REQUEST FOR PROPOSAL (RFP) FOR

DESIGN, DEVELOPMENT, IMPLEMENTATION, OPERATION AND MAINTENANCE OF INTELLIGENT TRANSPORT MANAGEMENT SYSTEM (ITMS) FOR BUS RAPID TRANSIT SYSTEM (BRTS), AMRITSAR

PART – 2
SCOPE OF SERVICES AND TECHNICAL SPECIFICATIONS DOCUMENT

FEBRUARY 2016
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

Table of Contents

1. INTRODUCTION ......................................................................................................................................... 4
2. ITMS OVERVIEW ........................................................................................................................................ 8
3. GPS BASED FLEET MONITORING SYSTEM/ AUTOMATIC VEHICLE LOCATION SYSTEM .................. 10
4. PASSENGER INFORMATION SYSTEM ..................................................................................................... 12
5. INCIDENT MANAGEMENT SYSTEM ........................................................................................................ 15
6. CENTRAL CONTROL SYSTEM (CCS) ........................................................................................................ 16
7. ENTERPRISE MANAGEMENT SYSTEM & SECURITY SOLUTION ............................................................. 38
8. TRAINING ROOM AND TEST SYSTEMS ................................................................................................. 58
9. HUMAN RESOURCE MANAGEMENT ..................................................................................................... 59
10. LEAD TIME ............................................................................................................................................... 59
11. APPLICATION AND SYSTEM AUDIT ..................................................................................................... 60
12. SCOPE OF PILOT IMPLEMENTATION ..................................................................................................... 60
13. CHANGE MANAGEMENT PROCEDURE ................................................................................................. 61
14. COMPUTERISED CALL MANAGEMENT SYSTEM .................................................................................. 61
15. PROJECT MANAGEMENT REQUIREMENTS ............................................................................................ 61
A. SERVICE LEVEL AGREEMENT ................................................................................................................ 84
List of abbreviations used in the document:

PBMS – Punjab Bus Metro System
ITS – Intelligent Transport System
ITMS – Intelligent Transport Management System
SP – Service Provider
SC – Smart Card
AVLS – Automatic Vehicle Locator System
AFCS – Automatic Fare Collection System
HTU – Handheld Ticketing Unit
BDC – Bus Driver Console
BCV – Bus Card Validator
STT – Station Ticket Terminal
SCV – Station Card Validator
BDU – Bus Driver Unit
SCU – Station Control Unit
CT – Central Terminus
DMS – Depot Management System
BTMS – Bus Terminal Management System
CCS – Central Computing System
BIM – Bulk Initialization Machine
CPD – Card Personalization Device
MTBF – Mean Time Before Failure
MTTR – Mean Time To Replace
CCHS – Central Clearing House System
GSM – Global System for Mobile communications
GPRS – General Packet Radio Service
GPS – Global Positioning System
IMS – Incident Management System
1. Introduction

The purpose of this document is to provide guidelines for procurement & implementation of Intelligent Transportation System for Amritsar BRTS. The document underlines all IT related requirements of PBMS to achieve a highly automated and stable environment for Bus Operations Management in city of Amritsar.

1.1. Objectives:

With a view to enhance commuter satisfaction, reliability and punctuality of bus operations thereby enhancing the efficiency of PBMS’s BRT operations and better management of fleet of buses and in order to instil confidence in commuters in PBMS’s services, PBMS is desirous of implementing the Intelligent Transportation Management Systems (ITMS)” (hereinafter referred to as the “ITMS” OR “The Project”). To this end, PBMS has decided to monitor the movement of the fleet of buses, collect data related to their geographical position, vehicle movement patterns and to provide relevant information to passengers.

1.2. Solution Summary:

PBMS envisages implementing ITMS for its BRT bus operations to bring in world class operational efficiency and automation for its transit operations. ITMS is expected to meet the corporate objectives of enhancing service standards, bring in commuter market approaches, better organization of planning and operations; integration of Para-transit, capital improvements, and marketing. BRT Buses shall be as per UBS 2 specification with PIS, AVLS and Surveillance equipment.

ITMS should enable PBMS to automate its Financial Characteristics, Operational Characteristics, better insight into Passenger profiles, perform Route Analysis to optimize on operational efficiency, Service Consumption, perform functional area productivity analysis and thereby creating PBMS BRTS a user choice.

ITMS shall provide a new set of tools for achieving urban local transport policies. This system shall provide services using modern computing and communications technologies. The system shall collect information about the state of the transport network, process that information, and either directly manage the network (e.g. headway management), or allow people to decide how best to use the network (e.g. incident detection, travel news). ITMS system shall play an important role in delivering policy objectives, including tackling casualty reduction, traffic congestion and pollution, as well as improving accessibility, providing integrated transport solution and making best use of existing infrastructure. The system shall deliver noticeable economic benefits through reduced journey times and increased journey time reliability, as well as improvements in safety and reductions in pollution. The benefits of using ITMS include:

- Making travel more efficient (safer, less polluting, economical, better informed travel);
- Helping to achieve ‘Best Value’ within network management as a result of greater information gathering and improved decision making;
• Simplifying public transport use by providing accurate real time information about services;
• Reducing the number of accidents by providing drivers with more information about conditions on the roads they are using;
• Helping drivers find the best route to their destination, and changing that route if major incidents occur on it;
• Improving the security of public transport passengers and staff by providing extra communications
• Providing immediate information of catastrophic incidents and prompting for immediate response (Accidents, Law & Order incidents etc).
• Two way communication between control room and crew
• Visual display of inside of a bus/BQS for control room/controllers.

ITMS for PBMS shall comprise of following distinct application areas: ("ITMS Project")
- GPS based Fleet Monitoring System / Automatic Vehicle Location System (AVLS)
- Passenger Information System (PIS)
- Incident Management System / Call Centre Management System
- Management Information System (MIS)
- Enterprise Management System (EMS)
The figure above is indicative and does not include all the activities that would need to be carried out as part of implementation of AVLS & PIS. Detailed scope is mentioned in the document below.

**Bus Station PIS Overview**
BUS AVLS Infrastructure Overview

Communication Overview

VPN Tunnel for communication over Private Network

Secure Communication link through Private Network

Cloud Computing service for Disaster Recovery
2. ITMS Overview

This following section describes overview of different component to be used for ITMS implementation for PBMS. The figure below provides conceptual view of the ITMS to be deployed for PBMS Amritsar.

The technical specification section provides specification for major IT components for PBMS:

- GPS based Fleet Monitoring System/ Automatic Vehicle Location System (AVLS)
- Passenger Information System

NOTE: All hardware equipment supplied as part of AVLS & PIS must carry industry standard certifications like U/L, CE, FCC etc. as may be applicable to different types of equipment to ascertain that, the equipment have been manufactured and certified based on international standards.

2.1 GPS Based Fleet Monitoring System

The Automatic Vehicle Location System (AVLS) shall primarily use GPS devices mounted on the vehicle as primary source of data for tracking purposes. The AVLS shall also facilitate CCS to enable public information system to act as a source of information to be displayed on the public display screens and voice based information. The AVLS shall essentially comprise of following components:

- Bus Mounted GPS based driver console- Pre-fitted in Bus (as per UBS II )
- GIS Based Fleet Monitoring and Control System

The AVLS system shall enable PBMS operations team to monitor vehicle movement in real-time and synthesize the AVL field data to deliver the same on the public information system devices installed on Bus stations, Terminals, Buses, PBMS customer portal and mobile information delivery system. GIS map of city, geocoding of route and bus stops shall be the responsibility of service provider. Vector Map scaling shall be 1:2500

2.2 Passenger Information System

The passenger information system shall consist of following units which shall offer passengers schedule and real-time information regarding operations of PBMS Bus Service and extend ease of information Delivery related to travel:

- Display Screen on Bus Stations
- Display Screens on Bus and speakers- Pre- Fitted on Bus (as per UBS II)
- Mobile App and Web PBMS Portal

The display systems at bus stations and bus terminal shall display real-time information of the route and estimated time of arrival using fixed data connections/mobile data connection with the central vehicle monitoring system. The system shall have capabilities to clearly indicate the direction and route no of the bus on the display to assist passengers.
The bus display units on the front wind shield and the back window shall display bus route information and the internal display shall display real-time information of the stations bus is going to pass through preferably by showing real-time position of the bus. The voice information system shall also derive information of the next station based on the location information derived from the GPS unit and shall have capabilities of playing pre-recorded voice information in the bus.

The web portal, at minimum, shall enable passengers to get information about the bus schedules on various routes operated on BRTS, emergency messages, concession schemes, information of other transport services etc. After selecting bus station and bus route number, it shall also have facility to deliver ETA based on the real-time data from GPS central system. The web portal shall also provide facility to passengers to extract such data through the mobile communication system.

Mobile app, at minimum, shall enable users to gain access to real time information mentioned afore for web portal. Mobile App shall also enable the user to get more specific information about their travel, recently used, mostly used routes and associated information. Mobile App shall more concentrate to provide information fast, accurate and relevant to the particular user. Communication between PIS on Bus, Bus station, Terminal and CCS shall be the responsibility of Service Provider.

2.3 Surveillance System in BRT Bus

PBMS BRT Buses shall be equipped with two inside infrared cameras and one back camera. SCU shall have features to store 48 hrs video backup with a resolution as specified in UBS 2 specification. Service provider shall have to take backup as and when required to analyse at Central Control System (CCS)

2.4 Functional units of ITMS and interrelation

The IT system for PBMS operations shall be designed to meet specific needs of following operational entities to achieve the above system needs:

- Central Control System (CCS)
  - Central Vehicle Monitoring System
- Bus Terminals
- Bus Stations
- Bus
- Surveillance System in Bus

The figure below describes the data exchange model between the individual entities of PBMS system.

Solution Landscape

The ITMS solution architecture shall be based on integrated approach wherein all the solution sub-components interact with each other to offer business computing outputs in the most optimized manner. The overall infrastructure, network and deployment architecture is depicted below:
ITMS Overview

3. GPS Based Fleet Monitoring System/ Automatic Vehicle Location System
   3.1 Bus Vehicle tracking device

   a) GPS and GPRS based Vehicle tracking unit – SCU and Bus Driver Console (BDC)

   The SCU and BDC shall be fitted in BRT Buses as per UBS 2 specification. The service provider is required to interface with the SCU / on-board computer to take necessary data required for control & operations purposes. Service Provider shall set up backend solution for the real time vehicle tracking/ central monitoring system, taking inputs from OBITS (On Bus ITS), which shall be pre-fitted in the bus.

   The SCU fitted in BRT Buses with wireless communication module (based on GPRS) shall be used to provide vehicle tracking accurately and reliably. The back end system shall be provided by service provider under the scope of this project and shall be able to produce MIS reports of the vehicle schedule adherence report and operated kilometres by each bus, by route and by fleet of each Service provider. PBMS may require additional information to be extracted from the vehicle tracking information logged at the control centre. Power system in PIS and AVLS fitted in Bus shall be through Multiplexer.

   The service provider under the scope of this project shall provide an on line WEB interface for positioning of the vehicles in the system which can be accessible to user from anywhere online.

   The single control unit (SCU) shall have two way communication and messages to be sent by driver and messages to be sent to the driver from the control centre.

Features of SCU and BDC UNIT:
For detailed specification refer Urban Bus Specification II.

The Unit should primarily be able to help central monitoring system to generate minimum of following data points as minimum and at the time of finalization of requirements a comprehensive requirement shall be furnished to the vendor:

- Start Stop
- Begin – End Shift
  - Fleet Summary
  - Detailed Activity
  - Speed
  - Fleet Status
  - Alerts
  - Battery Report
  - Unit ON/OFF Report
  - Ignition ON/OFF

PBMS can request for other reports / data / information as deemed necessary for management purposes.

b) AVLS Software:

The software shall be web based and utilizes high resolution digital map to show real-time position of the vehicles. The software shall provide map based tracking and transit route line based tracking of vehicles by the control centre operators. The software shall have enterprise capabilities which enables multiple user type to be enabled to carry out various functions like, Alarm Management, Vehicle Schedule Tracking, Speed Management, Stoppage management, Route replays, bus tracking dashboard etc as a standard functionality. The software shall enable control centre management staff quick decision making capability, which shall be achieved by providing graphical tools for visualization. The software shall enable PBMS to drill and analyse information and online data in a multi-dimensional manner. Comprehensive analysis and reporting capabilities are expected to be part of the application delivery which matches the world standard capabilities of AVLS systems.

The software should have capability to have a multi-screen based tracking system, so as to enable tracking staff to quickly analyse activities and have a better insight into operational data of all activities within the system.

Maintenance Requirements

- Device settings shall be updated including software/firmware updates through transmission via the secured communication network set up by the service provider. For reasons of security, device settings shall not be modifiable by field staff of the service provider/others.
- Any device settings modifications including software/firmware updates as well as business rules such as fare settings, discounts etc shall be done with prior authorization
by PBMS. A digital log of all changes of settings on each and every device shall be maintained and delivered to PBMS.

- Any faulty equipment shall be replaced with a tested unit from the spares provided by PBMS to the service provider
- Only a maintenance engineer with maintenance access card shall be able to access maintenance mode of the device which shall allow the maintenance engineer to diagnose the faults and update the device settings directly, if required.
- A repaired unit shall be tested by the Service provider for full functionality as at the time of initial deployment and certified before it is reinstalled at any site.

4. Passenger Information System

Passenger Information System hardware shall consist of LED based display system for bus stations and Buses. Following are the technical specifications for the display units. The passenger information system shall comprise of following components:

- Display Screen on Bus Stations and Terminal
- Display Screen on Bus
- Web Portal and Mobile App for Bus route Schedule & ETA etc..

4.1 PIS at Bus Stations and Terminal

LED based display screens that provide sufficient visibility in broad daylight condition shall be installed at PBMS bus stations and terminals. There shall be two displays per station. They shall display route and estimated arrival time (ETA) including digital advertisements and other digital content as may be approved by PBMS. They may also be used to display public service information.

The display shall receive encoded information of route and ETA from the AVTS control centre through the common wired/wireless communication link set up at each bus station. The displays must have the ability to decode the information received from CCS and display appropriate message on the screen.

4.1.1. LCD Board at Bus Stations shall have the following functional specifications:

- Display of PIS in a display unit at bus station shall be configurable based on bus station and platform. Single unit should display services of more than one platform.
- Information Display units will be supplied and mounted appropriately, configured and commissioned by the vendor.
- PIS information shall be displayed in Punjabi, Hindi and English alternatively (single or multiple language shall be configurable).
At all these bus stations, display units will receive/display transmitted contents from the central system through a gateway or mention other suitable means in the technical architecture.

Display systems need to support full colour display for streaming advertisements, digital display of text, images and video on LCD screens.

Displayed messages must be readable in high bright, day light.

Display system in addition to the display of information for PIS shall be capable of displaying advertisements and multimedia content at the bus stops and may need to alternate between Passenger information and Advertisements.

The frequency and period of information display on PIS display shall be configurable from central location for advertisements and other transit information.

Display shall provide for modular configurable layout enabling parallel display of content on different areas of the screen – Real time Transit information (Routes, ETA, Type of service, Fare, Time/Date, Public announcements, Safety information, Commercial advertising, a ticker tape at the bottom for text announcements/advertisements, other local Tourist information).

All displays for PIS will have a configurable refresh rate with minimum of 10 seconds.

4.1.2. **Display System Technical Requirement (PIS):**

- Display units shall be mounted on a rugged enclosure to withstand harsh environmental conditions with reasonable physical security.

