in accordance with Agile development practices, ensuring incremental delivery of functional components. The SIP shall also be responsible for providing comprehensive and structured training to the designated end users, enabling them to effectively practice, evaluate, and adopt each delivery or output as it is introduced.



(c) The Software Implementation Partner (SIP) shall utilize project management and collaboration tools that support the Agile methodology, with functionality equivalent to JIRA or other industry-recognized Agile tools. The DSA shall procure and maintain the necessary licenses for such tools until the completion of the project to ensure effective tracking, sprint planning, backlog management, and progress monitoring.

(d) As part of the agreed project plan, the SIP shall implement the scheduled activities on a monthly basis, in coordination and agreement with the DSA. During the implementation phase, the SIP shall prepare all required documentation as specified below and ensure that all processes are conducted in full compliance with the relevant procedures.

The SIP shall acknowledge, adopt, and strictly adhere to the Standard Operating Procedures (SOPs) developed by the DSA in accordance with ISO 27001 and ITIL standards. These SOPs shall comprehensively cover, but not be limited to, the following operational areas:

- Infrastructure Installation and Configuration
- System Monitoring and Performance Management
- Data Backup and Restoration Procedures
- Information Security Policies and Controls
- Business Continuity Planning
- Disaster Recovery Procedures
- Operational Workflow Management

The SIP shall ensure that all implementation activities align with these SOPs and meet the standards defined therein.

(e) The SIP shall fully support and comply with all activities outlined in the SOPs and shall bear complete responsibility for executing the Release Management Process as detailed in the SOP documentation.

Furthermore, the SIP shall prepare and submit to the DSA, for prior review and approval, the standardized formats for all key deliverables, including but not limited to:

- Software Requirements Specification (SRS)
- System Design Document
- Test Strategy Document
- Test Cases and Test Results
- Software Release Documentation
- User Manual
- Installation Guide
- IT Policy Document

The bidder shall clearly specify the proposed structure and format of these deliverables in their proposal submission to ensure alignment with project governance requirements.

4.2. Implementation Schedule

The following Table 4.2.1 outlines the implementation schedule for the eGPS. This schedule specifies the key deliverables and associated timelines to be achieved during each phase of the project.
In addition to the specific deliverables listed in the table, the Software Implementation Partner (SIP) shall be fully responsible for completing all activities and tasks stipulated in the Scope of Requirements (SoR) that are applicable to the respective project phase. These activities shall be executed in strict compliance with the approved project plan, agreed methodologies, and quality assurance standards.

Key Notes for Table 4.2.1:

(a) "**Go-live**" shall refer to the date on which the proposed eGPS solution is fully operational in accordance with the requirements specified in this Request for Proposal (RFP), together with any subsequent changes mutually agreed upon and formally signed off by the Software Implementation Partner (SIP). The Go-live milestone shall only be deemed complete once all acceptance tests have been successfully conducted and concluded to the satisfaction of the Department of State Accounts (DSA).

(b) The SIP shall be responsible for executing Change Management and Communications Management activities strictly in accordance with the agreed strategies and plans for these workstreams. These activities shall be completed within the overall project timelines and in alignment with the project governance framework.

(c) Upon completion of Go-live, and at the end of each quarter during the Operations and Maintenance (O&M) support period, the SIP shall submit the following updated deliverables to the MOFPED:
- System design documents
- Functional and technical specifications
- Source code for all customized components (If COTS product only the customized area)
- Application deployment packages
- User manuals
- Administration manuals
- Any other applicable deliverables required under the Contract

All deliverables shall reflect the latest system configuration, incorporating any changes implemented during the respective quarter.

(d) The SIP shall maintain all project documents and manuals in an up-to-date manner throughout the Contract period, ensuring that any changes to system functionality are accurately documented. A revision history log shall be maintained for all updates to track modifications over time. It is noted that the timeline for each milestone in the project plan will be enforced individually, even if certain milestones are dependent on others. Any delay in a precedent milestone will result in cascading penalties for subsequent dependent milestones. Accordingly, the SIP shall ensure robust project management practices to mitigate such risks.

(e) The Go-live of the eGPS solution shall occur only after formal certification by an independent third-party agency appointed for this purpose. The SIP shall resolve all gaps and deficiencies identified during testing to the complete satisfaction of the DSA prior to the Go-live declaration.

(f) Payments during the O&M phase shall be contingent upon the successful demonstration of the Service Level Agreement (SLA) measurement process and the generation of SLA compliance reports for the performance indicators defined in Annexure II. The SIP shall implement, customize, or develop any additional tools necessary to accurately record and report these performance indicators.

(g) In addition to the requirements under clause (d), upon completion of Go-live and at the end of each quarter during the O&M phase, the SIP shall submit to the DSA the following deliverables:

Updated system design documents and specifications

- The application's web server and database must be regularly updated with all relevant security patches, performance improvements, and version upgrades released by the respective vendors. This activity should be planned and carried out in close consultation with the Department of State Accounts (DSA), which will review, approve, and oversee the patching and upgrade process to ensure compliance with government IT policies and security standards. If, at any point, the web server or database environments are found to be outdated or not maintained at the required update levels, the State Accounts Department reserves the right to suspend all Operational and Maintenance (O&M) payments until the necessary updates and compliance measures have been fully completed and verified. Complete and up-to-date source code
- Application deployment files
- User manuals
- Administration manuals
- Training manuals
- Software change logs
- Any other deliverables listed in this section

The payment of fees associated with these milestones shall be strictly conditional upon the receipt, review, and acceptance of the above deliverables by the DSA.

Table 4.2.1. Implementation Schedule

#	Main Module	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12	M 13	M 14	M 15	M 16	M 17	M 18	M 19	M 20	M 21	M 22	M 23	M 24	Y 1	Y 2	Y 3	Y 4
1	Project Management Plan																												
2	Discovery Session																												
3	System Administration																												
4	Employee Master File, Leave & Attendance																												
5	Employee Movement																												
6	Transaction Module																												
7	Loan Module																												
8	Payroll Process																												
9	Salary Revision																												
10	Offline Payroll Tool																												
11	Reports																												
12	Interfacing																												
13	Dash Board																												
14	Pilot Run																												
15	Operational Acceptance																												
16	Warranty and Maintenance																												
		Activity Ongoing																											
		QA and Payment Milestones																											

Note: UAT must be completed before each payment milestones

5. Desired Future State

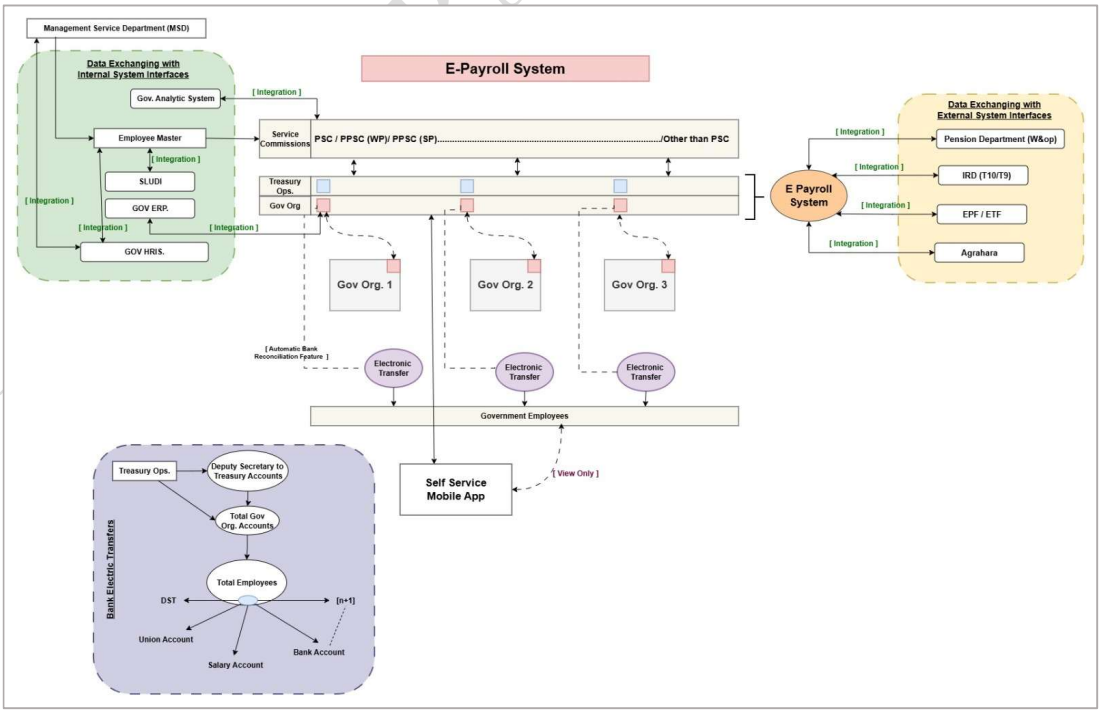
Functional and Technical Overview – eGPS

This section provides a summary of the functional and technical architecture of the proposed eGPS application. It outlines the broad functional architecture, key system features, the range of information and transaction services to be delivered, the intended target user groups, and related support services.

The detailed business and technical requirements specifications for the eGPS are provided in Annexure I of this document. These requirements have been developed with the objective of assisting bidders participating in the eGPS Implementation Partner selection process to:

- Understand the broad system requirements and intended scope.
- Accurately assess the effort, resources, and cost required for successful implementation.
- It is important to note that the requirements specifications discussed in this section, Annexure I, are preliminary in nature and intended as guidance for proposal preparation. The Software Implementation Partner selected through this procurement process shall, as an initial project activity, conduct a detailed study and analysis of all business functions, processes, and services to be automated through the eGPS.
- Following this analysis, the Implementation Partner will prepare a Final Requirements Specification Document that:
- Consolidates the outcomes of the detailed study.
- Reflects the agreed functional, technical, and operational requirements.
- Serves as the baseline reference for the design, development, configuration, testing, and implementation of the eGPS solution.