- Display will be located at a convenient height to have a clear view of the message of next arrival bus.

- Fitment provision will have to be provided in the Bus stations. The power supply shall be made available by PBMS.

4.1.3. **Display Hardware Specification**

- One integrated tamper proof casing for complete PIS Unit addressing physical security considerations.

- Provide any hardware like PC, networking, etc. required to run the PIS and advertisements on LCD Display Units.

- Ensure smooth transition from main power supply to UPS in case of power outage.
• Aesthetic requirements such as fonts, colours, rows per page, display time to be remotely configurable and displayed based on business requirement.

4.1.4. Minimum specifications for Display units

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Parameter</th>
<th>Min. Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of Display, Screen Size</td>
<td>Full Colour LCD Display, Day Light Readable Min 32 Inch LCD TV</td>
</tr>
<tr>
<td>2</td>
<td>Min &amp; max viewing distance and angle of viewing</td>
<td>Viewing distance 20 - 100 meters Minimum 60°V – 110°H</td>
</tr>
<tr>
<td>3</td>
<td>Environmental specifications</td>
<td>Temperature: 0 to +55 deg C; Sealing: IP 65 (Front), IP 54 (Rear) Humidity: 95% RH</td>
</tr>
<tr>
<td>4</td>
<td>Minimum life of the display system</td>
<td>100,000 hours</td>
</tr>
<tr>
<td>5</td>
<td>Power supply</td>
<td>90 V to 250 V AC</td>
</tr>
<tr>
<td>6</td>
<td>Display format</td>
<td>Multimedia content, Text in Punjabi, Hindi &amp; English with presentation in tables, Fixed and scrolling Text</td>
</tr>
</tbody>
</table>

4.2 PIS on bus

PBMS BRT Buses shall be equipped with PIS as per UBS 2 specification. Passenger information system on bus shall function as an independent system and shall not be directly dependent on the CCS. They shall receive display information and voice announcement commands from the on-board GPS vehicle control module based on stored memory on the bus.

Specifications of PIS units to be installed on bus:

Refer Annexure 1: Urban Bus Specification II.

Voice Announcement system on Bus- Pre fitted on bus (as per UBS II)

The Voice PIS must play clearly audible pre-recorded voice announcements informing passengers of next bus station on route. The voice PIS shall interface with the on-board GPS module to gather location information and making the appropriate next station announcement.

Data files for Announcement system and route information shall be uploaded and updated by service provider. UBS II equipment supplier shall assist the service provider in same.

4.3 Web Portal and Mobile app for Bus Schedule & ETA

PBMS’s web portal shall extend capabilities to passengers to download route information, route schedule and real-time ETA from the web portal. This information
must be accessible using WAP enabled mobile phones also. The portal shall have facilities for pass application, card top-up using credit/debit cards. Etc. This Portal shall also enable (for authorized users) to access real time vehicle monitoring and web based report generation.

The service provider shall also be required to develop mobile App for Iphone, Ipad, Android and windows mobile devices to enable commuter to use the same for the purpose of BRTS information relating to service which may include, route planning, ETA, Offers, Fare and route tables etc.

The web portal, at minimum, shall enable passengers to get information about the bus schedules on various routes operated on BRTS, emergency messages, concession schemes, fare calculator, information of other transport services etc. After selecting bus station and bus route number, it shall also have facility to deliver ETA based on the real-time data from GPS central system. The web portal shall also provide facility to passengers to extract such data through the mobile communication system.

Mobile app, at minimum, shall enable users to gain access to real time information mentioned afore for web portal. Mobile App shall also enable the user to get more specific information about their travel, recently used, mostly used routes and associated information. Mobile App shall more concentrate to provide information fast, accurate and relevant to the particular user. Communication between PIS on Bus, Bus station, Terminal and CCS shall be the responsibility of Service Provider.

SLA for availability of the Web Portal for citizen should be 99.9%.

5. Incident Management System

Incident management is the process of managing multi-agency, multi-jurisdictional responses to disruptions. Efficient and coordinated management of incidents reduces their adverse impacts on public safety, traffic conditions, and the local economy. Incident management yields significant benefits through reduced vehicle delays and enhanced safety to motorists through the reduction of incident frequency and improved response and clearance times.

Incident management is a planned effort to use all resources available to reduce the impact of incidents and improve the safety of all involved.

An incident is any non-recurring event that impacts the transportation system.

An incident includes:
- Crashes
- Disabled or abandoned vehicles
- Debris in the roadway
- work zones
- Adverse weather
- Other events and emergencies

The incident management process includes:
- Detection
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Verification
- Motorist Information
- Response
- Site Management
- Traffic Management
- Clearance

This system would ideally execute following phases:

- THE NOTIFICATION PHASE
- THE RESPONSE PHASE
- THE RECOVERY PHASE
- THE RESTORATION PHASE

Incident management system is envisaged to be implemented as part of ITM which shall facilitate communication of activities internally to enterprise and externally as well. IMS shall act as a single point of communication exchange for all activities related to incident management.

5.1 Call Centre Management

Service provider shall be required to implement a call management system which shall enable people to communicate internally and externally. Call centre system shall act as a communication carrier mechanism and shall help different stakeholders within the system to respond to desired activities in a pre-determined systematic manner for resolution. This system shall include call management system including PC’s, Call handling equipment and EPABX.

6. Central Control System (CCS)

Central Control System will act as a live hub to manage and monitor service related data which will be viewable through a centralized application. Activities at the control centre will comprise of monitoring services, incident management and all other features defined below in this document with defined escalation procedures, activities to include monitoring health of all components (hardware, software etc.) of ITMS project through automatic monitoring system . Service Provider to provide manpower personnel to manage and maintain the CCS.

In case of emergency or critical situation in DC, data backup procedures from Disaster Recovery (DR) site should be clearly followed.

a. The Central Control System of PBMS is to be located at PBMS Project premises in Amritsar . PBMS will make provision of allotting an area for the purpose of setting up the Command Control Center.

b. Service Provider can choose to set up the Data Center (DC) either at above mentioned PBMS location or cloud based at any location within India. DC must be a minimum Tier-III level Data Center guaranteeing 99.982% availability and uptime equipped with dual-powered IT equipment, sufficient cooling accommodation for colocating servers, multiple Internet links, common servers, storage with high availability etc.
While bidding for the project Service provider shall clearly state which options they have opted and add the cost for one of the two i.e. either physical or cloud based DC. All requirements defined in this document are by considering DC has physical set up in PBMS Amritsar location and for combined features of DC and CCS. In case bidder opts for cloud based DC, requirements remains the same.

c. Deleted

d. System Provider will train the PBMS staff for using the systems and appoint personnel for troubleshooting activities

e. All applications that are part of AFCS should be accessible from the CCS. The Work Stations will be web-enabled, provide for appropriate User Access (Role based, Read only/ Read write) and other security controls. All monitoring stations shall be able to receive alerts from the on field devices and display on screen on a dashboard.

DC will receive transactional data from on board and on field devices applications into servers and Decision Support/ Business Intelligence (BI) Applications respectively to generate alerts and reports on revenue and operational parameters.

The central control system represents the operational centre of the transport service where AVLS application system shall be used to manage inputs from the field devices, the schedule system, bus-stop database and radio system for general operational control, including vehicle dispatch and dynamic scheduling. Information retrieved by the control centre from the on-board AVLS devices shall be processed by PIS application for distribution of real-time passenger information services.

The Central Control System (CCS) shall act as a nerve centre for the purposes of operations management. The systems implemented as part of ITMS allow variety of technical and operations profiles to be deployed to manage transit needs on real-time basis. Some of the profile types are such as transit controllers, incident managers etc. including the technical staff ensure business services are delivered as expected and in-event of exceptions, the same are managed to reduce any impact on operations and business.

The job involves monitoring and maintaining operational functions of an electronic reporting facility requiring the ability to monitor and maintain a range of electronic & software services, security and telecommunications systems, receive, interpret and transmit information and determine responses to incidents and; monitoring the security of persons and infrastructure from a control room perspective requiring the ability to effectively operate security systems to monitor activities, coordinate appropriate responses to incidents and organise relevant procedures via stand operating procedures.

Some of the common functions carried out at CCS are:

- Monitor and maintain electronic & software systems
- Process and organize data
- Respond to incident
- Prepare for operations
- Monitor security activities
- Maintain systems and information
6.1 Functional Requirements

The Central Control System shall provide integrated console management for vehicle tracking and alerts management.

The system should be able to provide Decision Support System to the control centre managers to dynamically manage despatch and scheduling system.

6.2 System Description

The Central Control System shall act as the integration and common ITS infrastructure management centre which includes central applications, computing infrastructure and communication system. CCS will enable data and information from all equipment’s installed at Bus station/ Buses / Bus Terminals and other vehicles to be collected and processed for requirements mentioned in the scope of the implementation.

The CCS shall process data in real time and schedule basis based on the process requirements from all the equipment through an online connected compute infrastructure to enable AVLS functions, service control and management, compliances and planning purposes.

The service provider shall consult with the authority on proposals for the type and range of operational and maintenance information to be prepared. The final content and format of presentation of processed data shall be discussed and finalised with PBMS / Authority. All process as may be agreed between authority and service provider at requirement finalization stage shall be process in term of SOP’s and implemented on the integrated platform using appropriate applications within the scope of implementation.

The operator interface to the CCS shall facilitate operations management, reporting and service delivery based on the individuals functions identified for such resources. The service provider shall provide sufficient number of CCS workstations to facilitate audit, engineering, operations and maintenance functions.

A hierarchical Access control system shall be incorporated across the system to ensure that persons can only gain access to the information or facilities that are relevant and authorised to their specific job.

The CCS shall be capable of connectivity with various suitable communication service providers providing GPRS / CDMA / fixed line connectivity through leased lines. All communication networks shall be set up, managed and maintained by the service provider through appropriate contracting terms with communications service providers.

The CCS shall be protected by appropriate fire walls from external access and outside world connections. The data transferred from the field to the CCS shall include, as minimum, information such as usage of various equipment.

The CCS shall be designed for autonomous operation of the various components of the ITMS to ensure that a failure in any one component of the system shall not disrupt the system as a whole.

The CCS shall also provide stand-in facilities, in the event of prolonged communication failure with the systems. Such facilities may include updating on bus equipment via communication channels set up at Bus depots and other means for Bus station equipment.
Depot configuration data files on the CCS shall be copied onto a backup media and hand carried to the Depots for Bus devices, if necessary.

The system provider shall create a visual tracking space on the wall using LCD displays of appropriate sizes to enable control centre staff to monitor different tracking activities. This shall include and not limited to vehicle tracking console, Alerts console, Violations Console, Trip summary Controls etc.

The central control system operators should be provided with multi-screen option to perform analysis and event tracking in a way that data collaboration can be done.

The system should additionally provide ad-hoc query based interface for the analysts to perform complex analysis. The system should provide functions to create new analysis / reports based on the user needs and same shall become part of the user report bin.

The Central Control System shall generate the necessary management reports from all transaction information received from the field equipment’s.

The CCS shall automatically collate all operations data; authenticate security features of operations data from the AVLS to provide secure and accurate audit and traffic statistics for the Buses / Routes of the depot.

The Central Control System shall provide integrated console management for vehicle tracking and alerts management

Controllers shall be responsible for ensuring safe and effective delivery of transit services to customers through responsible supervision and communication with Bus Operators. Controllers are responsible for direct supervision, prudent communications and support of operations service transit staff with regards to safety, service, scheduling and detailed documentation. Goals are to ensure a high quality transit service to customers, while maintaining a safety-first environment and cost effective system. The CCS shall be responsible for Public Transit communications, vehicle fleet management, planning and directing bus operations, utilization of transit supervisors, spontaneous decision-making, answering phone calls, performing detailed data entry, and overall street management of Public Transit operations. The CCS shall maintain duties including Help Desk and support functions, with a complete working knowledge of the Radio System, Reporting, AVL mapping and scheduling software. CCS Staff must be knowledgeable of work rules, transit contract parameters and be proficient with Microsoft Windows Applications. The CCS creates and implements all text/audio announcements for the transit system. CCS Controllers work closely with and in support of Bus Operators, Transit Supervisors, and any other contractor or city department / personnel, to ensure a high quality customer service experience to ridership. Primary Controller duties include; responding to all communications in a professional and helpful manner, ensuring that actions taken are quick and effective in handling the variety of situations that occur on a daily basis, including routine and emergency situations. Controller duties involve a high level of stress, while maintaining composure, professionalism and courtesy. Controllers are responsible for making on-the-spot analyses and decisions within the realm of authority, transit policy, contract terms and agreements. Controllers work varied hours, days and shifts, and may fill in as necessary. Controllers will perform other CCS related duties as assigned.

The system should be able to provide Decision Support System to the control centre managers to dynamically manage despatch and scheduling system
6.2.1 Cloud Based Services for Disaster Recovery

The service provider shall provide Cloud based services for Disaster recovery System to mitigate risk of any outages on account of Hardware /Software / Connectivity failure.

General Software Architecture for PBMS

Typical View for Software Components and Interfaces
6.2.2 CCS Communication Links:

The Service provider shall provide a reliable method of verifying the integrity of the data and programme files sent from the CCS to the field equipments and the correct reception of data uploads received from the devices at the CCS.

6.2.3 CCS hardware and software

The proposed set up should be capable to cater to meet the needs of a Real time Transit system involving more than 400 buses and PIS at 50 Bus stations. Additionally, the system should be capable of expanding and scaling with additional deployment of hardware and necessary amendments to software for operations of 3 to 5 times the sizing stated above.

The vendor is expected to deploy state of art monitoring screen systems for monitoring various activities like vehicles, exceptions, late & early buses, etc on a video wall kind of setting.

6.2.4 Software:

The software deployed shall include a package consisting of computer operating system software, diagnostic, testing, development and support software and software for the generation and modification of report contents and presentation.

Security features shall be incorporated to prevent tampering with any data, programs, or other facilities of the CCS.

The service provider shall provide an inventory / asset management and tracking tools for the management of all devices supplied.
All computer software documentation for the CCS including workstations shall be provided by the service provider. Necessary technical information, concerning hardware, software and firmware including system architecture, shall be provided to PBMS by the service provider upon full deployment of the system.

Scope of software includes full functional CCH, AVLS, and PIS etc as mentioned in RFP Document. The service provider shall provide asset / inventory management system managed through RFID based tagging process. All equipment which form part of hardware supply shall have RFID tags attached to them.

6.2.5 Data Storage

The design of the database system shall be arranged to keep track of all valid SC in circulation. This information shall aid in reporting any abnormal usage of stored value or trips and in providing refunds for corrupted SC.

The database system shall satisfy the following requirements:

Full-function RDBMS to Support complicated data structure will be deployed, multi-user, multiprocessing, large capacity operation, Offer data integration, data recovery and security, Support parallel processing, Provide disk mirroring functions, Authority control shall be independent of that of the operating system and Offer multilevel security management of database.

Data storage capacity shall be sufficient to maintain six months transaction data available on line for ad hoc report generation and other investigations. The volume of data to be calculated for this requirement shall assume 1,000,000 transactions per day. The database shall be easily expandable to handle another 1 million transactions a day minimum.

To maximise the utilization of the disk space of the system, system data shall undergo a regular housekeeping process. Housekeeping shall cover the files created by the CCS and the files relative to each subsystem. Any out dated or invalid files shall be archived. Duplicated records in the database and records where only the latest data need to be retained shall be merged and archived.