Figure 5.1: eGovernment Resource Planning Interface



The system is fully integrated with the National eGovernment Resource Planning (NeRP) platform to ensure seamless information flow across government departments and agencies.

eGPS System – High Level Integration Architecture

The diagram illustrates the overall end-to-end data flow, integrations and stakeholder interactions related to the Government of Sri Lanka E-Payroll System.

There are three main integration domains:

I. Internal System Interfaces (Government Internal Systems)

These are systems within MSD / Treasury ecosystem that exchange employee-related data into the eGPS:

- Government HRIS
- SLUDI (Sri Lanka Unique Identification)
- Government ERP
- Government Analytics System
- Employee Master Database

These internal integrations ensure that employee profile data, HR records and organizational assignment data are automatically passed into the eGPS engine.

II. Government Organizations Using the eGPS

Different government organizations (Gov Org 1 / Gov Org 2 / Gov Org 3 … etc.) interact with the eGPS for monthly payroll processing.

Data flows include:

- Service Commission (PSC / PSPC / WPU / PPSC)
- Treasury Operations
- Organization level payroll processing
- Automatic Bank Reconciliation
- Electronic Payment Transfers to employee accounts

Government employees are the beneficiaries and they also have *"view only"* capabilities using the Self-Service Mobile App.

III. External System Interfaces (External Stakeholders)

Payroll outputs are transferred automatically to mandatory external institutions:

- Department of Pension
- Department of Inland Revenue
- EPF / ETF Authorities
- National Institute of Trust Fund (NITF)

These integrations ensure compliance, statutory deductions and pension contributions are automatically transmitted.

IV. Banking / Fund Distribution Pathway

After Treasury Operations finalize the totals, funds are routed:

- DST (Deputy Secretary to Treasury Accounts)
- Total Govt Org Accounts
- Distributed to:
  - Employee Salary Accounts
  - Union Accounts
  - Other Bank Accounts (N → 1 mapping)

This represents the final financial settlement sequence of government salary disbursement.

As illustrated in the diagram below, the Payroll Functionality is represented under Item No. 1, serving as a core financial component that interacts with multiple administrative and human resource management modules.

The payroll process is primarily driven by two types of transactions — *Earnings* and *Deductions*. Each transaction type can be categorized as Fixed or Variable, depending on the nature of the employee's entitlement or deduction. These transactions are governed by configurable rules embedded within the Pay Engine, which applies formulas, calculations, and validations based on institutional policies and service rules.

System Architecture and Major Components

The business architecture of the system is divided into several key components, as described below:

No (as per Diagram)	Component	Description
1	Payroll System	This module handles all payroll-related functions including the configuration of earnings and deductions. Each transaction (fixed or variable) is linked to a Rule Engine where formulas and business logic are defined. The payroll system integrates with other components to generate pay slips, handle loan recoveries, compute no-pay deductions, and interface with other systems.
2	Employee Master Information	This serves as the central repository for all employee-related data, containing details such as personal, employment, and service records. The Employee Master acts as an upper-layer data source that supplies essential information to the Payroll System. It ensures that all calculations, entitlements, and deductions are based on accurate and up-to-date employee data.
3	SLUDI and Organizational Structure	This layer integrates with the SLUDI (Sri Lanka Unique Digital Identity) system and the government's Organizational Structure Database. It ensures that every government employee has a unique identifier, while organizational hierarchies and reporting lines are consistently mapped and maintained across ministries, departments, and agencies.

4	GovHR (Public Administration)	Managed by relevant Public Service Commissions and authorities such as the Ministry of Public Administration, Health, and Education, the GovHR component covers key HR lifecycle processes including Recruitment, Probation, Confirmation, Promotion, Transfer, and Disciplinary Actions. Data from GovHR automatically updates the Employee Master, ensuring real-time synchronization.
5	Cadre Management (Department of Management Services)	This component, under the MOFPED, manages approved vs. actual cadre information. The Department of Management Services (DMS) authorizes cadre positions and vacancy approvals for government institutions, feeding structured establishment data to the Employee Master and organizational structure layers.
6	Leave and Attendance Management	This module records employee attendance and leave details, including various leave types and no-pay calculations. Relevant attendance and leave deductions are pushed to the Payroll System for accurate pay computation. Integration ensures that payroll reflects real-time attendance and absence data.

Functional Overview

- The integration of all above modules enables a single, unified HR and Payroll ecosystem across the government sector.
- Information flows bi-directionally between components to maintain data consistency and avoid duplication.
- The Employee Master Information acts as the central hub, receiving updates from GovHR, SLUDI, and DMS, while providing verified data to Payroll and Leave systems.
- The Payroll Engine executes all calculations based on approved rules, ensuring transparency, accuracy, and compliance with government financial regulations.
- The system supports inter-departmental interfaces with the Department of State Accounts, Inland Revenue Department, Pension Department, and Banking interfaces for salary disbursement.

Functional Overview of eGPS

The functional overview describes the key user groups, delivery channels, functional modules, and integration points with external systems.

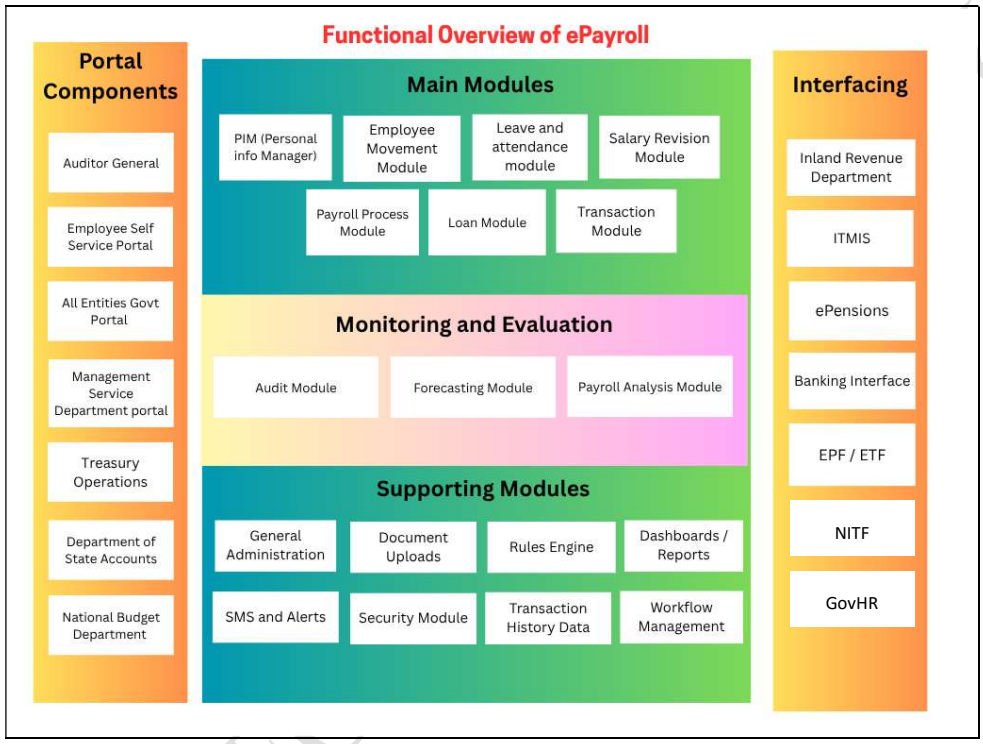
The illustrative functional overview Figure 5.2 below represents the proposed architecture for the eGPS, including:

- System Users – such as payroll administrators, HR officers, finance departments, audit units, and relevant government agencies.
- Portal Components – including secure web portals, mobile interfaces, and system-to-system APIs.
- Functional Modules – such as payroll processing, employee data management, benefits calculation, reporting and analytics, user access control, and compliance management.

- External Interfaces – integration points with financial systems, tax and pension systems, banking systems for payroll disbursement, and national identity verification services.

The high-level business and functional requirements for each component in the functional overview diagram are elaborated in this document.

Figure5.2: Illustrative Functional Overview of eGPS



The Government eGPS integrates a wide range of modules and portals to streamline payroll operations across government entities. Portal components provide targeted access to different stakeholders: the Auditor General can audit payroll data; employees use a self-service portal for payslips, leave, and personal updates; government institutions access payroll functions through a centralized portal; and specialized portals serve the Management Service Department, Treasury, State Accounts, and Budget Department for oversight, funding, and planning. The main modules manage the core payroll functions from maintaining personal employee data in the Personal Information Management, tracking movements like promotions and transfers, managing leave and attendance, handling salary revisions, processing payroll, managing loans, and recording all related transactions.

Supporting the core operations are monitoring and evaluation tools like the Audit, Forecasting, and Payroll Analysis modules, which ensure compliance, provide cost projections, and offer analytical insights. Supporting modules add essential capabilities such as administration, document storage, rule-based payroll calculations, reporting, security, and workflow automation. Finally, the system interfaces seamlessly with key external entities including the Department of Inland Revenue (RAMIS) for tax compliance, DSA (ITMIS) for treasury integration, Department of Pension for retiree payments,

banking interfaces for salary disbursement, and EPF/ETF systems for statutory contributions ensuring end-to-end payroll efficiency and compliance.

Category	Module / Component	Detailed Description
Portal Components	**Auditor General**	Provides the Auditor General's office with secure, read-only access to payroll data for compliance auditing. Enables sampling of payroll records, validation of payment accuracy, and verification against government policies. Includes data export tools for audit reports.
	Employee Self Service Portal	Enables employees to log in and view payslips, tax deductions, and leave balances; request leave; update personal information (address, bank details); and track payroll transactions. Reduces administrative workload by enabling self-service.
	All Entities Govt Portal	A unified access point for all government institutions to manage their payroll operations within eGPS. Ensures consistency in payroll processing standards and centralized reporting across ministries and departments.
	Department of Management Service	Used to manage staff establishment lists, approve new positions, view the actual cadre information, set salary structures, and oversee promotions and reassignments in line with government regulations.
	Department of Treasury Operations	Connects payroll with government treasury systems to enable timely fund allocation and salary disbursement. Supports reconciliation of payroll expenditures with treasury records.
	Department of State Accounts	Monitors payroll expenses against budget allocations, ensuring transparency in fund usage and compliance with financial reporting standards.
	Department of National Budget	Receives payroll cost data for workforce planning and budget forecasting. Supports decision-making for future staffing levels and salary revisions.
Main Modules	**PIM (Personal Information Manager)**	Serves as the central repository for employee personal data, such as full name, NIC/passport, date of birth, contact details, marital status, emergency contacts, and dependents. Ensures accurate data for payroll calculations and statutory reporting.
	Employee Movement Module	Records and tracks all employee movements including promotions, transfers, demotions, acting appointments, and secondments. Updates job title, department, reporting manager, salary grade, and other changes while maintaining an audit history.

	Leave and Attendance Module	In a Payroll module the employee leave for Payroll process need to enter and validate. Example No pay information.
	Salary Revision Module	Manages pay changes resulting from promotions, periodic increments, salary scale adjustments, or government policy changes. Updates payroll formulas automatically.
	Payroll Process Module	Automates payroll runs, calculates gross pay, applies deductions (tax, EPF, ETF), generates payslips, and processes arrears or back pay. Supports batch processing for large-scale payrolls.
	Loan Module	Handles employee loan requests, approval workflows, repayment schedules, and automatic deduction from payroll. Supports different loan types (housing, vehicle, personal).
	Transaction Module	Processes one-off or recurring transactions such as bonuses, allowances, incentives, deductions, or recovery amounts. Ensures proper ledger posting.
Monitoring and Evaluation	**Audit Module**	Tracks all payroll transactions and changes, including who made them and when. Generates audit logs and compliance reports for internal and external auditing.
	Forecasting Module	Predicts future payroll expenses based on staff strength, planned recruitments, and salary policies. Helps in budget allocation and long-term workforce planning.
	Payroll Analysis Module	Offers dashboards and analytical tools to identify payroll trends, cost breakdowns, overtimes, absenteeism impact, and workforce demographics.
Supporting Modules	**General Administration**	Handles administrative tasks such as managing organizational structures, user accounts, and general HR functions that support payroll.
	Document Uploads	Stores supporting documents like contracts, appointment letters, promotion orders, and resignation letters. Supports search and retrieval for compliance checks.
	Rules Engine	Applies configurable payroll rules, tax slabs, benefit eligibility, and compliance checks to ensure payroll accuracy and consistency.
	Dashboards / Reports	Generates pre-built and custom reports for HR, and management. Includes KPIs, statutory reports, and compliance forms.
	SMS and Alerts	Sends automated messages for payslip availability, leave approvals, payroll cut-off dates, and loan repayment reminders.

	Security Module	Ensures system security through role-based access control, audit trails, encryption of sensitive data, and compliance with ISO 27001 standards.
	Transaction History Data	Maintains complete history of payroll transactions for each employee for audit and reference purposes.
	Workflow Management	Automates approval processes for payroll changes, leave requests, and loan applications with multi-level authorization.
Interfacing	**Department of Island Revenue (RAMIS)**	Integrates with tax systems to calculate, deduct, and submit income tax and other statutory payments automatically.
	DSA (ITMIS)	Links to the Integrated Treasury Management Information System for real-time budget and expenditure reconciliation.
	Department of Pension	Interfaces with pension systems to process payroll for retirees, ensuring smooth benefit disbursement.
	Banking Interface	Enables direct transfer of salaries to employee bank accounts through secure banking APIs. Supports bulk transfers.
	EPF / ETF	Automatically calculates and remits contributions to Employee Provident Fund and Employee Trust Fund accounts.
	National Insurance Trust Fund	Automatically calculates and remits contributions to NITF accounts.
	Ministry of Public Administration (GovHR)	Interfaces with PUBAD/GovHR to process administration activities for government officials.

Government Payroll System – Security Policy

I. Purpose

This policy establishes mandatory security controls for the Government Payroll System to protect sensitive employee, payroll, and financial data against unauthorized access, tampering, and cyber threats. It ensures compliance with ISO/IEC 27001, local data protection regulations, and government IT security guidelines.

II. Scope

This policy applies to:

- All payroll system modules including self-service portals, administrative dashboards, and interfacing APIs.
- All employees, administrators, auditors, and external stakeholders access the system.
- All connected servers, databases, and storage repositories hold payroll data.

III. Password and Authentication Policy

- Minimum 12 characters including uppercase, lowercase, numeric, and special characters.
- Passwords must not contain easily guessable words such as employee names, NIC numbers, or "password."
- Password expiry every 90 days with a requirement to use a password not used in the last 5 changes.
- Account lockout after 5 failed login attempts with administrative review required for reactivation.

(a) Multi-Factor Authentication (MFA)

- All system logins must require One-Time Password (OTP) delivered via SMS, email, or authenticator app.
- OTP validity period shall not exceed 3 minutes to reduce replay attack risks.

(b) CAPTCHA Integration

- Login and password reset pages must implement CAPTCHA to prevent automated brute-force attacks.
- CAPTCHA must be dynamic and meet accessibility standards.

IV. Data Protection Measures

(a) Encryption

- All sensitive data in transit must use TLS 1.3 encryption.
- All sensitive data at rest must be encrypted using AES-256.

(b) File Integrity and Hashing

- All uploaded documents (e.g., scanned IDs, contracts) must be stored with a SHA-256 or SHA-3 hash to verify integrity.
- Payroll export files (e.g., salary sheets, audit reports) must be digitally signed to ensure authenticity.

V. Audit Logging

(a) Comprehensive Logging

- All user activities, including login attempts, record changes, approvals, and downloads, must be logged with timestamps, user IDs, and IP addresses.
- Logs must be stored in a tamper-proof location for a minimum of 7 years.

(b) Audit Review

- Security teams must review logs weekly for anomalies.
- Alerts must be generated in real time for high-risk actions such as bulk data exports, mass deletions, or unauthorized privilege changes.

VI. Malware and Threat Prevention

(a) Anti-Virus & Anti-Malware

- All servers and endpoints connected to the payroll system must have real-time anti-virus and anti-malware protection.
- Virus definitions must be updated daily.

(b) Intrusion Detection & Prevention Systems (IDS/IPS)

- Network-level IDS/IPS must monitor traffic for suspicious patterns.
- Immediate alerts must be sent to security teams upon detection of abnormal access attempts.

VII. Backup & Disaster Recovery Security

- Backups must be encrypted and stored in physically secure and geographically separate locations.
- Restore procedures must be tested quarterly to ensure data integrity and availability.

VIII. Compliance & Enforcement

- All users must sign a System Access Agreement acknowledging their understanding of security policies.
- Non-compliance will result in disciplinary action, including access revocation, legal prosecution, or both.

6. Technical Requirements

The total volume of Government employees that will be processed through the E-Payroll System at national level is approximately one million (1,500,000) employees. Due to this large scale, the Bidder is expected to clearly define and optimize their processing strategy. The Bidder may propose a segmentation approach (for example, distributing the workforce into multiple database clusters or parallel processing groups) to ensure that the system can execute payroll cycles simultaneously and efficiently.

According to the Service Level Agreement (SLA), the solution must be capable of processing approximately 300,000 employees within a maximum window of 3 hours per payroll execution cycle. This SLA requirement will be used during technical evaluation, and the Bidder will receive technical marks based on the ability of their proposed architecture to meet — or exceed — the required end-to-end payroll processing timeline.

The Bidder may propose any suitable architectural pattern, including but not limited to:

- Microservices architecture
- Modular Monolithic architecture
- Multi-tenant architecture
- Hybrid Solution

However, regardless of the selected method, the final architectural design must be able to fulfil the SLA performance criteria. In summary, the architecture must demonstrably support national-level scalability while ensuring the stipulated processing timelines are achieved.

The following illustrates a sample cluster mechanism approach that can be used as a reference concept for Bidders. These examples are provided only to convey the idea of how the payroll workload may be logically segmented and executed in multiple parallel clusters. Bidders are encouraged to use this as a conceptual guideline when designing their architecture and processing strategy.

Sector / Policy Area	Key Ministry / Ministries
Finance, Economy & Trade	Ministry of Finance, Planning and Economic Development; Ministry of Trade, Commerce and Food Security; Ministry of Investment Promotion; Ministry of Technology; Industry and Entrepreneurship Development
Infrastructure, Transport & Public Utilities	Ministry of Transport, Highways, Ports & Civil Aviation; Ministry of Power & Energy; Ministry of Water Supply; Ministry of Irrigation & Water Resources Management; Housing / Urban Development ministries
Agriculture, Fisheries & Rural Development	Ministry of Agriculture; Ministry of Fisheries, Aquatic & Ocean Resources; Ministries related to Livestock & Rural Community Development; Plantation Industries
Environment, Natural Resources & Wildlife	Ministry of Wildlife & Forest Resources Conservation; Ministry of Environment; Ministry of Irrigation (as water resource management); other agencies dealing with forests, biodiversity, land resources
Social Sectors (Health, Education, Welfare, Culture, etc.)	Ministry of Health; Ministry of Education, Higher Education & Vocational Training; Ministry of Women, Child Affairs & Social Empowerment; Ministry of Sports & Youth Affairs; Ministry of Culture / Religious Affairs; Ministry of Mass Media
Public Administration, Security & Justice	Ministry of Defense; Ministry of Justice, Prisons & Constitutional Reforms; Ministry of Public Security (or Public Administration / Provincial Councils / Local Government); Ministry of Home Affairs; Ministry of Labour & Foreign Employment
Energy, Digital Infrastructure & Innovation	Ministry of Power & Energy; Ministry of Telecommunication, Digital Infrastructure & Foreign Employment; Ministry of Technology; other institutions/agencies of ICT / atomic energy etc.
Environment / Disaster Management	Ministry of Environment; Ministry of Disaster Management; Ministry of Irrigation & Water Resources; sometimes overlap with Agriculture / Wildlife etc.