The system shall be able to backup and recovery of data according to different modes and periods of backup required based on their criticality and data volume. The system shall have the functionality to backup and recover all key data (usage data, system data) and files.

6.2.6 CCS Security

The Central Control System shall implement security systems to manage equipment authentication and administer the control over authority given to administrators of the operating system and others.

A stand alone, highly protected, access control system shall control access to every part of the system to the authorised personnel.
6.3 Clock Management

The Central Control System shall obtain the standard date and time and synchronize its clock automatically from PBMS or its designated master clock system. The CCS shall synchronize its clock at least once every 15 minutes. If the clock is not synchronous to the standard time, the correction shall be completed in one second.

6.4 Reports

The system as a minimum shall be delivered with capability to generate following reports; a comprehensive list of reports further than the mentioned below shall be finalized at the time of requirement finalization stage:

a. Conductor / Driver Login reports for Day, week, month
b. Non Compliance issues of different driver / conductors for the shift
c. Trip summary
d. Bus Equipment Fault Summary
e. Hourly Bus Usage Summary
f. Average Total Commuters and revenue per Route, per Bus station, per shift
g. Revenues collected on same bus station, same route, same trips by different Conductors
h. ROI route wise, trip wise, shift wise
i. Passengers boarding bus at a Bus station – Time of day
j. Daily pass usage and its ROI for the passes validated
k. Student pass usage and the Cost of the subsidy that has to be refunded by Government- daily, weekly, monthly, yearly.
l. Origin – Destination
m. SC Usage By Route Number
n. Test Card Usage by route Number
o. PBMS employees usage of services
p. Bus Service Disruption
q. En-route Ticket Inspector Summary
r. Boarding and Alighting Service
s. Boarding and Alighting statistics
t. Passenger KMS analysis per trip configurable by the user
u. Bus Rides and Revenue Statistics By Fare Code
v. Cash Revenues as per PBMS MIS
w. SCs not used for the week, Month
x. Half-Hourly Bus Usage Summary
y. Total Patronage
z. Bus Patronage And Revenue Statistics By Service Number
aa. Bus Service Revenue And Passenger Statistics Summary
bb. Boarding Ride Bus Station
cc. Summary Of Bus Passengers Boarding By Service Number
dd. System, Depot, Devices, STT CD parameters set current and pending future CD sets
e. Transfer Statistics

The above state reports are only indicative, actual list could be exhaustive based on PBMS’s requirements.

The Service provider shall provide PBMS a GRAPHICAL DASHBOARD to have visual view of all / some key reports/ parameters enabling quick decision making.

6.5 Business Intelligence Platform for Reporting

BI tool is part of ITMS project and AFCS data needs to be integrated for reporting and dash boarding purposes.

BI platform shall enable PBMS to build reports from operations data to perform multi-dimensional analysis enabling to have better insight into parameters and enable PBMS to take business decisions leading to higher operational efficiency. The BI tool hence should offer following:

6.5.1 Management Dashboard

Interactive Visualization

1) Display information in an easy-to understand format and use intuitive and interactive visualization to enable management users within authority to quickly navigate, understand, and investigate data elements to make informed decisions.

2) Allow users to capture and export the current display through electronic reports and in different printer-friendly formats, including, at a minimum, MS-Excel, PDF, and Web formats.

3) Have a default configuration and landing page for each user or user-group that are editable.

4) Allow multiple visual elements to be laid out on the same display.

5) Have the ability to display dashboards and reports using different visual elements including charts, maps, calendars, gauges, images, tables, visual and textual lists, and alerts as follows:
   o All visual elements shall have editable titles, labels, legends, axes, icons, and colors, where applicable.
   o Interactive visualization component shall display the overall aggregate status of a SMC’s KPI with proper color coding (green, yellow, red, or as defined by SMC’s preferences). It will allow the user to drill down and switch between different KPIs (e.g. KPI for average vehicle utilization, average vehicle duration, etc.)
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Display clickable contextual information related to the metrics being viewed and allows the user to drilldown on contextual information as required. Charts shall support at least the following chart types:
  a) Bar Charts
  b) Histograms
  c) Line Charts
  d) Heat Maps
  e) Pie Charts
  f) Grids
  g) Area Charts
  h) Timeline Charts
  i) Bubble Charts
  j) Radar Charts
  k) Scatter Plots
  l) Doughnut Charts
  m) Pyramid Charts

6) Maps shall have GIS Maps extension to allow plotting different mark-ups and indications on a map view using base and spatial map layers and allow the user to zoom and pan freely through the map, and be able to present heat map visualizations on GIS map data.

7) Calendars shall allow the user to intuitively navigate through calendar fields, such as day, month, and year. Calendars shall allow the user to intuitively navigate through calendar fields, such as day, month, and year. Gauges shall have the look and feel of an analog gauge (needle) with configurable level markings (green, yellow, red, or as defined SMC’s management preferences) that gives a visual display of the amount, level, and measure of defined KPI.

Tables shall be able to:
- Hold a large amount of data.
- Allow the user to scroll through the data in all directions.
- Freeze the header columns and rows when the user scrolls.
- Allow the user to enlarge/decrease the font.

Visual and textual lists shall allow the user to scroll through all of the available list items with smooth scrolling. Allow the user to choose the proper visual element required to display the required KPI data and allow the user to easily switch between alternative visual elements.

8) Have view-management tools, allowing the user to move, reorder, enlarge, shrink, open, and close visual elements with intuitive interaction.

9) Allow the user to create a new visual element based on the available visual element types and customize an existing visual element with an easy-to-use graphical interface.

10) Allow the user to save any customization done on a visual element.
11) Have zero-programming mashup capability that allows the user to configure queries and data mashups visually through drag-and-drop functionality.

12) Allow the user to drill down to display increasingly detailed data on various data elements.

13) Allow intuitive visual filtering, focusing, and selection of the displayed data and information.

14) Automatically update the parameters and filters of the displayed data when the user drills down through visual elements and update the other visual elements accordingly. Also, enable selection of filters through the visual elements and propagate selection to all visual elements in the dashboard.

15) Allow the user to filter and sort the presented data based on a number of attributes including the time period or on multiple attributes simultaneously.

16) Allow the user to search through visual elements that display numerous data entries such as tables and lists.

17) Allow the user to save the current filter and selection parameters.

18) Understand different types of structured data including numbers, percentages, fractions, general text, coordinates, and objects.

19) Store the user configuration and customizations information.

20) Have the ability to mashup different types of data from multiple sources with automatic detection of relationships between the data components and an option to manually define/overwrite relationship.

21) Run mathematical, statistical, and analytical operations on available data.

22) Compute trends and projections from data based on available historical data and based on data from external systems to enable informed decision-making.

6.5.2 Searching & Filtering

(1) Allow the user to drill down and search through the large amounts of data easily and quickly by time periods and other search criteria defined by the user. Also, provide user guidance for searching & filtering through data.

(2) Generate reports from the current view in different electronic formats including at least MS-Word, MS-Excel, PDF, and Web formats and that are printer-friendly. Not require programming knowledge or knowledge of SQL or databases to perform searches, queries, and filters.

(3) Allow reports to be sent directly to a network printer.

(4) Display a huge amount of data in a clear and organized view.

(5) Allow the user to hide or show parts of the data.

(6) Offer the capability to search multiple data sources effortlessly through a GUI.

(7) Allow the user to search, filter, and sort the presented data based on any attribute or on multiple attributes simultaneously.
(8) Allow the user to graphically define complex queries that contain multiple parameters and span different data sources.

(9) Allow the user to search through historical data

(10) Allow the user to save the current queries, filters, and selection parameters

(11) Have data-pivoting capabilities

(12) Understand different types of structured data including numbers, percentages, fractions, general text, coordinates, and objects

(13) Store saved custom queries

6.5.3 Reporting

(1) The system shall have the ability to allow the user to generate reports based on predefined report templates or by manually selecting the data and the corresponding visual elements.

(2) The system shall have the ability to provide a GUI with drag-and-drop functionality for creating custom formatted reports that include visual elements, objects, and formulas.

(3) The system shall have the ability to Display the list of available report templates, saved reports, and recently used report templates when the user logs in.

(4) The system shall have the ability to Allow the user to create, load, modify, delete, and save report templates graphically.

(5) The system shall allow reports to be generated and published on an ad-hoc or scheduled basis with the ability to predefined a list of recipients and a regular schedule through a GUI.

(6) The system shall be able to generate reports in different electronic formats including at least MS-Word, MS-Excel, PDF, and Web formats and that are printer-friendly.

(7) The system shall allow reports to be sent directly to a network printer.

(8) The system should have the ability to generate planning and forecasting reports for providing the information related to planning for no of buses to be transported

(9) The system shall have the ability for the reports to have the ability to drill down to multiple levels

(10) Reports should have the ability to print

(11) Publish reports and dashboards for planned Vs. actual data, for example the system should allow the management user to view the planned budget vs. the actual revenue spent for a particular route

(12) The system shall allow to publish reports and send them to recipients through email attachments and to a central data store to be accessed by different users.

(13) The system should not require any programming knowledge, knowledge of SQL, or dataset to create self-service ad-hoc reports.

(14) The system shall allow the user to use previously defined objects and formulas or create new custom objects and formulas and save them for repeated use.
(15) The system shall allow the user to save any configuration done on a visual element.

(16) The system shall have the ability to display data elements using different visual elements including charts, maps, calendars, gauges, images, tables, visual and textual lists, and alerts as follows:

- All visual elements shall have editable titles, labels, legends, axes, icons, and colors where applicable.
- Display the overall aggregate status of KPI with proper color coding (green, yellow, red, or as defined per SMC's preference) and allow the user to perform an interactive visual drilldown and to switch between different KPIs.
- Display clickable contextual information related to the KPI being viewed and allows the user to drill-down on contextual information as required.
- Charts shall have different types including: Bar Charts, Histograms, Line Charts, Heat Maps, Pie Charts, Grids, Area Charts, Timeline Charts, Bubble Charts, Radar Charts, Scatter Plots, Doughnut Charts, and Pyramid Charts.
- Maps shall have capabilities to show different mark-ups and KPIs on a map and allow the user to zoom and pan freely through the map.
- Calendars shall allow the user to intuitively and visually change the selected day, month, and year.
- Images shall allow the user to zoom and pan within an image and move between images intuitively.
- Tables shall be able to hold a large amount of data, allow the user to scroll through the data in all directions, freeze the header columns and rows when the user scrolls, and allow the user to enlarge/decrease the font.
- Visual and textual lists shall display an unlimited number of entries and allow the user to scroll through them.
- Alerts shall be configurable allowing for different alerts with various icons and colours to be defined and displayed.

(17) The system shall allow conditional formatting, based on thresholds or data ranges, for any cell/object in the report.

(18) The system shall allow the display of multiple data elements and result sets in the same report.

(19) The system shall allow the user to display historical data side-by-side or overlapping in views where applicable.

(20) The system shall display the generated report on screen.

(21) The system shall have zero-programming mashup capability that allows the user to configure queries and data mashups visually through drag-and-drop functionality.

(22) The system shall automatically update the parameters and filters of the displayed data when the user drills down through views.
(23) The system shall allow the user to display historical data for the current filter and selection.

(24) The system shall offer the capability to add new data sources easily through a GUI.

(25) The system shall allow the user to filter and sort the presented data based on any attribute including time period.

(26) The system shall allow the user to filter and sort the presented data based on one or multiple attributes simultaneously.

(27) The system shall have mathematical capabilities to be used to manipulate data, including basic and advanced arithmetic and statistical operations.

(28) The system shall allow the user to filter and search through the different data sources.

(29) The system shall allow the user to save the current queries, filters, and selection parameters.

(30) The system shall have data-pivoting capabilities.

(31) The system shall store the report templates and generated reports.

(32) The system shall understand different types of structured data including numbers, percentages, fractions, general text, coordinates, and objects.

(33) The system shall have the ability to mashup different types of data from multiple sources with automatic detection of relationships between the data components and an option to manually select the required relationship.

(34) The system shall run mathematical and statistical operations on available data.

(35) The system shall compute trends and projections from data series.

6.5.4 Data Retrieval & Management

General Data Retrieval

(1) Provide fast, secure, reliable, and easy mechanisms to retrieve information and data from the different data sources to meet the dashboard KPI requirements.

(2) Provide different mechanisms for retrieving data from different data sources including ETL, File Transfer, and Real-time integration.

(3) Log all received information from entities.

(4) Allow the user to define and connect new data sources and data stores effortlessly through a GUI.

6.5.5 ETL

(1) Perform ETL to extract, transform, and load operations to move the data from internal and external data sources to the staging environment and from the staging environment to the Storage environment.

(2) The system shall have the ability to perform multiple transformations on data including but not limited to
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

a. Selection
b. Translation
c. Encoding
d. Derivation
e. Sorting
f. Joining (merging)
g. De-duplicating
h. Aggregation
i. Transposing (pivoting)
j. Splitting
k. Lookup

(3) Provide the ability to define, configure, and manage ETL jobs
(4) Support import and export wizard and supporting connections with source and destination adapters including but not limited to OLEDB, flat files, and XML formats
(5) Have scheduling capabilities based on time, events, and triggers
(6) Offer the capability to define and connect new data sources and destinations effortlessly through a GUI
(7) Provide a user-friendly GUI to allow the user to handle ETL processes including:
   a. Modifying data feeds
   b. Changing of business logic used for data ETL
   c. Modifying ETL parameters
   d. Creating
   e. Editing
   f. Executing a large number of transformation rules
(8) Allow the user to view the data at different stages
(9) Allow the user to search, filter, and sort the data by stage, source, and type
(10) Allow the user to search the metadata
(11) Support batch data extraction, transformation and loading
(12) Store ETL rules and schedule
(13) Store the data at different stages including the raw data

Real-Time Integration with data sources

(1) The system shall have the capability to integrate with data sources on the real time basis to fetch the information
(2) The system shall be able to quickly retrieve the data with minimal time lag
(3) The system shall have the ability to capture the failed transaction

File Transfer

(1) The system shall support data retrieval through transferring files automatically using secure file transfer protocols such as the Secure File Transfer Protocol (FTP over SSL) protocol.
(2) The system shall support automatic file upload capabilities that can detect a new file and upload it.
(3) The system shall automatically rename the uploaded file to a proper filename including the source, date and version, based on configurable file-naming rules.
(4) The system shall properly manage duplicate submissions by keeping the old file and applying proper versioning and renaming.
(5) The system shall provide an intuitive graphical interface to AVLS Backend Users to:
   - Define the methods and rules for the file transfer such as maximum file size and supported types.
   - Define and manage the connections, file sources, file destinations, file processing, and file storage.
(6) The system shall allow the Backend Users to view file transfer history with filter and sort capabilities.
(7) The system shall perform quality management on data provided through file transfer including validation and verification of file type and size and return errors and required corrections accordingly.
(8) The system shall be able to receive and store large files as specified in the configurable file transfer rules.
(9) The system shall be able to store a history of uploaded files information and content.

6.5.6 Data Quality Management

(1) Perform data cleansing, verification, validation, and reconciliation automatically and based on defined rules.
(2) Allow the user to manage the data quality process workflow and rules using a GUI.
(3) Compare the data to historical data as reference data for detecting anomalies.
(4) Rank the completeness and validity of the processed data.
(5) Store data quality verification rules and process workflow.
(6) Store historical data.