6.1 Technical Details for LGC2+ Hosting Services for the Four Months Development, Testing and Training Instance

The environment is deployed on Red Hat OpenShift Container Platform Version 4.20, running on Sri Lanka Telecom's enterprise-grade cloud infrastructure.

a) Platform Overview

Platform: Red Hat OpenShift Container Platform (OCP) v4.20

- Underlying Infrastructure: SLT Cloud IaaS cluster (VMware VCF / Bare Metal for selected workloads)

- Architecture: Full-stack automated installation using Red Hat Enterprise Linux CoreOS (RHCOS)
- Deployment Model: Highly available multi-node cluster (Control Plane + Compute Nodes)

b) Resource Allocation for LGC2+

Dedicated Project/Namespace: Allocated exclusively for LGC2+ workloads

Compute Resources:

- Provisioned CPU and Memory limits/requests as per the contracted service tier
- Ability to scale within agreed resource quotas

Storage:

- Persistent storage provided through SLT Cloud enterprise storage backend
- CSI-managed persistent volumes with configurable performance tiers (Standard / High Performance)

Networking:

- Isolated SDN-based project-level network
- Secure ingress through OpenShift Routes and Load Balancer service
- Internal service-to-service communication managed through OpenShift Service Mesh (if required)

c) Security & Compliance

- Cluster Hardening: Based on Red Hat OCP security best practices
- Pod Security Admission (PSA): Enforced at namespace level
- RBAC: Role-based access control with project-level privileges

Image Security:

- Mandatory use of trusted container registries
- Image vulnerability scanning

Data Security:

- At-rest encryption via SLT storage platform
- In-transit TLS 1.2+/HTTPS enforced

Compliance Alignment:

- ISO 27001 / 27017 / 27018 controls supported
- Local data hosting in SLT Tier III Data Center

d) Availability

Cluster Availability: OpenShift control plane and supporting infrastructure

High Availability:

- Redundant control plane nodes
- Distributed compute nodes
- Load-balanced ingress and API endpoints

Backup & Recovery:

- Scheduled backups using Velero/OpenShift API-level snapshots
- Restoration support as per the contracted scope

e) Monitoring & Support

Monitoring:

- Centralized metrics through APM Tool
- Pod/Node/Route health monitoring

Logging:
Cluster-wide EFK/Logging stack for audit and application logs

Support Model:

- 24×7 support through SLT Cloud Operations
- Incident & service request handling via SLT ticketing system
- Escalation procedures defined under the contract

f) Optional Add-Ons (If required)

- CI/CD pipeline integration (GitLab, Tekton, Nexus)
- WAF and advanced network policies
- Auto-scaling configuration (HPA/VPA/Cluster Autoscaler)

g) Provide Bill of Materials for Lanka Government Cloud Solution

In accordance with government policy, the eGPS will be deployed on the Lanka Government Cloud solution. The bidder is required to clearly define and justify the technical specifications necessary to determine the appropriate system sizing and resource requirements. This should cover the entire lifecycle of the system, including the development phase, a four-year warranty period, and a subsequent three-year post-warranty support period.

The bidder must ensure that the proposed solution is scalable, secure, and capable of meeting the required service levels throughout these periods. As part of the implementation approach, the following key areas must be thoroughly considered and documented:

i. **Production Instance Requirements**
   Define the required production environment, including compute resources, storage capacity, database configurations, and network specifications necessary to support the payroll system efficiently.

ii. **High Availability and Scalability**
   Describe how the system will ensure High Availability (HA) with minimal downtime, including failover mechanisms and load balancing. The solution should also support horizontal and vertical scalability to accommodate future growth in users and data volume.

iii. **Security Aspects**
   Outline the security framework, including data encryption (at rest and in transit), access control mechanisms, identity and authentication systems, and compliance with government security standards.

iv. **Monitoring (Application Performance Monitoring)**
Specify monitoring tools and strategies to track system performance, availability, and health. This should include real-time alerts, logging, and reporting mechanisms to ensure proactive issue resolution.

v. **Backup and Replication**
Detail the backup strategy, including frequency, retention policies, and storage locations. The bidder should also describe data replication mechanisms to ensure data integrity and availability in case of failures.

vi. **Anti-Virus Protection**
Explain the anti-virus and endpoint protection measures that will be implemented to safeguard the system from malware and other security threats.

vii. **Disaster Recovery (DR) Site Requirements**
Define the disaster recovery strategy, including DR site setup, recovery time objectives (RTO), recovery point objectives (RPO), and procedures for failover and system restoration.

viii. **Additional Requirements for SLA Compliance**
Identify any additional technical or operational requirements necessary to ensure that the payroll system consistently meets the agreed Service Level Agreements (SLAs), including uptime, performance, and support responsiveness.

Technical Specifications for Government Cloud Solution based on the Bidder technical proposal

(1)	(2)	(3)	(4)	(5)
Line Item No	**Description**	**Technical Specifications and Standards**		
		Details	**Detail Specification**	**Remarks**
Bidder's Requirements				
Examples				
1.	***Back Up Appliance***	*Should provide remote replication over IP network with bandwidth throttling*		
2.		*should support 2TB or above NLSAS drives, RAID 6 protection*		
3.		*Must support up to 12TB/hour throughput*		
4.		*Must support LAN backup using CIFS & NFS protocols and license should be provided*		
5.		*Must support SAN based Fibre Channel (FC) protocol with Tape library emulation (VTL) & VMware VMDK backup over NAS and license should be provided*		
6.		*Should have 4 x 1Gbps & 2 x 10Gbps IP ports and 2 x 8Gbps FC ports*		
Below is the guide to the bidder				
	WAF			
	Firewall			

(1)	(2)	(3)	(4)	(5)
Line Item No	**Description**	**Technical Specifications and Standards**		
		Details	**Detail Specification**	**Remarks**
Bidder's Requirements				
	Production Instance			
	Development			
	Testing			
	APM			
	NMS			
	PAM			

7. Implementation Approach of e-Government Payroll System Application

(a) Strategic Implementation Framework

The Department of State Accounts (DSA) shall place significant emphasis on ensuring the long-term sustainability, accuracy, and transparency of the e-Government Payroll System (e-GPS). This will be achieved through a phased implementation strategy guided by Agile methodology principles, enabling iterative development, continuous validation, and feedback-driven improvement throughout the system lifecycle.

The objective is to ensure that all payroll computations, integrations, and reporting mechanisms function accurately across ministries, departments, and provincial councils, supporting the establishment of a unified national payroll management framework.

(b) Development Methodology

The System Implementation Partner (SIP) shall design, develop, and implement the National Payroll System using Hybrid Agile practices, ensuring incremental delivery of functional modules such as:

- Employee Master Data Management
- Earnings and Deductions
- Leave and Attendance Integration
- Loan and Pension Modules
- Pay Engine and Bank Interface

Each component will undergo continuous testing, validation, and user feedback to ensure alignment with DSA's operational and regulatory requirements.

(c) Project Management and Collaboration Tools

The SIP shall utilize industry-standard Agile Project Management Tools (e.g., JIRA or equivalent) to support sprint planning, issue tracking, and backlog management. The Department of State Accounts shall procure and maintain the necessary tool licenses until project completion to ensure proper governance, visibility, and control of progress through sprint dashboards and automated reporting mechanisms.

(d) Implementation Phasing and Compliance

The SIP shall implement project activities in accordance with an agreed monthly project plan, jointly developed with DSA. During the implementation phase, the SIP shall prepare and submit all required documentation as listed below and ensure adherence to Standard Operating Procedures (SOPs) established by the Department of State Accounts.

The SOPs shall comprehensively cover, but not be limited to, the following operational areas:

- Release Management Process
- Issue and Change Handling Mechanism (via JIRA or equivalent)
- Service Level Agreement (SLA) Compliance Monitoring
- Testing Strategy and Test Plan Execution
- Source Code and Repository Management (Bitbucket / GitHub)
- Risk and Issue Management
- Daily/Weekly Progress Reviews and Project Steering Committee Operations
- Software Requirements Specification (SRS) Management
- System Design and Architecture Documentation

The SIP must ensure that all implementation activities, reports, and documentation comply with these SOPs and the standards prescribed therein.

(e) Reference to the eGPS Development Road Map

Upon contract award, the successful bidder shall mobilize and establish the full project team within three (03) weeks. It is important to note that previous payroll modernization efforts have faced significant delays; therefore, the project will be managed using structured phases and tight governance mechanisms to ensure continuity, accountability, and measurable progress.

While a high-level Functional Requirement Specification (FRS) has been provided in the bid documentation, the bidder shall conduct a Discovery and Requirement Clarification Session to gain a comprehensive understanding of payroll workflows, integrations, and reporting expectations.

Each functional and technical requirement shall be finalized jointly by the SIP project team and the Department of State Accounts project steering committee. The Software Requirements Specification (SRS) will be continuously refined and aligned to each Sprint cycle.

The Department of State Accounts shall review and approve the commencement of each Sprint, which shall be executed within a two-week (14-day) time-boxed iteration.

(f) Sprint Execution Framework

Each Sprint cycle shall include the following mandatory activities:

I. UI/UX Prototype Development
   - The bidder shall develop a working prototype for payroll-related interfaces such as employee dashboards, pay-slip generation, and approval workflows.

II. Prototype Review and Feedback
   - The Department of State Accounts will review and provide consolidated feedback within two (02) working days.

III. Draft SRS Preparation and Initial Development

- Based on feedback, the SIP shall update the draft SRS and commence development in parallel.

IV. Daily Incremental Releases and Testing
- The development team shall release small, testable increments daily, validated against predefined test cases and payroll calculation rules.

V. Joint Review of Progress
- DSA officials, the SIP, and the Independent Assurer (IA) will jointly evaluate released functionality and compliance with payroll standards.

VI. Sprint Closure and Release Planning
- At the end of each Sprint, the team shall finalize the Sprint deliverables, conduct regression testing, and plan subsequent releases.

Each set of completed Sprints shall be considered a Sub-Phase of the project. Certification for each Sub-Phase will be provided by the Independent Assurer (IA), ensuring transparency, accountability, and alignment with national payroll governance standards.

(g) Resource Structure and Expertise

The Department of State Accounts will evaluate bids based on the quality, experience, and availability of the proposed implementation team. The SIP must allocate qualified professionals with proven experience in payroll, HRIS, and government finance systems.

No	Position	No of People	Full Time/Part Time assign to the DSA project (Time commitment)	Minimum Work Experience / Years	Specific Experience/ Years
1.	Project Manager	1	Full Time	10	5
2.	Business Analyst	1	Part Time	10	5
3.	BPR Expert	1	Part Time	10	5
4.	Domain Expert	1	Part Time	10	5
5.	Legal Expert (IT + Tax)	1	Part Time	10	5
6.	Software Architect	1	Part Time	10	5
7.	Cloud Architect	1	Part Time	10	5
8.	Senior Software Engineers	2	Part Time	5	4
9.	Cloud Engineers	2	Part Time	3	2
10.	QA Lead	1	Part Time	3	2
11.	QA Engineers	3	Part Time	3	2
12.	Training Expert	1	Full Time	1	2

13.	IT Infrastructure and Implementation Engineer	1	Part Time	2	2
14.	Support / Help Desk Engineer	1	Part Time	1	2

All proposed team members must possess the minimum academic qualifications and relevant domain expertise as defined in the bid documentation.

Any replacement or substitution of key personnel must receive prior written approval from the Department of State Accounts, and replacements must meet or exceed the originally proposed qualifications and experience levels.

(h) Governance and Quality Assurance
The Department of State Accounts reserves the right to request the replacement of any personnel if their performance is deemed unsatisfactory or non-compliant with contractual expectations.

All newly introduced personnel shall be subject to an evaluation and interview process by DSA prior to formal onboarding. The approval of personnel lies solely at the discretion of the Department of State Accounts.

To ensure continuous compliance, all deliverables will undergo Independent Assurance (IA) certification for quality, performance, and security validation before final acceptance.

8. Project Governess Structure

Role / Entity	Responsibilities
Project Steering Committee (PSC)	- Provide strategic oversight and guidance to the project. - Approve major deliverables, including requirements, design, and go-live decisions. - Resolve high-level issues escalated from the Project Management Unit (PMU). - Monitor progress against the approved project plan and timelines. - Approve change requests with significant scope, budget, or schedule impact.
Project Management Unit (PMU) – MOFPED / DSA	- Manage day-to-day project activities on behalf of MOFPED/DSA. - Coordinate with the SIP to ensure adherence to the project plan. - Review and sign off on all project deliverables. - Facilitate communication between government departments and the SIP. - Monitor compliance with contract, SLAs, and quality standards. - Manage risks, issues, and dependencies. - Ensure execution of stakeholder engagement and change management plans.
Software Implementation	- Serve as single point of contact between SIP and PMU. - Prepare and maintain Project Management Plan (PMP) and Work Breakdown

Partner (SIP) Project Manager	Structure (WBS). - Ensure delivery of milestones according to the schedule. - Manage SIP resources, development activities, and quality assurance. - Report project status, risks, and issues to PMU weekly. - Lead resolution of technical and operational issues. - Ensure use of approved project management tools.
SIP Technical Lead	- Oversee technical architecture, development, and system integration. - Ensure compliance with technical specifications, security policies, and industry standards. - Coordinate dependencies with third-party systems (Treasury, EPF/ETF, and Banking). - Provide technical documentation and participate in reviews. - Support performance tuning, load testing, and disaster recovery setup.
DSA Functional Leads	- Represent end-user requirements and validate business processes. - Participate in requirement gathering, design validation, and UAT. - Approve functional specifications and test scenarios. - Review training materials and participate in Train-the-Trainer programs.
Independent Assurer / QA Agency	- Conduct independent QA, security, and performance testing. - Certify compliance with requirements, SLAs, and security standards. - Report findings directly to PSC and PMU. - Verify resolution of identified gaps before go-live.
Help Desk Coordinators (DSA)	- Manage first-line user support post-implementation. - Coordinate with SIP support agents for escalation and resolution. - Track and report help desk performance metrics. - Ensure bilingual/trilingual support coverage.

9. Software Quality Assurance

We are breaking the testing into two parts one is Sprint level testing and final operational testing. The two different strategies involved and couple of testing will conduct in phase manner. The Exit criteria for each sprint and operational acceptance.

The primary goal of Sprint level Testing and Certification is to ensure that the eGPS solution including all systems, deliverables, and services meets the requirements, standards, specifications, and performance criteria defined in the Request for Proposal (RFP) and the agreement.

This process shall ensure that the following elements are measured against clear, quantifiable metrics for accountability:

- Functional Requirements
- Cloud Deployment requirements
- Availability of Services at the defined locations
- System Performance
- Information Security
- System Manageability
- Application Scalability

- Accessibility Testing
- Project Documentation (design, development, configuration, training, and administration manuals, etc.)

10. Code Architecture and Quality Review Requirements

10.1. Evaluation of COTS Products

If the proposed solution is based on a Commercial Off-The-Shelf (COTS) product, the State Accounts Department (DSA) shall conduct a code architecture review as part of the due diligence process prior to bidder selection.

Evaluation marks shall be awarded based on the robustness of the architecture and the completeness of the code review process.

The bidder's source code (or representative code components, where applicable) shall be deployed in SonarQube or an equivalent code review platform to assess adherence to industry-standard coding practices, security guidelines, and quality metrics.

11. Quality Assurance process

11.1. Background

During the bid evaluation process for the eGPS, the Department of State Accounts (DSA) will place significant emphasis on assessing each bidder's Quality Assurance (QA) Strategy and Implementation Process. The objective is to determine whether the bidder demonstrates a strong, practical understanding of QA methodologies, tools, controls, and testing practices that are required for a mission-critical government payroll platform.

To prevent this, the current procurement and evaluation process will allocate explicit scoring weight to:

- QA governance and planning,
- testing approach and coverage,
- tooling and evidence management,
- and readiness to comply with required SLAs.

Bidders who present a mature QA framework backed by clear, auditable processes will receive higher technical scores.

All software components of the National Payroll System — including core payroll modules, HR data integration components, interfaces with Attendance/Leave, statutory deduction calculation engines, bank file generation, pensions and taxation outputs, and any related cloud or infrastructure services — shall be subject to a comprehensive Quality Assurance process. This is required to ensure reliability, correctness of payroll computation, legal/statutory compliance, data protection, auditability, and resilience before final acceptance.

The QA process shall operate in two layers of validation:

I. Internal Testing by the Software Implementation Partner (SIP) (the bidder's own QA function)
II. Independent Verification and Validation (IV&V) by the Independent Assurer (IA) (an external/independent assurance body endorsed by DSA)

11.2. Testing and Quality Assurance Workflow

(a) Internal Testing by the SIP

The Software Implementation Partner (SIP) shall conduct rigorous internal testing as part of its QA plan before releasing any build to the Department of State Accounts.

This internal QA effort shall include at minimum:

- Functional testing, integration testing, payroll rule validation, and regression testing across all relevant modules (e.g. earnings, deductions, loan recovery, EPF/ETF, gratuity, pension contributions, no-pay handling, arrears adjustments, bank export, pay slip generation).
- Verification that each Sprint/release meets all agreed Entry Criteria and Exit Criteria before it is promoted to the next stage.
- Full documentation of all test cases, expected results, execution evidence, and screenshots/logs for critical calculations.
- Resolution of all Critical and Major defects in line with the agreed Service Level Agreements (SLAs).
- Internal confirmation that statutory and regulatory calculations (tax, deductions, pension, etc.) match published formulas and circulars.

The SIP's internal QA team must:

- Achieve a minimum 80% functional test coverage across implemented features.
- Maintain objective, reviewable evidence demonstrating adherence to the QA strategy submitted in the proposal.

(b) Independent Assurer (IA) Validation

Once the SIP completes internal testing for a Sprint, release, or sub-phase, the Independent Assurer (IA) will perform an external verification of quality.

The IA shall:

- Review, audit, and cross-check all test plans, test cases, execution logs, calculation samples, and defect reports submitted by the SIP.
- Independently re-execute or extend the same test cases to confirm accuracy of payroll computations, handling of leave/no-pay, attendance rules, arrears, recovery, and statutory remittances.
- Identify any gaps, inconsistencies, or non-compliance in the SIP's testing coverage, and instruct the SIP to carry out corrective actions.
- Produce a Sub-Phase Certification Report confirming whether the release meets functional, performance, compliance, and security expectations.

Payments for that sub-phase shall only be released to the SIP after the IA issues its formal Sub-Phase Certification.

This ensures that quality validation and compliance sign-off come before any financial disbursement.

11.3. Functional Testing Requirements

All bidders are required to clearly describe how they will achieve the QA objectives of the National Payroll System and comply with entry/exit gates for each testing phase. The proposal must explain specific methods, tools, governance, and controls for ensuring payroll accuracy, stability, and auditability.

The following areas must be addressed:

I. Scope Identification
- Define the full scope of functional testing: payroll processing, retroactive adjustments, overtime calculations, leave/no-pay integration, attendance-based deductions, statutory deductions (e.g. taxes, pension fund), loan recovery, bank interface generation, and reporting to State Accounts and other agencies.
- Specify which modules, submodules, APIs, and integrations are covered in each round of testing.