Data Stores

(1) Retrieved data from different data sources should be temporarily stored and processed in separate Operational Data Stores (ODSs).
(2) Data used to perform visualization, reporting, and searching operations should be stored in appropriate Storage environment (e.g. Data warehouse)

6.5.7 BI Configuration and Management

BI Configuration Management

(1) The system shall allow the authorized user to complete the following functions:
   - Manage the different KPIs available by adding, modifying, or deleting KPIs or KPI groups areas using a GUI.
   - Enable or disable KPI which activates or inactivates it but does not delete it (soft deletion).
   - Configure a KPI including its ID, name, description, area, data source, format, unit, frequency, and formula.
   - Configure the user access level required to view each KPI.
   - Choose the default and alternate views for displaying a KPI.
   - Drill down by clicking on a KPI to view its details and edit it.
   - Search, sort, and filter KPIs by ID, name, frequency, measure, and indicator area.
   - Show/hide disabled KPIs from the KPI management screen.
   - Manage data sources for the KPIs easily through a GUI.

(2) The system shall have the ability to present an intuitive GUI allowing the authorized user to configure the threshold values and levels (green, yellow, red, or as defined per management preference) for a KPI by defining score card algorithms.

(3) The system shall have the ability to clearly present multiple KPIs in the same view

(4) The system shall have the ability to Configure KPIs that are aggregates of multiple other KPIs from different areas

(5) The system shall have the ability to instantly and automatically update the other dashboard components with any new KPI or changes to the configuration of current KPIs

(6) The system shall have the ability to Store each KPIs current and historical measure

(7) The system shall have the ability to Configure KPIs with multiple data sources

(8) The system shall have the ability to run algorithms to calculate the measure of a KPI based on data from subset KPIs

(9) The system shall have the ability to Store the different access levels for each of the authorized users
6.6 Dashboard and Reporting Requirement for ITMS

The list of reports given below is partial list and is being provided for the sake of understanding from the perspective of providing insight into the type of solution required to meet PBMS’s business process requirement.

List of Daily Reports needed for the service performance monitoring:

6.6.1 Category: Bus Maintenance and Availability

- **Bus Availability**
  How many buses are available in the depot at the beginning of the shift daily?

- **Bus Breakdowns**
  How many buses are in the workshop for repairs, how many buses breakdown during while in service? When multiple routes are operations, this information will be needed per individual route as well.
  Bus kilometers between two breakdowns of same bus (individual bus wise)

- **Bus Maintenance**
  Individual Bus report consists of preventive maintenance and all other work done on that bus with kilometers.

- **Schedule Adherence of individual trip of bus**
  Scheduled adherence report based on published schedule and actual schedule. Ability to sort the report by the operator by the trip will be useful.

- **Operational Issues on Field: Bus bunching, rowdy crowd etc**
  Incident reports to be generated based on information gathered by the control room on a daily basis. These reports should have bus number, trip number, operator number, time of the day, type of incident.

6.6.2 Category: On Time Performance

Definition of On Time Performance will be finalized in consultation with PBMS. Time Points within individual routes will be introduced for OTP. For all OTP, need % early, % OT and % late.

- **Scheduled KM by trip versus Actual KM by trip and Summary for day**
  The report will have scheduled kilometers against actual kilometer by trip and by day. When multiple routes are operational, this information will be needed per individual route as well.
  The report should generate missed trips or missed kilometers per individual routes.

- **On Time Performance (OTP) for Individual Trip**
  System and trip on time performance report for individual routes.

- **Daily peak, base and evening performance OTP**
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Cumulative daily performance OTP
- Weekdays and weekend performance OTP
- Waiting time of bus at the junction and time to clear the junction during off peak, medium peak and peak hours.
- Speed of a bus between stations
- Speed violation

6.6.3 Category: Station and Passenger Information

- Arrival and departure per station by individual trip
  
The report should be generated to give arrival and departure information per station for individual trips. Then for each station, the average dwell time should be calculated and measured against the total number of boarding if available.

6.7 Transit Performance Measures

<table>
<thead>
<tr>
<th>Service Offered / Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Average Daily Ridership</td>
</tr>
<tr>
<td>2 Total Monthly Ridership</td>
</tr>
<tr>
<td>3 Average Trip Length</td>
</tr>
<tr>
<td>Week day</td>
</tr>
<tr>
<td>Week End</td>
</tr>
<tr>
<td>4 Vehicles operated in Maximum Service / day</td>
</tr>
<tr>
<td>Total no. of buses operated during peak hours</td>
</tr>
<tr>
<td>5 Vehicle utilization / day</td>
</tr>
<tr>
<td>6 Passenger / revenue km</td>
</tr>
<tr>
<td>7 Fares / revenue km</td>
</tr>
<tr>
<td>8 Vehicle Operating expenses / revenue km</td>
</tr>
<tr>
<td>9 Operating Ratio</td>
</tr>
<tr>
<td>10 Staff / bus ratio</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Economics</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Service Coverage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Service Coverage</td>
</tr>
<tr>
<td>12 Frequency of buses</td>
</tr>
<tr>
<td>No.</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>22</td>
</tr>
<tr>
<td>23</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>25</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>27</td>
</tr>
<tr>
<td>28</td>
</tr>
</tbody>
</table>

### 6.8 Data centre

The data centre shall be secured access control and operated by authorised personnel only.
The data centre shall have adequate bandwidth and established DMZ for WEB casting.

The data centre shall be capable of handling a minimum of 500 transaction packets per second.

The data centre shall have fault tolerant UPS system powering all the equipments. (The service provider has to recommend if any changes are required).

The data centre shall have back up power from a diesel generator set and same shall be provided by PBMS.

The data centre shall be protected from fire hazards by suitable fire extinguisher system.

The data centre servers shall work on reliable / stable / multi-tasking operating systems.

The data centre shall have reliable communication, processing and web hosting software packages for the transit management application.

Secure data centre facility shall be provided by PBMS and Service provider shall be required to carry out all ITS related installation.

### 6.9 Specifications for LED based Video Wall Module:

<table>
<thead>
<tr>
<th>Specification Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td>LED Video wall of (Columns) x (Rows) of Super narrow Bezel LCD panels of 55&quot;</td>
</tr>
<tr>
<td>Resolution</td>
<td>1920 x 1080</td>
</tr>
<tr>
<td>Pixel Pitch</td>
<td>0.53 mm</td>
</tr>
<tr>
<td>Light Source</td>
<td>LED</td>
</tr>
<tr>
<td>Contrast Ratio</td>
<td>4000:1</td>
</tr>
<tr>
<td>Color Capability</td>
<td>1.07 Billion</td>
</tr>
<tr>
<td>Response Time</td>
<td>8 ms</td>
</tr>
<tr>
<td>Viewing Angle</td>
<td>H : 178°, V : 178°</td>
</tr>
<tr>
<td>Scan Rate</td>
<td>H: 30<del>75kHz, V: 50</del>85Hz</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>NTSC, PAL, SECAM</td>
</tr>
<tr>
<td></td>
<td>480i, 480p, 720p, 1080i, 1080p,</td>
</tr>
<tr>
<td><strong>Standard Inputs</strong></td>
<td>1x Digital DVI-I ; 1x Digital DVI-D ; 1x CVBS BNC ; 1x Component Video BNC ; 1x 5BNC (RGBHV or YPbPr)</td>
</tr>
<tr>
<td><strong>Standard Outputs</strong></td>
<td>1x Digital DVI-D ; 1x CVBS BNC</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>RS-232/RS-422/IR</td>
</tr>
<tr>
<td><strong>Input Voltage</strong></td>
<td>AC 90~240V@50/60 Hz</td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>&lt; 160W</td>
</tr>
<tr>
<td><strong>Standby Mode</strong></td>
<td>&lt; 2W at 110V</td>
</tr>
<tr>
<td><strong>Temperature</strong></td>
<td>0°C - 35°C (32°F - 95°F)</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>10% - 90%, non-condensing</td>
</tr>
<tr>
<td><strong>Operating Life</strong></td>
<td>&gt; 50,000 hours</td>
</tr>
<tr>
<td><strong>Maintenance Feature</strong></td>
<td>Quick Swap Modules</td>
</tr>
<tr>
<td><strong>Combined Bezel (Typical)</strong></td>
<td>5.7 mm</td>
</tr>
<tr>
<td><strong>Video Wall Tiling</strong></td>
<td>20 X 15</td>
</tr>
</tbody>
</table>
## ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

<table>
<thead>
<tr>
<th>Display controller</th>
<th>Controller to control Display module in a matrix of 2 (C) x 2 (R) with 4 outputs, DUAL LAN input &amp; 8 DVI inputs along with necessary software's</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Single Quad Core Intel® Xeon 64-bit 2.0 GHz CPU or latest</td>
</tr>
<tr>
<td>Ram</td>
<td>8 GB minimum</td>
</tr>
<tr>
<td>HDD</td>
<td>Min 500 GB Hard Disk</td>
</tr>
<tr>
<td></td>
<td>Hard disk Capacity should be upgradable</td>
</tr>
<tr>
<td>Networking</td>
<td>Dual-port Gigabit Ethernet Controller inbuilt</td>
</tr>
<tr>
<td></td>
<td>Support for Add on Network adapters</td>
</tr>
<tr>
<td></td>
<td>Support for Optical Fiber interface Adapters</td>
</tr>
<tr>
<td>Accessories</td>
<td>DVD-R,DVD+RW,, Keyboard, mouse</td>
</tr>
<tr>
<td>OS</td>
<td>Support 64-bit Operating Systems Windows 7</td>
</tr>
<tr>
<td>Power Supply</td>
<td>(1 + 1) Redundant AC-DC high-efficiency power supply w/ PFC</td>
</tr>
<tr>
<td></td>
<td>AC Voltage 100 - 240V, 50-60Hz</td>
</tr>
<tr>
<td>Chassis</td>
<td>19” industrial Rack mount movable</td>
</tr>
<tr>
<td></td>
<td>Front Panel should have lockable Door to Protect Drives</td>
</tr>
<tr>
<td>Wall configuration</td>
<td>4 DVI-D Outputs</td>
</tr>
<tr>
<td>Resolution output support</td>
<td>1920x1200 per output minimum</td>
</tr>
<tr>
<td>Universal Inputs</td>
<td>2 DVI Inputs</td>
</tr>
<tr>
<td>Redundancy Support</td>
<td>System Should have the redundancy support for following:</td>
</tr>
<tr>
<td></td>
<td>Fans</td>
</tr>
<tr>
<td></td>
<td>Power Supply</td>
</tr>
<tr>
<td></td>
<td>LAN</td>
</tr>
<tr>
<td>Display &amp; Controller</td>
<td>Display &amp; Controller should be from the same manufacturer</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>OEM should have a manufacturing facility in India with its own service center manned by its own engineers for providing support</td>
</tr>
</tbody>
</table>
6.10  Display Control System

6.10.1  Specifications

- Server-grade super computer architecture with 19" rack mountable chassis: Single or multiple based on configuration
- Runs on all standard operating systems: Win XP, Vista, Windows 2003 Server-64 bit, Windows 7 and with Linux Emulation
- Core 2 Duo and Xeon Quad Core with multiple processor support
- Redundant & hot swappable components: Power supplies, cooling fans, hard disk drives; dual redundant networking with optical fiber support
- Raid 0,1, 5 & 10 support
- Hardware decoding of IP streams: Supports decoding of multiple camera types, multiple formats, custom formats and resolutions from QCIF, D1 to megapixel
- Displays resolutions up to 1920 x 1200
- Single source window per channel up to 64 sources windows per channel
- Advanced control systems provide edge blending features to create seamless displays
- Full control on window sizing, positioning and scaling
- Switch fabric chassis for high demanding applications
- CPU, fan, temperature and chassis intrusion detection & alarm
- Remote management for hardware functions
- KVM over LAN, serial over LAN, LAN alert
- SNMP trap, event log, remote power control, command line interface

6.10.2  Input Sources and Capability

- Analog & digital sources supported and displayed on the same canvas
- DVI-D, RGBHV, HD Video, display over LAN, VNC, IP stream decoding
- Hardware based cards as well as software based decoding

7.  Enterprise Management System & Security Solution

7.1  EMS solution consists of the following core modules:

i)  Network Fault Management System - Provides fault and performance management of the network infrastructure that various services operate in. It provides Network Discovery & Reporting, Fault Analysis, Configuration Management, Advance IP Services Management, Service Management and Integrations with other modules.

ii)  Integrated Performance Management System - Provides comprehensive end-to-end performance management across key parts of the IT infrastructure. It allows identifying trends in performance in order to avert possible service problems and consists of:
   a.  Network Performance Monitoring - The Network Performance Management consoles provides a consistent report generation interface from a single central console. This central console also provides all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure.
b. Integrated Network Traffic Analysis System — provides details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems. Traffic monitoring system is able to track 100% of all flow traffic on the network and identify malicious behaviour with all IP conversations. It uses non-intrusive monitoring to reduce the impact on the monitored network and improve scalability.

c. Server Performance Monitoring - integrates network performance management systems and give the unified performance state view in a single console. The performance state of the entire network and server infrastructure is visible in an integrated console.

d. Database Performance Monitoring - integrates network and server performance management systems and provides the unified view of the performance state in a single console. It automates monitoring, data collection and analysis of performance from single point.

iii) Application Performance Management System

a. Application Transaction Performance Monitoring System - determines if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view. It proactively monitors 100% of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.

b. End-user Experience Monitoring System - measures the end users' experiences based on transactions without the need to install agents on user desktops. It detects user impacting defects and anomalies and reports them in real-time: Slow Response Time, Low Throughput, Partial Response, Missing component within transaction

iv) Integrated Helpdesk Solution – an ITIL v3 based Helpdesk Management Solution improves quality and responsiveness of IT support by automating help desk, self-service, knowledge management and root cause analysis. It provides flexibility of logging, viewing, updating and closing incident manually via web interface. The helpdesk solution integrates with EMS event management and support automatic problem registration, based on predefined policies and supports request management, problem management, configuration management and change order management.

7.2 Management of Infrastructure at Client-side locations

Under the proposed ITMS, there will be a number of client-side IT infrastructure components, (Desktops, Servers, Laptops, Printers etc.) that will need to be managed from various aspects like asset management. Specific management solutions should be provisioned to carry out Asset Management, Hardware Delivery at client side locations and central data centre.

1. Security Management System

With the ever-increasing number of security breaches and the potential of crippling the entire transport system of a city down with such a kind of a breach, the importance of security of the entire system cannot be under-mined. While the external threats are warded off with provisioning of firewalls, anti-virus, Intrusion Detection and Prevention systems and cordon off DMZs, the threat from internal users (departmental users and personnel of the contracted agencies) to the system also need to be recognized and guarded from.
The Security Management solution must consist of the following core module:

i. **Log Record Collection and Management** – helps automatically collate logs from the various infrastructure elements across the system, provides a graphical user interface/wizard to rules for normalizing custom log sources or modifying existing integrations, provides automatic update mechanism for Content (product integrations and reports) and monitors the current status and relative health of the logging infrastructure.

2. **Service Level Management**

The entire BRTS operations would be run in a services model, with several parts of the operations contracted to various agencies/vendors (including a number of bus operators who will run buses on various routes, IT service providers and numerous other vendors). Service Level Management for each of these service vendors and the associated contracts with each of them will be a challenge.

In such a scenario it is necessary to automate, activate and accelerate the management, monitoring and reporting of Service Level Agreements (SLAs) and service delivery. Provisions should be made for a Service Level Management (SLM) tool that takes a top-down approach – starting from business relevant service descriptions and measurement, define service metrics, establish contractual obligations and performance targets in real-time, take action based on this performance, and collaboratively report performance to both service provider and service consumer.

7.3 **Detailed Specifications for Enterprise Management System**

Enterprise Management Solution should provide end-to-end, comprehensive, modular and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance. The management system needs to aggregate events and performance information from the domain managers and tie them to service definitions.

The proposed tools should automatically document problems and interruptions for various IT services offered and integrate with the service level management system for reporting on service level agreements (SLAs). The proposed solution must be unified and also generate a comprehensive view of a service with real-time visibility into service status and identify the root cause of various infrastructure problems as well as prioritize resources based on impact. The proposed EMS solution must consist of the following core modules:

a. **Network Fault Management System**

b. **Integrated Performance Management System** for:
   i. Network Performance Monitoring
   ii. Integrated Network Traffic Analysis System
   iii. Server Performance Monitoring
   iv. Database Performance Monitoring

c. **Application Performance Management System**
   i. Application Performance Monitoring System
   ii. End-user Experience Monitoring System
d. Integrated Helpdesk Solution

a. **Network Fault Management System** – which will provide fault and performance management of the network infrastructure that various services operate in. The proposed Network Fault Management System will provide the following features:

- The Network Fault Management consoles must provide the topology map view from a single central console.
- The proposed Network Fault Management console must also provide network asset inventory reports and SLA reporting for the managed network infrastructure.

**Network Discovery and Reporting**

- The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them.
- The proposed system must support multiple types of discovery including the following:
  - IP range discovery – including built-in support for IPv6
  - Import data - from pre-formatted files (IPs, ranges, strings or ports)
  - Seed router based discovery – Using route tables and SNMP MIBs
  - Trap-Based Discovery – whenever new devices are added with capability to exclude specific devices based on IP addresses / IP Address range
- The proposed fault management system must also utilize IP Net To Media (ARP) table during router discovery for quick subnet discovery.
- The proposed fault management system must support exclusion of specific IP addresses or IP address ranges from trap based discovery.
- The system should provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
- The system must be able to support mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments
- The modelling of network connectivity must be performed using standard or vendor-specific discovery protocols to ensure speed and accuracy of the network discovery
- The system should support maps grouped by network topology, geographic locations of the equipments and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.
- It shall be possible to reduce the set of displayed devices in the topology views by flexible rules, based on the attribute contents stored with each device.
- The system must provide visualization tools to display network topology and device to device connectivity. The system must also be able to document connectivity changes that were discovered since the last update.
- The system must provide a user-configurable event to alarm mapping system that sets a differentiation that events do not necessarily need an alarm to be generated
- The proposed solution must support Network segmentation by supporting IPSEC / GRE Tunnels as well MPLS Layer 3 VPNs (e.g. VRF) & VLANS.
- The proposed solution must provide a firmware exception report that identifies devices within a group with a user-specified firmware level.
- The proposed solution must provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. When a report is run the administrator must have an option of specifying the number of consecutive days the port must be “unused” in order for it to be considered “available”.
The proposed solution must provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed management system must also intelligently determine which ports are operationally dormant.

The proposed solution must poll all the ports to determine if any traffic has passed through it. If not the port must be marked unused for that day.

### Fault Analysis

- The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
- The system must be able to ‘filter-out’ symptom alarms and deduce the root cause of failure in the network automatically
- The system should support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures and provide immediate notification when service metrics fall outside the baselines.
- The proposed system must include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
- The proposed solution must detect virtual server and virtual machine configuration changes and automatically update topology
- The proposed system must support enhanced fault isolation to suppress alarms on logical VMs when physical servers fail
- The proposed solution must have the ability to collect data from the virtual systems without solely relying on SNMP
- The proposed solution must support a an architecture that can be extended to support multiple virtualization platforms and technologies

### Configuration Management

- The system should be able to clearly identify configuration changes as root cause of network problems
- The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “startup” configurations and alert the administrators.
- The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements:
  - Capture running configuration
  - Capture startup configuration
  - Upload configuration
  - Write startup configuration
  - Upload firmware
- The proposed fault management solution must able to perform “load & merge” configuration changes to multiple network devices
- The proposed fault management solution must able to perform real-time or scheduled capture of device configurations
- The proposed fault management solution must able to store historical device configurations captured in the database and thereby enable comparison of current device configuration
against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.

- The proposed fault management solution must also support a self-certification option to support device configuration load and capture thereby enabling users to “self-certify” devices not supported.
- The proposed system should be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.

Advanced IP Services Management

- The proposed solution should be able to map and manage MPLS – VPNs by automating the provider connection resolution and monitoring the service health with an option to auto-provision service assurance tests to proactively calculate the availability of remote sites
- The proposed solution should be capable of managing the VPN Service including a complete Service Discovery of all the Devices and components that support each VPN. The solution must be able to automatically configure and provision site-to-site VRF Ping tests on each router that support VPNs to verify the ability to ping each other.
- The proposed solution should be able to support response time agents to perform network performance tests to help identify network performance bottlenecks.
- The proposed solution should be able to monitor QoS parameters configured to provide traffic classification and prioritization for reliable VoIP transport. The proposed solution should discover and model configured QoS classes, policies and behaviors.
- The proposed solution should provide the ability to discover, map & monitor multicast sources & participating routers wherein the system should be able visualize the distribution tree in the topology map.

Service Level Management

- The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
- The proposed Service Dashboard should provide a high level view for executives and other users of the system
- The system should provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
- The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/Organizations with the services they rely on and related Service/Operational Level Agreements.
- The Users definition facility must support defining person(s) or organization(s) that uses the business Services or is a party to a service level agreement contract with a service provider or both. The facility must enable the association of Users with Services and SLAs.
- The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service Guarantees that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on). Guarantees supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Root cause analysis of infrastructure alarms must be applied to the managed Business Services in determining service outages.
- SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
- The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA must be available.
- The system must provide the capability of Advanced Correlation for determining Service health, performing root cause analysis, and fault isolation. This must include applying complex Boolean logic on multiple attributes and infrastructure alarms.
- The system must provide a real time business services Dashboard that will allow the viewing of the current health of required services inclusive of real-time graphical reports.

Deployment Features

- The operations console and associated management system should be deployable in a separate physical web-server to reduce the load on the primary management server.
- The security must be able to permit or restrict operator access to different areas of information based on user security rights assigned by the administrator.
- The system needs to support concurrent multi-user access to the management system, enabling multiple read-write access to different areas of the management domain and support operator workflows.

Integrations

- The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive report generation.
- The proposed fault management system should integrate with the performance management system using a synchronized discovery and single sign-on for operators / administrators between them to enable unified Administration and ease of workflow
- The system must support seamless bi-directional integration to helpdesk or trouble ticketing system
- The proposed network fault management system should integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk
- The proposed network fault management system should attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it should be automatically created prior to submitting the ticket.

b. Performance Management – Provide comprehensive end-to-end performance management across key parts of the network infrastructure. It should allow identifying trends in performance in order to avert possible service problems.

- The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.
The proposed solution must scale to large networks while supporting a single web interface for access to reports. The system must support multiple locations and a distributed deployment for collection and monitoring. Primary instrumentation should exist in the data center.

- Provide SNMP device management of the network and server infrastructure
- Provide flow-based reporting for network troubleshooting and capacity management
- Provide Server Performance Monitoring as described
- Provide Database Performance Monitoring
- Provide Application Transaction Deep-Dive Monitoring for Web-Based Business Applications
- Provide End-User Response Time Monitoring for Browser-Based Applications

Network Performance Management and Performance Reporting System:

- The Network Performance Management consoles must provide a consistent report generation interface from a single central console.
- This central console will also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure.
- The proposed system shall collect, analyze and summarize management data from LAN/WAN, MIB-II interfaces and various servers for performance management.
- The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources.
- The proposed system shall provide Performance of Network devices like CPU, memory & buffers etc, LAN and WAN interfaces and network segments.
- It shall provide comprehensive health reporting to identify infrastructure in need of upgrades and immediate attention. Capacity planning reports shall identify network traffic patterns and areas of high resource utilization, enabling to make informed decisions about where to upgrade capacity and where to downgrade or eliminate capacity. It should also support ‘What if’ analysis and reporting to enable understanding the effect of growth on available network resources.
- The proposed system shall provide easy to read representations of health, utilization, latency and availability.
- It shall provide Real time network monitoring and Measurement end-to-end Network performance & availability to define service levels and further improve upon them.
- The proposed solution should provide the following performance reports out-of-the-box:
- The proposed system must have a report authoring capability built-in which will enable complete customization flexibility of performance reports for network devices and monitored servers.
- The proposed system should provide a real-time performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports.
- The tool should have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices using 30 second poll periods.
- The system must provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly:
o Trend Reports to present a single graph of a single variable (e.g. CPU utilization) for multiple devices across time. This would help network operators & IT managers plan or capacity and identify long drawn problems

o Top N Reports to present a list of elements that exceed / fall below a particular threshold value. This would help network operators to identify elements that share specific performance characteristics (for example, to identify over utilized elements, you would run a Top-N report for all elements whose bandwidth utilization exceeds 90% or availability falls below 95%)

o What-If Reports to perform capacity planning by observing the effect of changes in capacity & demand (for example, the report should indicate what the bandwidth utilization would be if the demand was double the historical value)

o Executive Summary Report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.

o Capacity Planning Report which provides a view of under-and-over-utilized elements.

o Service Level Reports to analyze & display service level information for an enterprise, region, department or business process. This report must show the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.

o Health Reports to analyze trends calculate averages and evaluate the health of the infrastructure. With this information, operators should be able to determine how efficiently applications and systems are running, whether critical resources are available, and what capacity planning initiatives make sense.

- The system must provide capability to measure & generate detailed performance reports for the following common TCP/IP applications:
  o DHCP: Measure the round trip latency required to obtain an IP address.
  o DNS: Measure the DNS lookup time including Latency and Packet Loss
  o FTP : Measure the time it takes to connect and transfer a file including Latency and Packet Loss
  o ICMP Ping : Measure round trip source to destination including Latency and Packet Loss
  o Latency and Packet Loss for:
    - POP3
    - SMTP
    - TCP
    - UDP Echo Test

- The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

- The tool should provide Latency (both one way and round trip times) report for critical devices and links

- The proposed system should use intelligent alarm de-duplication and automatic base lining capability to learn the behaviour of the managed infrastructure components over a period of time.

Flow-based Traffic Analysis System:

- The proposed traffic monitoring system must be able to track 100% of all flow traffic on the network and identify malicious behaviour with all IP conversations
• The proposed system must use non-intrusive monitoring to reduce the impact on the monitored network and improve scalability.
• The proposed system must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems.
• The proposed system must provide eight-hour, daily, weekly, monthly, yearly, or customizable reporting time periods.
• The bidder must provide a solution for collecting Flow data from multiple devices simultaneously across the network. The solution must provide the following Flow-based metrics:
  o Rate
  o Utilization
  o Byte Count
  o Flow Count
  o IP hosts with automatic DNS resolution
  o IP conversation pairs with automatic DNS resolution
  o Router/interface with automatic SNMP name resolution
  o Protocol breakdown by host, link, ToS or conversation.
  o Utilization by bit pattern matching of the TCP ToS field.
  o AS number
  o BGP next hop address
  o IPv6 addresses
• The proposed solution must be able to monitor and report on a minimum of 15000 unique protocols per day and display utilization data for each protocol individually. This capability must be available for each monitored interface uniquely.
• The proposed solution must keep and report on a minimum 25000 unique hosts and conversations per day for each monitored interface.
• The proposed solution must keep historical rate and protocol data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity.
• The proposed solution must keep historical rate and protocol data for a minimum of 30 days (most recent) in its short term operating database. All data in that database must have a maximum 1 minute window granularity.
• The system must support the ability to specify which hosts, conversations, IP ports, custom ToS matches and interfaces are included or excluded from the web based report.
• The system must support the ability to create reports that allow the user to search all IP traffic over a specified historical period, for a variety of conditions. The system must have the ability to search all IP traffic without loss or exclusion of any traffic. The system must support search within this period for the following at a minimum;
  o Search for any traffic using a specific configurable destination port, or port range.
  o Search for any traffic using a specific autonomous system (AS) number.
  o Search for any traffic using a specific IP subnet mask.
  o Search for any traffic using a specific IP ToS bit.
  o Search for any clients or servers communicating with more than a specific number of other unique clients or servers.
  o Search for any clients or servers that are experiencing more than a specified number of TCP resets per hour within a specified reporting period.
  o Search for any IPv4 or IPv6 conversation across the entire network.
  o Search for any protocol in use by a specific host, interface or list of hosts or interfaces.
The proposed system must be capable of automatically detecting anomalous behavior such as virus attacks or unauthorized application behavior. The system should analyze all Flow traffic and alert via SNMP trap and syslog of any suspicious activity on the network.

Flow collection systems must support a minimum of 5 million flows per minute and be capable of storing gathered information in a common database where all long term reporting information is held.

The proposed system must spot potential bottlenecks with color-coded indicators for interfaces that breach defined thresholds and durations.

**Server Performance Monitoring:**

- The proposed server performance management system shall integrate network performance management systems and provide the unified performance state view in a single console. The current performance state of the entire network and server infrastructure shall be visible in an integrated console.
- The proposed tool must provide lightweight server agents to ensure availability and performance for target server nodes and deliver scalable, real-time management of critical systems.
- The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
- It should be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.
- The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms including Windows, UNIX and Linux.
- It should also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
- The proposed tool should be able to gather information about resources over a period of time and provide historical performance and usage information through graphical reports, which will quickly show performance trends.
- The proposed solution should support management following parameters:
  - Processors: Each processor in the system should be monitored for CPU utilization. It should compare Current utilization against user specified warning and critical thresholds.
  - File Systems: Each file system should be monitored for the amount of file system space used, which should be compared to user-defined warning and critical thresholds.
  - Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem, and in applications. System agents should also analyze log files residing on the host for specified string patterns.
  - System Processes: System agents should provide real-time collection of data from all system processes. Using this it should help identify whether or not an important process has stopped unexpectedly. It should provide an ability to automatically restart Critical processes.
  - Memory: System agents should monitor memory utilization and available swap space and should raise an alarm in event of threshold violation.

**Database Performance Monitoring**
The proposed database performance management system shall integrate network and server performance management systems and provide the unified view of the performance state in a single console.

It should be able to automate monitoring, data collection and analysis of performance from single point.

It should also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.

Database performance management solution for Distributed RDBMS must include hundreds of predefined scans for monitoring various database, operating system and network resources. This should minimize the need to write and maintain custom scripts. If a special monitoring situation exists, you can modify an existing script to meet your requirements.

The event management system must send alerts for an array of server conditions, including inadequate free space, runaway processes, high CPU utilization and inadequate swap space.

The database performance management solution must support historical archive store for performance information in a compressed time-series form. DBAs should be able to drill down through layers of data to discover the cause of a condition occurring with the databases, operating system or network. These historical reports must also be usable to perform trend analysis and capacity planning.

The database performance management solution must have a console to enable users to monitor, analyze and take corrective action from a centralized point. It should also include a platform-independent, browser-based console to monitor performance from remote locations.

c. **Web-Application Performance Monitoring:**

Application Performance Monitoring System:

- The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view.
- The proposed solution must proactively monitor 100% of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.
- The proposed solution must provide deeper end-to-end transaction visibility by monitoring at a transactional level and without deploying any software at end user desktop.
- The proposed solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.
- The proposed solution must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.
- The proposed solution must support any combination of operating platforms that support JDKs higher than 1.2 or Application Server (or .NET v1.1 and above) with a single methodology.
- The proposed solution must provide a real-time application topology map to triage and quickly pinpoint the component causing a performance bottleneck in the end-to-end transaction flow.
The proposed solution must gather available performance indicator metrics from all within real-time production environments and real user transactions 24x7 with minimal overhead on monitored applications without sampling.