II. Test Coverage Definition
- Describe how test coverage will be measured, reported, and maintained.
- The expected minimum functional test coverage is above 80%.

III. Testing Coverage Approach
- Explain the strategy to maintain that coverage level, including:
  - unit tests,
  - automated regression tests,
  - end-to-end payroll run simulations using realistic employee datasets,
  - edge cases (acting allowances, interim payments, suspensions, backdated increments, etc.).

IV. Test Case Preparation
- Describe how test cases will be authored, peer-reviewed, approved, version-controlled, and linked to requirements.
- Identify any test automation / execution tools to be used (e.g. Selenium for UI workflows, JMeter or equivalent for performance scenarios, automated payroll calculation checks, etc.).

V. Defect Management and SLA Compliance
- Describe defect logging, prioritization, triage, tracking, retesting, and closure.
- The bidder must show how Critical and Major defects will be resolved within the SLA windows agreed with the Department of State Accounts.

VI. Additional QA Measures
- Describe any further QA controls such as:
  - peer code reviews,
  - secure coding review,
  - continuous integration / continuous delivery (CI/CD) pipelines,
  - automated regression packs per Sprint,

- performance validation of bulk payroll runs across ministries.

11.4. Application Security Testing (OWASP Focus Areas)

Before any production deployment, the entire National Payroll System (application layer, integrations, infrastructure, and associated cloud services where applicable) shall undergo an independent security and controls audit by a certified third-party security assessment agency.

This is mandatory to protect payroll, personal data, bank account details, deduction summaries, tax identifiers, pension eligibility data, etc.

I. Security Standards and References

The independent security assessment shall align with internationally recognized best practices, including:

- OWASP Application Security Verification Standard (ASVS) and OWASP Testing Guide (for web and API security).
- Cloud Security Alliance (CSA) Guidelines.
- ISO/IEC 27001 (information security management), ISO/IEC 27017 (cloud security controls), and ISO/IEC 27018 (protection of personally identifiable information in cloud environments). These frameworks are widely accepted for public-sector systems handling personal and financial data.

II. Scope of Security Assessment

The assessment shall cover, at minimum:

- Authentication and Identity Management
  - Validation of secure login/authentication across all user portals (payroll admins, HR officers, finance officers, audit roles, etc.).
  - Testing for weak/broken authentication scenarios, MFA enforcement, session hijack resistance.
- Access Control and Authorization
  - Validation of Role-Based Access Control (RBAC), segregation of duties (e.g. payroll calculation vs payroll approval vs bank file authorization), and prevention of unauthorized access between ministries/agencies.
  - Detection of Broken Access Control vulnerabilities.
- Data Protection and Encryption
  - Review of encryption for data at rest (salary info, bank accounts, personal identifiers) and in transit.
  - Review of key management.
  - Compliance with OWASP guidance on cryptographic failures.
- Input Validation and Injection Prevention
  - Testing for SQL injection, command injection, cross-site scripting (XSS), API misuse, and tampering of calculation parameters.
- Session Management
  - Review of session timeout, cookie flags, logout/invalidation, concurrent session limits, etc.
- Logging and Monitoring

- Review of audit trails for payroll changes, overrides, exception payments, and approval steps.
- Monitoring of privileged activities and access to sensitive payroll data.
- Alignment with OWASP Logging and Monitoring best practices.

11.5. Outcome and Compliance Reporting

After completion of QA, functional testing, performance testing, security assessments, and IA review:

- The Independent Assurer (IA) shall prepare a consolidated Quality & Security Report summarizing:
  - test execution outcomes,
  - unresolved defects,
  - performance and load test observations,
  - security assessment findings,
  - compliance gaps.
- The Software Implementation Partner (SIP) must address all Critical and Major issues identified by the IA before the solution can proceed to pilot or production rollout.
- Final acceptance and authorization to go live shall only be granted when:
  - all Critical issues are fully closed,
  - all Major issues are either closed or formally risk-accepted by the Department of State Accounts,
  - the IA and DSA both sign off.

11.6. Infrastructure & Network Security Review

The testing agency (or IA, where applicable) shall also assess the robustness of the hosting environment for the eGPS:

- Network and Perimeter Security: Firewall rules, IDS/IPS behavior, secured VPN access for remote payroll users, and restricted administrative ports.
- Server & Operating System Hardening: Patch level compliance, removal of default credentials, disabling of unnecessary services, and baseline hardening.
- Database Security: Access restrictions to payroll databases, encryption of sensitive payroll/HR/benefit data, protection against unauthorized ad-hoc queries.

11.7. Cloud Deployment Security Testing (if cloud or hybrid deployment is used)

This section will focus exclusively on application-related components, considering only activities performed by application developers, and excluding any infrastructure, hardware, or external system aspects.

- Cloud Infrastructure Configuration Review: Secure configuration baselines for compute, storage, IAM, VNET/VPC, key vaults, etc.
- IAM in Cloud: Least-privilege enforcement, MFA for administrative access, role separation between application support and infrastructure support.
- Data Residency & Compliance: Validation that hosting and data storage meet all national data residency requirements and public-sector ICT security policies defined by the Government of Sri Lanka / Treasury / DSA.

- Resilience and Disaster Recovery: Verification of backup, high-availability, failover, disaster recovery (DR) procedures, and restore times to ensure payroll continuity (e.g. month-end payroll run cannot fail).
- Cloud Logging & Threat Detection: Verification that all relevant audit and security events feed into centralized monitoring and alerting.

11.8. Security Testing Deliverables

The independent security assessment agency shall produce the following deliverables:

- A detailed Vulnerability Assessment and Penetration Test (VAPT) Report, classifying findings by severity (Critical, High, Medium, Low).
- Recommended mitigation actions, timelines, and responsible parties.
- A Remediation Validation Report, confirming that fixes applied by the SIP have been re-tested and verified as effective.

11.9. Performance Testing

The National Payroll System shall be tested against performance thresholds defined in the Service Level Agreements (SLAs), including but not limited to:

- End-to-end payroll run time for a defined number of employees across multiple ministries.
- Request/response time for core user operations (e.g. payslip view, approval workflows, exception handling).
- Processing time for high-volume workflows (bulk updates, arrears adjustments, mass allowance changes, cost-of-living increments, etc.).
- Supported number of concurrent sessions (e.g. finance officers, HR officers, auditors logging in at the same time near month-end).

Additional mandatory checks:

- Disaster Recovery drill and recovery time validation.
- Scalability assessment to confirm the system can handle phased national rollout (central government, provincial councils, semi-government bodies, etc.).
- Full load testing must be completed prior to Go-Live to confirm compliance with SLA targets.

11.10. Availability / Continuity Testing

The National Payroll System shall be architected with no single point of failure for critical services.

The testing agency (or IA) shall validate:

- High availability and failover of application servers, database servers, and network components.
- DC/DR (Data Centre / Disaster Recovery) switch-over tests.
- Continuity of payroll services from alternate infrastructure in the event of a primary site outage.
- Accessibility of the system from all approved user locations after failover.

11.11. Project Documentation Review

The IA / designated testing authority shall review all documentation to ensure completeness, traceability, and operational readiness. This includes:

- Requirements Specifications: Functional and non-functional requirements for payroll, attendance integration, statutory deductions, reporting, etc. Must be clearly defined, testable, and traceable.
- System and Technical Design Documents: Architecture diagrams, integration specs (e.g. to attendance systems, HR master, bank interfaces), data flow, security model.
- Source Code for Custom Components: Reviewed for coding standards, maintainability, audit logging, and secure coding practices.
- Installation and Deployment Manuals: Clear deployment/runbooks for production, DR, and test environments.
- Training Materials: End-user manuals (payroll officer, HR officer, approving authority), administrator guides, and support procedures.
- System Administration Manuals / Operations Manuals: Including backup/restore steps, environment configuration, and escalation procedures.
- Version Control and Release Records: Proof of controlled change management and traceability of code changes.

Any gaps, inconsistencies, or missing information identified during this review shall be rectified by the SIP to the full satisfaction of the Department of State Accounts before acceptance.

11.12. Entry and Exit Criteria for Quality Assurance

I. Entry Criteria (Before QA Activities Begin)

Before formal QA testing starts for a Sprint/release, ALL of the following must be in place:

(a) Approved Requirements and Design Documents
- All functional and non-functional requirements for that Sprint/release are baselined and approved by DSA.
- High-level and detailed design documents are available.

(b) Stable Build Release
- A testable build of the National Payroll System is deployed in the QA environment.
- Build/installation notes, version numbers, configuration steps, and release notes are documented.

(c) QA Environment Readiness
- The QA environment mirrors production as closely as possible (infrastructure, configuration, security, datasets).
- Representative payroll data sets and test employee records are prepared and verified.

(d) Availability of Test Artifacts
- Approved test plans, detailed test cases, and automated test scripts (where applicable) are ready.
- Requirements → Test Cases traceability is established.
- Target test coverage: > 95% of planned test cases prepared for execution.

(e) Access and Resources

- QA team has valid credentials and correct role-based access.
- Test management, defect tracking, and automation tools are configured.

II. Exit Criteria (When QA for that Sprint/Release is Considered Complete)

QA for a Sprint / release is considered complete only when ALL of the following are true:

(a) Execution of All Planned Tests
- All planned test cases have been executed, with outcomes recorded and reviewed.

(b) Defect Closure and Acceptance Thresholds Met
- All Critical (S1) and Major (S2) defects are fixed.
- All known open issues are documented, impact-assessed, and formally acknowledged by DSA.

(c) Acceptance of QA Deliverables
- Test Summary Report, Defect Logs, and QA Release Notes have been reviewed and accepted by the QA Lead and Project Manager.
- The Requirements Traceability Matrix confirms full coverage.