The proposed solution must provide for easy dynamic instrumentation of application code, i.e. be able to enhance out of the box monitoring with extra monitoring definitions without having to restart application or JVM.

The proposed solution must be able to detect production Memory Leaks from mishandled Java Collections and Sets and isolate exact component creating leaking Collection or Set (or .NET Memory Leaks within the CLR).

The proposed solution must allow monitoring granularity of no more than 15 seconds for all transactions.

The proposed solution must provide real-time monitoring of resource utilization like JVM memory usage, Servlets, EJB pools, DB connection pools and Threads.

The proposed solution must be able to identify socket and file Input / Output activity from the application.

As a means of detecting poorly performing SQL, the solution must be able to proactively record all SQL calls, and report on the slow performing ones. The SQL measurements must be made from within the monitored application – not using an external database agent.

The proposed solution must monitor performance of all stored procedures being executed from within the Java/.NET application.

The solution should have provision for automatic transaction discovery, for example by setting up some bounding parameters to describe transactions like the web site, the language, and parameters (such as post, query, and cookies).

The proposed solution must provide ability to monitor performance of applications up to the method level of execution (Java/.Net method) 24x7 in production environments with negligible impact on monitored application.

The proposed solution must be able to report on any application errors occurred while executing application functionalities and pinpoint exact place of error within transaction call stack.

The proposed solution must provide for at least 2 levels of thresholds which can be set on alerts and provide for actions so that alerts can automatically trigger other processes when thresholds are breached. The proposed solution must not necessitate any changes to application source code.

The proposed solution must proactively identify any thread usage problems within applications and identify stalled (stuck) threads.

The proposed solution should allow SQL statement normalization by aggregating hundreds of related SQL statements into a single performance metric using regular expressions and pattern matching.

The proposed solution must monitor individual web service and performance transaction debugging for web services. The proposed solution must also monitor web services across multiple processes (cross JVM tracing)

End-User Experience Management System:

The proposed solution should measure the end users’ experiences based on transactions without the need to install agents on user desktops.

The solution should be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.

The proposed system must be able to detect user impacting defects and anomalies and reports them in real-time:
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Slow Response Time
- Fast Response time
- Low Throughput
- Partial Response
- Missing component within transaction

- The proposed system must be able to provide the ability to create user groups based on application criteria or location and link user ids to user names and user groups.
- The proposed system must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.
- The proposed system must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.
- The proposed system must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.

**d. Helpdesk Management**

- The proposed Helpdesk Management System must be ITIL-v3 based and provide support for various defined ITIL processes
- The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface.
- The web interface console would also offer power-users tips.
- The proposed helpdesk solution must provide seamless integration to log incident automatically via system and network management.
- The proposed helpdesk solution must provide classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, severity levels and impact levels.
- The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.
- Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no programming.
- The escalation policy would allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact.
- The proposed helpdesk solution must provide web-based knowledge database to store useful history incident resolution.
- The proposed helpdesk solution must contain built-in knowledge tools system that can provide grouping access on different security knowledge articles for different group of users.
- The proposed helpdesk solution must integrate with EMS event management and support automatic problem registration, based on predefined policies.
- The proposed helpdesk solution must be able to log and escalate user interactions and requests.
- The proposed helpdesk solution must provide status of registered calls to end-users over email and through web.
- The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- The proposed helpdesk solution must have the ability to track work history of calls to facilitate troubleshooting.
- The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.
The proposed helpdesk solution must support request management, problem management, configuration management and change order management.

The proposed helpdesk solution must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.

The proposed helpdesk solution must have an integrated CMDB for better configuration management & change management process. The proposed helpdesk solution must have a top management dashboard for viewing the helpdesk KPI in graph & chart formats.

The proposed helpdesk solution must support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.

### 7.4 Detailed Specifications for IT Asset Management

- The proposed solution shall provide inventory of hardware and software applications on end-user desktops including information on processor, memory, operating system, mouse, key board of desktops etc. through agents installed on them.
- The proposed solution shall also provide the ability to obtain similar information as above without the agent installed on target workstations (also known as agent-less).
- The proposed solution shall have reporting capabilities; provide predefined reports and the possibility to create customized reports on data in the inventory database.
- The proposed solution shall provide facility for user defined templates to collect custom information from users at desktops / workstations.
- The proposed solution shall provide facility to recognize and provide inventory for custom applications on desktops.
- The proposed solution shall provide facility for queries and automated policies to be set up on existing data in database and permit scheduling of data collecting engines to pick up the data at defined intervals.
- The proposed solution shall support UNIX, Linux, Apple OSX apart from Windows environment for inventory management.
- The proposed solution shall provide file management capabilities for the monitored systems: it should be able to find out specific files and directories on a workstation based on queries.
- The proposed solution shall allow collection / restoration of configuration files at remote desktops, using which standardization of configuration can be achieved of all the desktops. e.g. configuration files / settings related to a particular application which involves changing of registry parameters and configuration files.
- The proposed solution shall display the names of the applications being monitored for usage.
- The proposed solution shall support dynamic grouping for enabling assets to be grouped dynamically based on some pre-defined criterions. Like a Group can be able to display how many and which computers have a specific application installed. As and when a new computer get the new application installed it should dynamically get added to the group. Another Example: If a hardware upgrade is taking place, two Dynamic Groups can be created; one to reflect the computers not yet upgraded, the other group, the upgraded computers.
- The proposed solution shall be able to use the query tool to identify specific instances of concern like policy violation (presence of prohibited applications/games and old versions etc.), inventory changes (Memory change etc) and accordingly it could perform several actions as reply. These actions could be:
  - Sending an email
  - Writing to files, sound an alarm
Adding the computer to a Group
Message to scroll on Monitor screen of the administrator

- The proposed solution shall provide the facility to track changes by maintaining history of an asset. History period shall be configurable.
- The proposed solution shall provide a web-based console.
- The proposed solution shall be able to collect inventory from add/remove program functionality in Windows environment.
- The proposed solution shall support event policies such that pre-defined actions can be triggered when key events occur such as software license violations etc.
- The proposed solution shall provide an option to share the database with the proposed service desk solution such that it can leverage information available in Asset management database.
- The proposed solution shall provide delivery, installation, and de-installation of software etc. installed on end-user desktops by software delivery remotely through agents installed on them. It should allow pre- and post-installation steps to be specified if required & support rollback in the event of failure in installing software to end-user desktops.
- The proposed solution shall leverage information stored for intelligent software distribution - e.g. identify systems satisfying certain prerequisites and ensuring delivery of the right software to the right system. It should also be able to integrate with the asset management solution.
- The proposed solution shall support both push and pull software distribution modes. A catalog/advertisement option of the existing software delivery packages should be provided for end-user, if required, and an option regarding which software to pull can be exercised by the end-user at his will.
- The proposed solution shall facilitate distribution to be scheduled for a single unit, a group of units, or the whole domain. Software delivery solution should report on what software is installed where, when it was installed, and by whom. The job status could inform the administrator about the current status of any distribution.
- The proposed solution shall provide User Control on the software distribution: Users should be allowed to cancel jobs if they are launched at an inconvenient time. Cancelled jobs should be reactivated. Forcing packages onto the computer should also be possible.
- The proposed solution shall support software Package Creation using Generic scripts. The software delivery software should provide a Wizard for auto script builder on Intel platform.
- The proposed solution shall support reinstall after crash for the systems which crashes and requires the same set of software after it has been serviced. It should identify such machines and would automatically install the required software.
- The proposed solution shall have the intelligence to install a required set of software for any computers added in a particular department/group based on the predefined criteria.
- The proposed solution shall ensure that software deliveries run in the background ensuring that the end user cannot click any buttons or change settings.
- The proposed solution shall support software distribution to Dynamic groups. Administrators should have the ability to create distribution groups based on relevant criterion. Dynamic Groups to be built using search arguments presented to an asset and inventory management solution.
- The proposed solution shall support a wide variety of clients. This includes all desktop systems, including Windows Server and Desktop operating systems, various flavors of UNIX & Linux. It shall also provide inventory collection functionality from mobile operating platforms such as Windows Mobile and Palm OS via Proxy agents.
The proposed solution shall offer several levels of security for remote control, ranging from defining users with specific rights to requiring a specific IP address and local confirmation before a remote session is enabled.

The proposed solution shall have the ability to perform diverse tasks on multiple remote systems simultaneously, view a host machine from multiple viewers, transfer control between users and allow a host machine to initiate a connection to a viewer.

The proposed solution shall provide users the ability to record a session of remote control for later playback.

The proposed solution shall provide chat functionality between remote control viewer and host as well as a file transfer utility for drag and drop transfer of files between remote control viewer and host.

The proposed solution shall allow administrators to centrally manage remote control users’ and their access rights. In one easy-to-use interface administrators would be able to define preferences and capabilities different users or user groups have, as well as defining which targets they can control. It should restrict users from changing the policies permanently.

The proposed solution shall support remote reboot functionality.

The proposed solution shall provide the facility to throttle the bandwidth used by the tool while communicating over the network if required.

The proposed solution shall provide the facility for encrypting the authentication traffic and additionally encrypt viewer/host traffic as well.

The proposed solution shall support centralized policy management.

The proposed solution shall support centralized access control management for users/groups.

The proposed solution shall provide the facility to lock/unlock remote host to prevent remote control connections to the host.

The proposed solution shall provide Windows integrated authentication as well as its own application based authentication option to choose from for the agent installed.

The proposed solution shall allow users to connect over the Internet and through proxy servers without having to re-configure the firewall or the proxy servers. Should support certificates like X.509v3.

The proposed solution shall provide a uniform patch management process framework with a dedicated content research team to manage the central repository of software patch information.

The proposed solution shall manage and preserve desktop software configuration, such as user settings, preferences and data so that it helps in seamless migration or upgrades to new OS such as Vista/Windows 7 etc.

The proposed solution shall provide a web access console for a comprehensive view of asset management information, including: - Computers, Users, Software packages, Software definitions, Jobs, Policies, Queries

The proposed solution shall provide support for ITIL release management support and integration with tools like service desk/helpdesk.

The proposed solution shall collect and report information such as antivirus signature data and information on host based intrusion prevention system agents.

The proposed solution shall allow launching of antivirus/antispyware signature updates at agent level and should also have capability to start services for product such as HIPS.

The proposed solution shall support Security Content Automation Protocol (SCAP) for enabling automated vulnerability management, measurement, and policy compliance of IT systems.
The proposed solution shall support Open Vulnerability and Assessment Language (OVAL).

The proposed solution shall support Federal Desktop Core Configuration (FDCC) to help ensure compliance with regulations and also generate compliance reports.

The proposed solution shall provide High Level Executives intelligence with regards to existing IT data, derive governance context and presenting all this information in the most appropriate and intuitive fashion for key stakeholders to make decisions.

The proposed solution shall provide Request Management functionality

The proposed solution shall provide Contract Management, Vendor Management, Financial Asset Management functionality.

The proposed solution shall provide Software License Management features.

7.5  Detailed Specifications for Security Management System

Security Management solution should address identity risk and compliance by validating user access, preventing users from gaining conflicting access rights, controlling orphaned accounts. It should improve business efficiency and user productivity by enabling users to be immediately productive and allowing administrators to focus on business initiatives rather than mundane, labor-intensive tasks. The Identity Lifecycle Management solution should deliver comprehensive capabilities that include identity compliance, privilege cleanup, user provisioning and role management in an integrated solution. The proposed Security Management solution must consist of the following core modules:

7.5.1  Host-based Server Access Control System

The proposed Host-based Server Access Control Solution should be able to protect critical server infrastructure and minimize security risks by regulating access to confidential data and mission critical services. The solution should provide policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Specifically, it should proactively secure access to data and applications located on Linux, UNIX and Windows system servers throughout the infrastructure.

- Host based security solution must allow controlling of access to all system resources including data files, devices, processes/daemons and audit files.
- The solution should provide fined grained User Control. The proposed solution must allow controlling actions and access to resources of all users including privileged accounts such as root / administrator. The solution must track the "real user" even in case of surrogates.
- The solution should provide Rights Delegation. The proposed solution must provide the ability to designate specific users as Administrators, Auditors, and Password Managers etc with appropriate rights. The proposed solution must also provide the ability to designate specific users as Subordinate or Group Administrators, to manage users and file permissions for their Group
- The solution should support cross platform Management. The proposed solution must support management and policy distribution across various Windows, Linux and UNIX platforms from a central management console. It must support the deployment of the same policies across multiple servers ensuring consistency of security policies across machines in the enterprise.
- The solution must provide capability to allow access to sensitive resources only through approved programs.
The solution should provide Process Controls – Administrator must be able to control the circumstances, under which authorized users may terminate sensitive processes (daemons), including time and day, where from, etc.

The solution must provide Stack Overflow Protection (STOP) – Must be able to prevent stack overflow exploits on UNIX systems, to ensure that arbitrary commands cannot be executed in order to break into systems.

The solution should be able to fully work with Windows Active Directory in both directions, ensuring any existing deployment of AD infrastructure is not affected.

The solution must provide support for IPv6 and FIPS140-2

The solution must provide administrative password checkout function. It should provide workflow for requesting and checking out a system-generated. The solution should provide the functionality to force the user to check the password in once their task is completed, or PUPM should provide the capability to be configured to automatically check the password in after a specific time period; and it can be a manually forced check in as well.

The privilege user password management (PUPM) must provide a fully functional and customizable workflow that provides common out-of-the-box use cases for PUPM. The solution must provide a break glass feature. A break glass scenario occurs when a privileged user needs immediate access to an account that they are not authorized to manage. Break glass accounts are privileged accounts that are not assigned to the user according to their role. However, the user can obtain the account password immediately, without approval, if the need arises. This eliminates the possibility of a delay for an admin to approve the request. All transactions related to the break glass scenario must securely be logged for audit purposes.

The solution should provide a feature to eliminate passwords from scripts. Via PUPM, it should be possible to replace hard-coded passwords in scripts with privileged account passwords that are generated by PUPM only when needed.

The solution should provide a unified web based console which consolidates all aspects of privileged user management under a single console — host access control and privileged user management across physical and virtual systems, devices and applications.

The solution must support a wide range of virtualization platforms including but not limited to: VMware ESX, Solaris 10 Zones, LDOMs, Microsoft Hyper-v, IBM VIO, AIX LPAR, HP-UX VPAR, Linux Xen and Mainframe x/VM, providing for more consistent security management of access control risks across these virtual partitions, in addition to physical platforms.

7.5.2 Identity and Access Management

- Must provide centralized administration of user-ids and password management.
- Must provide a central directory of users, their real-world business information, their accounts, and their access rights across the enterprise without requiring changes to end-systems.
- Must have APIs to enable additional user management operations on UNIX, NT over and above the default operating system account set-up.
- Must have LDAP interface to enable queries/updates by authorized third-party customer tools.
- Must support enforcement of a centrally-defined security policy, e.g. for access rights, password lengths
• Role-based Administration. Role Based & Rule Based User Provisioning.
• Should have an embedded work flow which would help in automating routine tedious tasks like approval processes.
• Must provide advanced Web support, to allow for smooth access and personalization of the user interface for each user. Once a user has been authenticated to the sign on system, access to all authorized Web applications and resources must be handled by this system.
• Must include out-of-the-box support for specified relevant third-party technologies - Authentication, PKI, and smart cards.
• Must provide access to only those applications/resources that the user/customer has authority to.
• Must be able to integrate with user administration product.
• Provide capabilities to perform recertification of identities across the Enterprise.
• Should provide capabilities to have Corporate Directory as well as Provisioning Directory.
• Web access management system itself should use 128-bit RC4 encryption between its distributed components.
• Web access management system should support single sign-on across security domains.
• If a user is authenticated at a low level of security (e.g., password), then they should be forced to re-authenticate when they attempt to access a more sensitive resource (e.g., one protected by a token card).
• The priority of these authentication methods should be Administrator specified. It should not be hard-wired into the product, and Administrator should be able to control the priority of each Authentication method. 1000 levels of priority should be supported.
• Solution should support directory chaining.
• Solution should provide protection from cross-site scripting.
• Administrator should be able to integrate dynamic/external data (at run-time) in the enforcement of my policies via a Web service.
• The solution should provide a seamless universal single sign-on across web and client server applications. Both client server single sign-on and web single sign-on solutions should integrate out of the box.
• Administrator should be able to create policies that perform comparative tests on each user’s directory profile information.
• Solution should support controlled “impersonation” of users allowing certain users to temporarily use the entitlements of other users without sharing of passwords.
• Solution should provide single sign-on between the main user portal and its affiliates.
• Solution should support SAML (the standard for exchanging authentication and authorization information between security management systems) without coding, including both SAML Consumer & SAML Producer modes of operation.
• SAML Consumer capability should support both one-to-one user mapping as well as many-to-one user mapping.
• Solution should support full replication of all components.
• Solution should support automatic failover and Failover between clusters
• Solution should support 4 & 8-way SMP servers.
• Solution should do dynamic load balancing across all servers.
• Solution should also load balance across directories.
• Administrator should be able specify that a certain directory be used for user authentication, but a different directory be used for user authorization. It should also allow multiple directories to be configured. For example: Customers can be managed in one directory, employees in another, partners in another, etc.
7.5.3 Log Record Collection and Management

- The system shall provide a graphical user interface/wizard to rules for normalizing custom log sources or modifying existing integrations.
- The system shall provide automated update mechanism for Content (product integrations and reports). This process shall occur seamlessly and transparently without any customer intervention as part of the subscription update process.
- "The system shall support the following methods for log collection:
  o Windows Management Instrumentation (WMI) for remote collection from the Windows Event Log
  o System log
  o Open Database Connectivity (ODBC)
  o Text Log (flat file)
  o Open Platform for Security (OPSEC)"
- The system shall provide a mechanism to monitor the current status and relative health of the logging infrastructure.
- The system shall have the capability to drag and drop building of custom queries & reports.
- The system shall be capable of operating at a sustained 3000 EPS per collection device. The system shall provide the ability to scale to higher event rates by adding multiple collection devices.
- The system shall have the capability for updates delivered and applied via an update service provided by the vendor to keep the system up-to-date. This includes the agents and it should be pushed centrally without having to reinstall the agents.
- The system shall have a secure and preferably embedded log repository to store logs that does not require separate database expertise to administer and manage.

8. Training Room and Test systems

8.1 Scope:

The service provider shall set up training and test facility adequate for training all staff of the service provider. Each staff member shall be deployed on the front end or at CCS centre only after certification jointly by Service provider and PBMS.

Service provider shall create training manuals and other necessary aids to ensure the perpetual need for training as and when required for PBMS/Operator Personnel is required.

The training room shall be general training room pertaining to all ITS components and operational requirements.

8.2 Handover/Takeover

The service provider shall ensure that PBMS is sufficiently trained and skills are continuously upgraded to ensure complete takeover of the system at completion of the contractual agreement.

The service provider is required to impart training and necessary tools in-order to take-up operations whenever necessary. Service provider shall six months before the end of the contractual period go through a process of hand-over take-over with PBMS personnel’s and act in supervisory role for smooth take over.
8.3 **Functional Requirements:**

The devices and sub-systems shall be connected to the test CCS by an independent LAN / WAN that will permit the exchange of controls and data in a similar manner to that implemented for equipment installed in field.

8.3.1 **Use as Prototype**

The service provider shall develop software applications / manufacture equipment or accessories at the training and testing facility for testing as a prototype. Deployment will follow after joint evaluation by PBMS and the service provider.

9. **Human Resource Management**

There shall be a Project manager as a representative of the service provider at the time of implementation followed by an Operations manager, employed as the head of operations by the service provider, after the start of commercial operations. Project manager shall act as the single point of contact and shall be responsible for all the deliverables of this agreement. The operations manager shall be the single point of contact with PBMS after the start of operations.

10.1 **Central Control System**

All the manpower required for Central Control System including the hardware maintenance shall be arranged by the service provider. Required database, SW and report experts shall be organised by the service provider. The proposal must include the costs for these operational personnel. Any shortcomings shall be made good by service provider, and if needed, deploy additional personnel to ensure satisfactory services.

10. **Lead Time**

The successful bidder will initiate the Project activities within a maximum period of 3 weeks as defined in Part -1 of this RFP. The successful bidder shall have to set up a pilot demonstration at one bus station with respect to Passenger information system. They shall also install and demonstrate Automatic Vehicle Location system on one bus. This pilot demonstration shall be done within 3 Weeks as defined in Part -1 of this RFP.

The Project Implementation shall be done in timeline specified in Lead Time. The Lead Time for each phase/Request Order of ITMS Project shall to be stipulated in discussion with the Service Provider before implementation order is given. Authority's decision in this regard shall be final but reasonable time would be given. This will form the basis for application of Liquidated Damages.

The service provider shall give PBMS a clear project implementation plan within 20 days after signing the service agreement, in consultation with and to the satisfaction of PBMS. This plan shall include details of the project implementation team and benchmarks of delivery of equipment, installation of equipment, integration and setting up of the Central
Control System (CCS). Upon completing the set up, the service provider shall do a test run for the entire system, remove any shortcomings and resolve any bugs in hardware, software, communication network and Central control system and have the system ready for commercial operations one month from the completion of set up.

11. Application and System Audit

PBMS shall appoint a third party auditor capable of auditing IT systems envisaged as part of AVLS & PIS implementation. The service provider shall be required to provide necessary information to the third party auditor to facilitate testing and audit of hardware, software and processes related to AVLS & PIS.

12. Scope of Pilot Implementation

a) Central Computer System
   - Central Computer System
   - Upload data from Field equipment to Central computer system
   - Processing the data and generating the reports
   - Backend Hardware and Software Setup (Not needed on actual configuration systems)
   - Reports and Sample MIS will be generated

b) GPS Based Fleet Management System
   - Backend Hardware and Software Setup
   - Real time tracking of GPS fitted vehicles (Preferred UBS -2 compliant GPS)
   - Refreshing data at a fixed interval of time
   - System can be accessed over the internet
   - Sample MIS & Reports will be generated

   -

c) Public Information System
   - Bus Stop Display Boards will be fitted at one bus stop and they will fetch the information over GPRS currently
   - System can be accessed over the internet
   - Sample MIS & Reports will be generated
13. Change Management Procedure

Any changes having technical or commercial implications will have to be mutually agreed upon in advance, prior to making the change. In case of situations, that the impact is not dependent on one or both parties’ agreement, the revised commercials will be effective from the date of impact.

For avoidance of doubt, the parties expressly agree that

- Change Request shall not be effective and binding unless agreed in writing and signed by both PBMS and Service Provider.
- The payment of any additional cost agreed under a Change Request shall be in addition to the payments agreed upon under this Agreement.
- Upon a Change Request becoming effective, the Project Schedule shall automatically stand adjusted by the additional time required for implementing the Change Request.

14. Computerised Call Management System

The service provider shall be required to implement service call management system capable of logging service request call within the enterprise of PBMS ITMS. The system shall uniquely identify all calls by way of assigning ticket numbers and resolution procedure. This system shall provide PBMS a computerised log of all incidents logged as part of the ITMS operations. The system should further provide analytical reports to evaluate problem areas and escalation system to ensure problems are reported properly and resolved.

15. Project Management Requirements

The scope, duration and size of this project require the service provider to create an effective Project Management team to assure the success of the work. The following Project Management elements shall be incorporated as a key component of the project.

a) Project Management Personnel

The Service Provider shall establish a Project Manager, who shall be highly responsive to the needs of PBMS as required in these Specifications and subject to PBMS acceptance. The Project Manager shall coordinate design and engineering activities and provide a technical liaison to PBMS. This person shall be highly competent and fully qualified in all aspects of the System. Where support is provided from individuals or groups outside the project, the support personnel shall be under the control of the Project Manager during the period of support, and support groups shall be required to provide support as their highest priority. An organization structure that diffuses responsibility and does not require that resources be assigned at management request is not responsive to this Contract and will not be accepted or tolerated by PBMS. To accomplish the above, the Service Provider shall assign a permanent Project Manager and Senior Technical Staff Member (STSM), subject to PBMS approval and assure compliance with the project management requirements of the Specifications and Agreement.

b) Project Manager
The Project Manager shall be identified to PBMS, within seven (7) days after notice to proceed.

c) Authority

The Project Manager shall have the contracting authority to issue and approve purchase orders and to contractually bind the Service Provider. The Project Manager shall have the authority to assign and schedule Service Provider to perform all of the Work required by this Agreement, and act as Service Provider’s representative for dispute resolution.

d) Responsibility

The Project Manager shall provide a single point of contact for PBMS to resolve all issues related to this Contract. The Project Manager shall be responsible for directing all Subservice providers’ designs and work.

e) Project Understanding

The Project Manager shall have a full and complete understanding of the Contract Documents and site conditions sufficiently to provide adequate direction for coordination of work.

f) Qualifications

The Project Manager shall have at least 10 years of experience in design and management of Transit ITS projects, with at least one completed project assignment for a fleet in excess of 200 vehicles. PBMS shall be the sole determinant of the suitability of the proposed Project Manager’s qualifications. PBMS reserves the right to have the service provider replace the Project Manager if qualifications are not met.

g) Availability to the Project

The Project Manager shall be available to PBMS on a twenty-four hour per day, seven days per week basis and shall respond promptly to any reasonable PBMS request. Coverage of this requirement by any alternates shall be subject to approval by PBMS.

The Project Manager shall be on site during all significant project events, as necessary to facilitate meetings, project activities, and information flow between the service provider and PBMS, and as requested by PBMS.

h) Senior Technical Staff Member

The STSM shall be available to the Project within seven days after LOI issuance.

i) Responsibility

The STSM shall act as a technical resource for coordinating all system design and implementation issues. The STSM shall check each technical submittal prior to its being sent to PBMS for approval. The STSM shall all technology related work to assure quality.
j) **Project Understanding**

The STSM shall have a complete understanding of the technical requirements of the Contract Documents and site conditions sufficiently to provide design direction and to determine compliance of the service provider’s design submittals and work.

k) **Qualifications**

The STSM shall be a Professional Engineer, who qualifies as acceptable to PBMS. The STSM will have a minimum of 10 years of experience, including three years or equivalent experience in coordinating engineering and administrative support activities for ITS. PBMS shall be the sole determinant of the suitability of the proposed STSM’s qualifications. PBMS reserves the right to have the service provider replace the STSM if these qualifications are not met.

l) **Availability to the Project**

The STSM shall be on site during all significant project events, as necessary to facilitate meetings, project activities, and information flow between the service provider and PBMS, and as requested by PBMS. In no case shall it be considered acceptable for the STSM to be on site less than ten (10) days per month. Coverage of this requirement by any alternates shall be subject to approval by PBMS.

m) **Project Meetings**

i) **Attendance**

The service provider’s Project Manager and STSM shall attend Progress Meetings held weekly.

The service provider’s Project Manager and STSM shall conduct a Project Kick off Meeting with PBMS stakeholders, Steering Committee, and the PBMS Consultant Manager.

The service provider’s Project Manager and STSM shall attend additional meetings, as requested by PBMS and the PBMS Consultant pursuant to the coordination of the Work.

ii) **Location**

Progress meetings shall be held at PBMS facilities unless otherwise specifically approved by PBMS. Other meetings shall be held at a mutually agreeable location, conducive to the topic of the meeting. For any project meetings conducted by conference call, service provider shall, at the service provider’s expense, provide a conference call-in number.

iii) **Meeting Minutes**

The service provider shall prepare minutes for each meeting, unless specifically instructed otherwise by PBMS. The Service provider shall prepare the minutes and distribute them to the attendees within two working days after the meeting. Minutes of Meetings shall include names of attendees, significant proceedings, decisions, unresolved issues, and a list of information requested by PBMS. The minutes shall be of sufficient detail to record any decisions made at the meeting and any follow-up actions required. The minutes shall include
a summary of open action items, the party responsible for each, scheduled date for the action, and the respective resolution. Service provider shall provide a rolling project report, adding and deleting items as necessary.

iv) Agenda
The Service provider shall prepare the agenda for each progress meeting. The Service provider shall provide a draft agenda to PBMS at least one week prior to each meeting and request that PBMS add any additional items. Review of the previous meeting minutes and any outstanding action items shall be included on the agenda for each meeting. Each progress meeting agenda shall also include the item, “Additional PBMS Issues and Concerns.”

n) Schedule
Detailed Contract Schedule
The detailed contract schedule shall be a critical-path-method schedule constructed using Microsoft Project or other software application acceptable to PBMS. The detailed contract schedule shall show each activity, including interface activities, for completion of the Work, and shall be properly ordered and sequenced. Six printed copies and one electronic copy of the detailed contract schedule shall be submitted for PBMS approval within 15 calendar days after LOI.

Task Duration Limits
The detailed contract schedule shall be sufficiently detailed to preclude the use of activity durations greater than 15 working days. Activity durations shall include allowances for lost time and inefficiencies.

Task Designations
Each task designation shall delineate the phase or stage of the work, and the component of the work such as design, submittal, submittal review, procurement, fabrication, delivery, installation, and testing.

Task Details
Where appropriate to the understanding of the task, additional details shall be provided, such as:

• A clear description of the activity, including its location.
• The duration expressed in full working days.
• A responsibility code denoting the Service provider, a subservice provider, PBMS, a government Agency, or a utility performing the activity.
• The quantity of material, in units.
• The integer percent complete representing the installed progress.
• The actual start and finish dates when applicable.
• Unless specifically agreed to in writing by PBMS, Service provider is responsible for all Work to complete any task.

Critical Path
The detailed contract schedule shall show a clear and definable critical path(s) for the Work and each specified milestone. Requirements and events which impose limitations, as well as dates and milestones which constrain the time, shall be clearly identified. Days of float time shall be shown. Items that require PBMS inputs and response shall be clearly identified.

**Updates**

The detailed schedule shall be updated every 15 days to show actual progress and changes to projected dates. Each update shall include a narrative describing the changes made since the last update. Each update shall be provided to PBMS within 5 working days from the month end cut-off date and submitted with each invoice. hardcopies and one electronic copy shall be provided.

**Four-Week Rolling Schedules**

The four-week rolling schedule shall show one week of historical information and two weeks of planned activities in support of and consistent with the detailed contract schedule.

**Format**

The four-week rolling schedule shall be presented as a chart with tasks along the left side and days along the top of the table. A shaded bar or “X” entered in the chart shall indicate work to be performed on each day for that task.