(d) Regression Testing Completion
- Full regression completed to ensure no breakage in previously working payroll functionality.

(e) Formal Approval for Release
- QA provides signed confirmation that the release meets quality standards and is ready for submission to the Department of State Accounts and the Independent Assurer (IA) for certification.

11.13. Test Metrics and Defect Severity

Defect Severity Classification

Severity determines how urgently an issue must be resolved before the build can progress:

Severity Level	Code	Description
Critical / Blocker	S1	No workaround. Total system failure, payroll calculation failure, data loss, or critical security gap. Testing cannot continue.
Major	S2	Impacts major payroll functions or financial accuracy. Workaround exists but is complex or risky.
Minor	S3	Affects non-critical functions or secondary data. Simple workaround is available. Limited operational impact.
Trivial (Cosmetic / UI)	S4	Does not affect functionality or data. Cosmetic/usability issue only.

11.14. Criteria for Handover of QA Release to the Department of State Accounts and IA

Before submitting any release of the National Payroll System for acceptance by the Department of State Accounts, the SIP must provide evidence that the following quantitative thresholds have been met:

(a) Defect Status Thresholds (to be met by the SIP at handover):
- S1 Critical Defects: 0 open issues permitted.

- S2 Major Defects: Maximum of 2 open issues permitted.
- S3 and S4 (Minor / Trivial): Maximum combined total of 15 open issues.

(b) Test Coverage and Execution Quality:

- Test Case Execution Coverage: Greater than 95% of all planned test cases executed.
- Test Case Pass Rate: At least 85% of executed test cases must pass.
- Defect Severity Index (DSI): Less than 2.0, indicating acceptable overall stability.

(c) Regression Testing:

- Full regression testing on the final release build to confirm that fixes and new features have not broken core payroll processes.

(d) Release Documentation:

- A formal QA Release Note including build/version details, modules included, known issues, and constraints.
- Complete test results and execution evidence must be attached/archived.
- A current Defect Log showing severity, status, and operational impact of remaining issues.

(e) Stakeholder Communication:

- All remaining open issues must be clearly communicated to the Department of State Accounts, with documented impact analysis and explicit acknowledgement of any accepted residual risks.

11.15. Smoke Testing by IA / Department of State Accounts

Upon receipt of the QA Release Note and supporting documentation from the SIP, the Independent Assurer (IA) and/or the Department of State Accounts will conduct a Smoke Test on the submitted build.

Purpose:

To verify that the build is basically stable and that critical payroll functions (e.g. payroll run, approval workflow, statutory deduction export, pay slip generation, bank file generation) work in principle before entering acceptance or production-level testing.

Key Provisions:

(a) Test Execution

- IA / DSA will execute predefined smoke test cases covering login/authentication, payroll calculation, pay slip generation, approval and sign-off workflows, and critical statutory outputs.

(b) Acceptance Threshold

- A minimum 80% smoke test success rate is required for the build to be considered acceptable for further evaluation.

(c) Rejection and Rework

- If smoke test results fall below 80%, the build is rejected.
- The SIP must correct the issues, prepare a new build, update the Release Note, and resubmit for re-evaluation.
- No further acceptance testing will proceed until the smoke test passes.

(d) Documentation and Reporting

- The IA / DSA will document smoke test results, including pass/fail status, critical observations, and recommendations.
- This record becomes mandatory evidence before any move toward production readiness.

11.16. Quality, DSI Compliance, and Payment Linkage

(a) Compliance with QA and DSI Requirements

- The SIP must maintain the Defect Severity Index (DSI) within the approved limit (< 2.0).
- All QA Exit Criteria (defect closure, regression completion, coverage levels, documentation completeness) must be fully satisfied.
- Any deviation triggers mandatory rework and can delay milestone approval.

(b) Payment Linked to Quality Milestones

- All project milestone payments are performance-based.
- Payment will only be released once the Independent Assurer (IA) and the Department of State Accounts verify that QA exit conditions for that sub-phase have been met.

(c) Quality as a Prerequisite for Acceptance

- Quality is a contractual obligation, not an afterthought.
- Final acceptance of the National Payroll System depends on:
  - evidence of successful test execution,
  - closure of critical and major issues,
  - compliance with performance/security requirements,
  - and complete delivery of QA documentation.
- The Department of State Accounts reserves the right to reject, delay, or return any release that does not meet the approved quality gates, including the DSI limit and QA Exit Criteria.

12. Functional Requirements Review – Agile Delivery Alignment

The eGPS solution, customized and developed by the Software Implementation Partner (SIP), shall be reviewed and verified against the Functional Requirements formally signed off between the MOFPED and the SIP.

Under the Agile methodology, functional requirements shall be implemented, tested, and validated iteratively within each sprint or incremental delivery cycle, ensuring early detection and resolution of any gaps.

I. Gap Identification and Resolution in Sprint level testing

Any severe or critical gaps identified during functional testing—whether within an iteration, sprint review, or pre-Go-live phase—shall be addressed immediately by the SIP. Resolution of such gaps shall be prioritized in subsequent sprints or release cycles to prevent delays to the overall Go-live schedule.

II. Traceability and Testing Plans

A Requirements Traceability Matrix (RTM) shall be developed and continuously updated by the SIP to ensure that every functional requirement is mapped to its corresponding SRS, test case, and acceptance criteria.

In addition to the RTM, the SIP may create and maintain Agile-compatible test plans (including acceptance criteria within user stories) to validate compliance of the system with the defined requirements.

The RTM shall be reviewed at the end of each sprint and updated to reflect the status of completed and tested functionalities. Each Sprint level testing will be conducted by DSA testing team or Third party selected by the MOFPED.

III. User Acceptance Testing (UAT) in Agile

For UAT, MoFPED shall nominate employees from relevant divisions who are directly responsible for day-to-day payroll operations automated through the eGPS solution.

UAT shall be executed iteratively, aligning with sprint or release cycles, enabling progressive validation of features as they are delivered. The third-party acceptance testing agency, members of the Project Management Unit (PMU) from MoFPED, and nominated business users shall jointly participate in UAT cycles.

IV. Notification of Deviations

MoFPED shall establish a formal process for notifying the SIP of any deviations from defined requirements at the earliest opportunity, enabling corrective action. The involvement of the QA/Acceptance Testing & Certification agency shall not absolve the SIP from its primary responsibility to design, develop, install, test, and commission all project components to deliver services in full conformity with the Service Level Agreements (SLAs).

All SIP deliverables and services shall be subject to ongoing audit and certification. Payments to the SIP shall only be released upon successful completion of the relevant audits and certifications from the third party.

V. Technical Requirements Review

The **technical design** of the eGPS, including architecture, customization approach, and source code for custom components, shall be reviewed by an independent agency.

Any **non-compliance** or gaps in design must be corrected and formally signed off **before** proceeding to the next phase of implementation.

13. Security Review – Application, Infrastructure, and Lanka Government Cloud Deployment

The eGPS solution, including all customized software components, deployed infrastructure, and associated cloud services, shall undergo a comprehensive security and controls audit conducted by an independent security assessment agency.

The security review shall align with:

- OWASP Application Security Verification Standard (ASVS) and OWASP Testing Guide for web application testing.

The assessment shall include, but not be limited to, the following areas:

I. Application Security Testing (OWASP Focus Areas)

- Authentication & Identity Management
  Verification of secure authentication mechanisms across all application modules (e.g., system-managed, LDAP, Single Sign-On, Multi-Factor Authentication).
- Testing against OWASP Broken Authentication vulnerabilities.
- Access Control & Authorization
  - Validation of role-based and function-based permissions to prevent Broken Access Control vulnerabilities.
  - Verification of segregation of duties between functional users and system administrators.
- Data Protection & Encryption
  - Assessment of encryption mechanisms for data at rest and in transit.
  - Verification of proper key management and adherence to OWASP Cryptographic Failures guidelines.
- Input Validation & Injection Prevention
  - Testing against SQL Injection, Command Injection, and Cross-Site Scripting (XSS).
  - Validation of secure API and web service input handling.
- Session Management
  - Assessment of session expiration policies, secure cookie handling, and session hijacking prevention.
- Logging & Monitoring
  - Review of audit trail implementation for user activities, administrative actions, and security events.
  - Verification of alignment with OWASP Security Logging and Monitoring Failures recommendations.

II. Infrastructure & Network Security Review

- Network and Perimeter Security
  Firewall configuration audits, intrusion detection/prevention systems (IDS/IPS) validation, and secure VPN access controls.
- Server & Operating System Hardening
  Patch management, removal of default accounts, and disabling of unnecessary services.
- Database Security

Access restrictions, encryption, and prevention of unauthorized queries.

III. Cloud Deployment Security Testing

- Cloud Infrastructure Configuration Review
  Verification of secure configuration baselines for compute, storage, networking, and identity services in the chosen cloud platform (e.g., LGC 3).
- Identity and Access Management (IAM) in Cloud
  Role-based access policies, principle of least privilege enforcement, and Multi-Factor Authentication (MFA) for cloud console access.
- Data Residency & Compliance
  Validation of compliance with data residency requirements and government ICT security policies.
- Resilience and Disaster Recovery
  Verification of failover, backup, and disaster recovery configurations.
- Cloud Logging & Threat Detection
  Validation of integration with cloud-native logging and security monitoring tools (e.g., Azure Monitor, AWS CloudTrail).

IV. Security Testing Deliverables

The security assessment agency shall provide:

- A detailed vulnerability assessment report categorizing findings by severity (Critical, High, Medium, Low).
- Recommended mitigation actions with timelines.
- A remediation validation report after fixes are implemented by the SIP.

V. Performance Testing

- The system's performance shall be tested against SLA-defined parameters such as:
  - Request-response time
  - Workflow processing time
  - Maximum supported concurrent sessions
- Disaster recovery drill results
- Performance review shall also verify system scalability to meet MOFPED's phased expansion needs.
- Comprehensive load testing shall be conducted prior to Go-live to ensure the system performs within agreed service levels.

VI. Availability Testing

- The eGPS shall be designed with no single points of failure.
- Critical components shall have built-in redundancy for failover recovery.
- The testing agency shall conduct:
  - Network, server, and security failover tests
  - Data Center / Disaster Recovery (DC/DR) switch-over tests
  - Verification of service availability across all defined user locations

VII. Project Documentation Review

- The testing agency shall review all project documentation, including:
  - Requirements specifications
  - Design documents
  - Source code for customizations
  - Installation manuals
  - Training materials
  - Administration manuals
  - Version control records
- Any gaps must be rectified to MOFPED's satisfaction.

14. Scope of Work – Data Digitization of Historical Data for eGPS Implementation

This section defines the responsibilities of the Software Implementation Partner (SIP) for the digitization and migration of historical payroll data as part of the eGPS implementation.

I. Background

The Ministry of Finance, Planning and Economic Development (MOFPED) and its associated departments are currently utilizing legacy payroll systems developed in dBASE. All organizations within the scope of eGPS implementation follow a uniform data structure in their existing payroll databases.

II. Data Migration Requirements

The SIP shall be responsible for:

- Tool Development for Data Upload and Processing
- Develop a specialized migration utility capable of reading and processing the existing dBASE database files.
- The tool must allow for the upload of current payroll data into a temporary staging area.
- Once the full data validation and entry process is completed, the tool shall push the verified data into the main operational tables of the eGPS database.
- Historical Data Upload Capability
- The system must have a facility to upload and store up to one year of prior payroll data into a historical data schema within the eGPS.
- This functionality should be designed to ensure historical payroll records are readily accessible for reporting, auditing, and compliance purposes without affecting ongoing operations.

III. Data Architecture Considerations

The SIP shall design the data migration architecture in such a manner that it does not adversely impact the performance of the live eGPS during operational hours.

Appropriate data indexing, partitioning, and scheduling techniques shall be applied to optimize performance and ensure system stability during migration activities.

IV. Performance and Quality Assurance
The SIP shall ensure data integrity, accuracy, and completeness during migration.

Pre-migration and post-migration validation scripts shall be prepared and executed to confirm the successful transfer of data.

The migration utility must generate comprehensive logs and error reports to support troubleshooting and audit requirements.

15. Training and Capacity Building Requirements for eGPS

The Software Implementation Partner (SIP) shall be responsible for educating and providing comprehensive training to all personnel nominated by the DSA. This shall include staff from Project Management Units (PMUs) and other related stakeholders, to ensure that they are fully capable of testing, administering, operating, and effectively using the eGPS.

I. Training Plan Development
Before conducting any training activities, the SIP shall:
Prepare a Detailed Training Plan that aligns with the finalized eGPS design and covers:
Specific categories of training.

- Number of personnel to be trained in each category.
- Roles and responsibilities of the targeted trainees.
- Develop a Training Manual that includes:
- Curriculum structure.
- Course descriptions.
- Delivery methods.
- Training schedules.
- Training locations.

The preliminary training program shown in the reference table is informational only, representing DSA's current perspective. The SIP must conduct a detailed training needs assessment and produce a final training plan that ensures all required skills for the effective operation of eGPS are developed.

II. Training Delivery Methods
The training program may include, but shall not be limited to:

- Presentations and lectures by senior instructors.
- Intensive classroom-based training sessions.
- Distribution of manuals, handbooks, and other technical documentation.
- Briefings and orientation sessions for stakeholders.
- Interactive workshops.

- Study tours (if applicable).

On-the-job and on-site training sessions for practical application.

III. Bid Submission Requirements for Training

The Bidder shall include in their proposal a Preliminary Training Plan containing detailed descriptions for each training course to be delivered, including:

Course Title.

- Learning or Training Objectives.
- Class Size and Composition.
- Course Duration.
- Training Sequence (relation to other courses).
- Course Outline (subject areas, topics, and critical learning points).
- Delivery Methods.
- Locations of Course Offerings.

IV. Training Instructors

- All instructors proposed by the SIP must have substantial experience in their respective fields.
- All instructors must receive prior approval from DSA before delivering any training.
- DSA reserves the right to request the replacement of any instructor whose performance is deemed unsatisfactory.

V. Training Courses Overview

The table below outlines the indicative list of training courses for eGPS.

List of Training Courses for eGPS

Category of Training Course	**List of Training Courses**
a. Training courses for system users	o eGPS Usage and Operations Course for business users at DSA and PMUs. o IT Systems Usage and Operations Course for employees of DSA and PMUs.
b. Training course for IT back-office staff at DSA	eGPS Administration and Maintenance Course for technical staff at DSA.
c. Training on Trainers	eGPS Training Course for Trainers of DSA.

VI. Course Description – eGPS Usage and Operations

Target Audience: Applicable staff from DSA and PMUs who will use eGPS in their daily operations.

Business Need:

- This course will equip participants with the knowledge and skills to:
  - Perform daily payroll processing activities using eGPS.
  - Generate and interpret system reports.

- Use the system in compliance with operational and security policies.

Course Objectives:

Knowledge	**Skills**
○ Understanding of eGPS functions and services applicable to DSA operations. ○ Familiarity with new payroll workflows and administration processes. ○ Awareness of reporting capabilities. ○ Knowledge of operational and security protocols for system use.	○ Processing payroll transactions. ○ Generating payroll and compliance reports. ○ Administering assigned system functions efficiently and securely.

VII. Training Methods, Tools, and Languages

Given the diversity of users, the SIP shall adopt multiple training methods as follows:

Method of Training	**Description**	**Training Artifacts**	**Languages**
Classroom Training	Instructor-led, interactive sessions for DSA and PMU staff.	○ Pre-course reading materials. ○ Course content. ○ Participant handouts. ○ Trainer handbook. ○ Course evaluation tools.	English, Tamil, Sinhala
Self-Learning Modules	Independent learning resources for DSA and PMU users to encourage self-paced adoption of the system.	○ Digital course materials (PPTs). ○ Computer-based training modules (CBTs). ○ Instructional videos. ○ Built-in online help within eGPS. ○ User manuals and guides.	English, Tamil, Sinhala

VIII. Target Number of Participants

The indicative number of target participants for each training course is as follows:

Illustrative Number of Participants for eGPS Training Courses

Category of Users	**Training Course**	**Target No. of Users**
Operational-level users	eGPS Usage and Operations Course for DSA and PMUs	30
Trainers	eGPS Training of Trainers Course	30
Technical Staff (IT/DSA)	eGPS Administration and Maintenance Course	20

16. Warranty Operations & Maintenance of Application & System Software

The following section outlines the overview of warranty, operations, and maintenance (O&M) services to be provided by the Software Implementation Partner (SIP) for the eGPS application and related system software implemented under this contract.

- The scope of warranty, operations, and maintenance includes, but is not limited to:
- Ensuring defect-free operation of all application and system software components.
- Continuous system monitoring to proactively identify and address potential issues.
- Troubleshooting and resolution of functionality, availability, and performance-related issues.
- Implementation of approved system change requests and enhancements.

Execution of upgrades and updates to maintain system compliance, performance, and security.

The SIP shall keep the application software in good working order at all times, ensuring that any changes or upgrades requested by the Department of State Accounts (DSA) are performed within agreed timelines and in accordance with approved change management procedures.

Scope of Support Services for Application and System Software

Requirement	Scope
Compliance to SLA	The SIP shall ensure full compliance with the uptime and performance requirements of the eGPS solution as defined in the Service Level Agreement (SLA) and specified in Annexure II. All upgrades or major software changes shall be planned in advance to ensure SLA compliance and minimize disruption to services.
Application Software Maintenance	- The SIP shall rectify all errors, bugs, and functional gaps in the eGPS solution (as defined in the signed-off Functional Requirements Specification –System Requirements Specification – SRS) at no additional cost during the warranty and O&M periods. - Any functional changes outside the scope of the signed-off SRS shall require a Change Control Note (CCN). The SIP shall provide effort and cost estimates for such changes based on the per man-month cost quoted in its original commercial proposal, which shall remain unchanged for the duration of the contract. - All changes and upgrades made during the O&M phase shall undergo comprehensive, integrated testing to ensure they meet MOFPED requirements and do not negatively affect other system functionalities.
Database Management	The SIP shall manage the performance, optimization, and monitoring of database systems and application servers supporting eGPS. The SIP must ensure that database performance meets the defined SLA standards at all times.
Problem Identification & Resolution	The SIP shall detect, diagnose, and resolve all application-related issues, including but not limited to system malfunctions, performance degradation,

	and data corruption. Root cause analysis (RCA) reports shall be submitted for all critical incidents.
Software Change & Version Control	- All planned changes to the application shall be managed through a formal Change Control process, ensuring: a) Adequate communication and stakeholder notification prior to implementation. b) Necessary approvals are obtained from DSA. c) Implementation schedules are adjusted to minimize production impact. - The SIP shall define and submit for DSA approval a Software Change Management & Version Control Process. - For each change, the SIP shall prepare detailed documentation, including: • Proposed modifications • Impact analysis (functional outcomes, new features, affected modules) • Rollback plan - All change documentation shall be reviewed by DSA on a quarterly basis during the O&M period.
Maintain Configuration Information	Maintain complete and updated version control records and configuration management data for all application components, system software, and related documentation.
Maintain System Documentation	The SIP shall ensure continuous maintenance and updating of all system documentation to reflect changes, enhancements, and upgrades. This includes: a) Documenting source code for all customizations. b) Maintaining up-to-date functional specifications. c) Updating application documentation to align with current FRS and SRS. d) Updating user manuals and training manuals to reflect ongoing system enhancements. e) Adopting industry-standard practices for version control and documentation management.