**Task Detail**

The level of detail shown on the four-week rolling schedule shall be greater than the level shown on the detailed contract schedule. In general, it shall show the Work to be done each day and the location(s) where the work will be done and by whom. Work done in buses and other vehicles shall be identifiable uniquely or as part of an easily traceable group of buses. Work that requires PBMS input or response shall be clearly identified.

**Updates**

The four-week rolling schedule shall be updated weekly and provided to PBMS by the end of the first day of the active week. Printed copies and one electronic copy shall be provided.

**o) Submittals**

**General**

This Section describes general requirements and procedures for preparing and transmitting information to PBMS for review, acceptance or approval.

**Scheduling of Submittals**

Transmit submittals sufficiently in advance of Contract requirements to permit at least Ten (10) calendar days for review, checking and appropriate response by PBMS or designated representative.

**Transmittal Forms**

Furnish the transmittal forms sequentially numbered and clearly indicate the Project Name; Project Number; Date; "To:”; "From:”; names of subservice providers, suppliers or manufacturers; required Specification references; category and type of submittal; purpose; description; distribution record (for transmittals and submittals); and signature of transmitter.

**Checking of Submittals**
Examine and check the submittal for accuracy, completeness, and compliance with the Contract before delivery to PBMS. Stamp and sign each submittal with the statement reading as follows: "Having checked this submission, we certify that it conforms to the requirements of the Contract in all respects, except as otherwise indicated". By reviewing, approving, and submitting a submittal, the Service provider has determined and verified materials, field measurements, and field implementation criteria related thereto, and has checked and coordinated the information contained within such submittals with the requirements of the work and the Contract.

Record of Submittals
Maintain at the worksite a complete up-to-date, organized file of all past and current submittals including an index and locating system, which identifies the status of each submission.

- Assign sequential numbers to each submittal.
- Assign revisions levels (A, B, C, etc.) to all re-submittals. Assign new transmittal numbers and cross references to previous submittals.

Electronic Format
All submittals shall be provided in electronic format as well as hardcopy. File formats for electronic copies shall be subject to PBMS approval. Current version, industry prevalent software shall be utilized for preparing all submittals. Drawings shall be submitted in AutoCAD format. Drawings or studies involving geographic information shall be submitted in a format that can be viewed by GIS software.

PBMS Review
PBMS and/or designated representative will review and approve or take other appropriate action upon the Service provider's submittals only for the limited purpose of checking for conformance with information given and the design concept expressed in the Contract requirements. PBMS's action will be taken as to cause no delay in the Work or in the activities of the Service provider. Review of such submittals is not conducted for the purpose of determining the accuracy and completeness of other details such as dimensions and quantities, or for substantiating instructions for installation or performance of Equipment or systems, all of which remain the responsibility of the Service provider as required by the Contract. PBMS's or designated representative's review will not constitute approval of safety precautions or, unless specifically stated by PBMS or designated representative of any construction means, methods, techniques, sequences, or procedures. PBMS's or designated representative's approval of a specific item does not indicate approval of an entire assembly of which the item is a component.

PBMS Review Stamp
All Service provider's submittals will be stamped by PBMS or designated representative with (a) the date of receipt, and (b) one of the following dispositions (see Review Stamp Exhibit hereafter), and two sets will be returned to the Service provider. (Submittals for record of the Authority will not be returned).

1. APPROVED: Work may proceed, provided it complies with the Contract. The approval of shop drawings and samples is not construed;
   a. As permitting any departure from the Contract requirements;
   b. As relieving the Service provider of responsibility for errors and omissions, including details, dimensions, and quantity of materials; or
c. As approving departures from details furnished by the Contracting Officer or designated representative.

2. APPROVED AS NOTED (Correct and resubmit): Work may proceed, provided:
   a. It complies with the Contract as well as the corrections on the submittals, and the Service provider resubmits within fifteen (7) days corrected copies of the specifications, working drawings, or miscellaneous submittals for final approval; and
   b. Work performed by the Service provider prior to receiving final approval will be at the Service provider's risk.

DISAPPROVED (Revise and Resubmit): Work not recognized as being able to proceed. Revise submittal in accordance with notations thereon, and resubmit without delay. Handle re-submittals in the same manner as first submittals, except designated with suffix A, B, C, etc. to indicate 1st, 2nd, or 3rd re-submittals. On re-submittals, direct specific attention in writing on re-submitted documents, working drawings, samples, mock-ups, sample panels, or miscellaneous submittals to revisions other than the corrections required on previous submissions. Make corrections required by PBMS or designated representative.

Actions Following Review
If APPROVED, each of the documents will be identified as having received such approval by being so stamped and dated. Documents stamped DISAPPROVED and with required corrections shown will be returned to the Service provider for correction and re-submittal. Service provider will be returned one copy of each document duly stamped, signed, and dated.

p) Drawings

Quality of Drawings
The Service provider shall be responsible for accuracy and correctness of all drawings. The Service provider's Project Manager and STSM shall initial each drawing after checking it, indicating that it complies with all requirements of this Specification and accurately reflects intended or actual field conditions.

The Service provider shall check each drawing for:
• Conformance with Contract Documents
• Logical grouping and arrangement
• Accuracy
• Legibility
• Neatness
• Line Quality
• Lettering Quality
• Reproduction Quality
• Completeness

Product Data Submittals

Quality of Submittals
A submittal shall be prepared for each major piece of material or equipment that the service provider intends to furnish. These submittals shall be known as "Product Submittals." Copies of each product submittal shall be furnished. Each submittal shall be accompanied by a cover letter with reference number, signed by the Project Manager. Each submittal shall contain a list of any parameters for which the submitted products do not meet the Specifications and a description of how these changes will affect system design. Each submittal shall contain a description of any changes in design or products that the submitted products will cause.

**Content**

Each submittal shall contain sufficient information to determine that the System Component complies with the Specifications and Agreement. Actual values of all specified parameters shall be listed; a simple statement that the product complies will not be sufficient. Each product submittal shall be accompanied by Engineering Drawings necessary to determine the product's applicability to PBMS ITM design. All closely related products shall be submitted as a single package. When pre-printed material is used in a submittal, the specific model number and options to be furnished shall be clearly identified. Standard data sheets can be used, subject to the following:

- Modify manufacturer's standard and/or schematic drawings to delete information, which is not applicable to the Contract. Supplement standard information with additional information applicable to this contract.
- Modify manufacturer's standards, diagrams, schedules, performance charts, illustrations, calculations, and other descriptive data to delete information, which is not applicable to the contract. Indicate dimensions, clearances, performance characteristics, capacities, and any other diagrams, as applicable.
- Modify installation, erection, application, and placing instructions to delete information, which is not applicable to the Contract.

**Test Procedures**

The Service provider shall submit copies of each test procedure description, accompanied by a cover letter with reference number.

**Submittal Organization**

Each test procedure description shall include the following information:

- A statement of the purpose of the tests.
- The location, date(s) and time(s) tests will be performed.
- The quantity of units to be tested.
- The test equipment to be used, identified by manufacturer and model number.
- A step by step description of the procedure to be performed.
- Specific pass/fail criteria for each test.
- A sample of the form(s) to be used to record test data. Each test form shall include the following information:
  a. Test title
  b. The manufacturer, model number and calibration date of each piece of test equipment.
c. A table to record individual readings taken and inspections performed for each unit tested, identified by the serial number of the unit tested.

d. An indication that the unit has passed or failed each individual test.

e. A line for signature of the technician performing the test and date.

f. A line for signature of the Project Manager and date.

g. A line for signature of PBMS representative witnessing the test.

h. Drawings illustrating the configuration of the Equipment tested and all test equipment utilized.

q) Test Results

**Content**

One original and copies of the results of each test shall be submitted. The original of the test results shall contain the original test forms filled out by the technician(s) performing the tests and original signatures. Test forms shall be filled out in ink and no erasures shall be made. Errors shall be crossed out with a single line and initialed by the person making the correction. Each set of test results shall be accompanied by a cover letter with reference number.

**Organization**

Each set of test results shall include the following information:

- The complete test procedures used.
- The completed, signed test forms.
- A summary of the test, indicating quantity tested, quantity that failed, quantities that failed each individual procedure, and a statement of the remedy to be applied for failed units.

r) AS-BUILT DOCUMENTATION

As-built documentation shall include drawings and software documentation. As-built documentation shall include:

- Design and Installation Plans of the On-Bus Subsystems for each Bus and Vehicle Type
- Design and Installation Plans of the BQS Subsystem
- Design and Installation Plans of the Central Control System (CCS) Subsystem
- Design and Installation Plans of the LAN and WAN
- Design and Installation Plans of the Scheduling & Dispatch Subsystem
- Design and Installation Plans of the communication Subsystem
- Design and Installation Plans of the AVLS Subsystem
- Design and Installation Plans of the Passenger Information Subsystem

**As-Built Drawings**

**Drawings Content**

As-built drawings shall provide a permanent record of the finished system. Each design document that was submitted for approval shall be modified to reflect the actual installed condition and shall become an as-built drawing. These drawings shall be supplemented with
site specific information. Where a document is typical for more than one location, the locations shall be explicitly listed on the drawing & documents:

- All nomenclature and labels shall correspond to the actual labels on installed Equipment.
- Each connection to each piece of equipment, junction box, or terminal block shall be identified by function and color code.
- All dimensions, physical details, connections, and other information pertinent to system diagnostics, maintenance or troubleshooting shall be shown.

Organization of Drawings

All drawings pertaining to a subject shall be submitted as a package with cover sheet, index, and symbols and abbreviations table. A master index of as-built drawings shall be provided that organizes the drawings by package and drawing number.

Submittal of Drawings

A pre-final version of the as-built drawings shall be submitted to PBMS prior to maintenance training and prior to acceptance testing. The Service provider shall correct any inaccuracies and add plans to correct any deficiencies as identified by PBMS or as necessary to document changes made during acceptance testing. Final versions of as-built drawings shall be submitted within two weeks after acceptance testing or maintenance training, whichever is later.

As Built Software Documentation

The Service provider shall provide all "Computer Software" and "Data" to allow PBMS to fully maintain and update all "Applications Software". "Computer Software" and "Data" shall include as-built versions of ITM:

- Software Requirements Specification;
- Software Version Description Document, or equivalent;
- All "batch" or equivalent files, and all object libraries and "include" files, for editing, compiling, linking, and installing application software. Corresponding instructions shall also be provided;
- All files required to define, allocate, and load the database, and any other data files required to define, configure, load, or operate the system. Corresponding instructions shall also be provided.

Copies of each document shall be submitted in electronic form (CD-ROM, DVD ROM or other media and in a format that is accessible by PBMS) in order for it to be incorporated into PBMS's Electronic Document Library.

The Service provider shall be required to provide source code and sufficient documentation including source code documentation in Escrow to permit modification of the delivered software without the necessity of contacting the Service provider in the event the Service provider is unwilling or unable to undertake such modifications. Proposers shall explain, in detail, the documentation to be supplied, provide samples, and guarantee of content with proposals.

5) PROJECT CLOSEOUT

Project closeout shall include an initial survey and a final survey.

Initial Survey

Pre-Requisites
Prior to requesting an initial closeout survey of ITM, the following conditions shall have been met:

- The systems acceptance test has been conducted.
- The Service provider has listed those items yet to be completed or corrected and has submitted a detailed plan of action and schedule for completion of the outstanding items.
- The Service provider has submitted special guarantees, warranties, maintenance agreements, final certifications and similar documents.
- The Service provider has obtained and submitted operating certificates, if required, final inspection and test certificates, and similar releases enabling full and unrestricted use of the work.
- The Service provider has submitted operations and maintenance manuals and final as-built documentation.
- The Service provider has delivered tools, including special tools, test equipment, standby equipment, and similar items.

**Conducting the Survey**
Up on receipt of the request for initial survey, PBMS will prepare a listing of any additional work items that are outstanding.

**Final Survey**

**Pre-Requisites**
The Service provider shall perform the Work necessary to complete and correct the items noted during the initial survey. The Service provider shall provide written notice to PBMS that the items have been completed and ITM is ready for final survey.

**Conducting the Survey**
Upon receipt of the notice, PBMS will schedule a final survey to verify that all of the Work items have been completed satisfactorily.

**t) SYSTEM DELIVERABLES**

ITM deliverables provided by the Service provider shall include all work required to deliver the System and System Components in accordance with this Specification and Agreement.

**Manuals, Training, and Training Tools**
The Service provider shall provide manuals, training, and training tools for the proper operation, maintenance, and repair of ITM equipments and applications. Delivery of the manuals, training, and training tools shall be accomplished per the Service provider-provided and PBMS-approved schedule.

**Design Submittals**
The Service provider shall provide preliminary and final design submittal packages, as well as individual design details for all elements specified herein. The Service provider shall provide detailed cut-over plans and procedures. All submittals shall be in both hardcopy and electronic format.

**As Built Documentation**
The Service provider shall provide As Built Documentation. Delivery of the As Built documentation shall be accomplished per the Service provider-provided and PBMS-approved schedule. All as-built documentation shall be provided in both hardcopy and in electronic format.

**Monthly Status Reports**

Monthly status reports shall be submitted to PBMS on the 7th of each month detailing the previous month’s progress. The monthly status report shall contain a description of the activities and accomplishments, an updated schedule showing the progress, and any issues or concerns. Service provider format is acceptable.

**Test Plans/Procedures and Test Results**

Service provider shall provide all Test Plans/Procedures required for the ITM project and the Test Results. The Test Plans/Procedures and Test Results format shall be submitted to PBMS for approval.

u) **System Support**

**Prior to System Acceptance**

Support for the maintenance and operation of installed ITM subsystems shall be provided after incremental acceptance and prior to System Acceptance. It is PBMS’s intent to begin operating ITM after completion of the first incremental acceptance.

- Support shall be provided on-site at PBMS during testing and cut-over of Equipment on a continuous basis.

- Support for in-service ITM Equipment shall be provided twenty-four hours per day, seven days per week. A request by PBMS for assistance shall be answered within SLA parameters as required by PBMS.

**Post System Acceptance**

The Service provider shall provide end-to-end support during the contract period of 5 years.

v) **QUALITY ASSURANCE**

The Service provider shall submit to PBMS within 15 days of the Notice To Proceed (NTP) or LOI a comprehensive Quality Assurance (QA) Program Plan designed to ensure the quality of all activities, including design, purchasing, inspection, handling, assembly, fabrication, testing, storage, shipping, and warranty/repair work. The plan shall describe all quality control procedures of the Service provider and any sub-suppliers. The Service provider shall conduct regular inspections in accordance with guidelines defined by the QA Program Plan. Performance of any manufacturing or construction work shall not commence until the Quality Assurance and Control Plan relating to such Work has been accepted by PBMS. The Service provider shall update the QA Program Plan as necessary, when any deficiencies in the Work are discovered.

PBMS will, at its own discretion, perform QA monitoring of work done under this Contract, including monitoring of the Service provider’s or Subservice provider’s QA activities. Upon request, the Service provider’s QA records shall be made available to PBMS for inspection. Such QA activities performed (or not performed) by PBMS shall not reduce nor alter the Service provider’s QA responsibilities or its obligation to meet the requirements of this document.
At any time during the manufacturing process, PBMS may choose to visit the Service provider’s facility or a Subservice provider’s facility during normal working hours to audit the manufacturing and quality control processes.

**w) Technical Documents**

A key component of the ITM implementation is the accuracy and value of all deliverables. The technical documents prepared by the Service provider during the course of this project will include design reports, installation drawings, test plans, test reports, progress reports, and other technical memos. A review process shall be established by the Service provider to assure all System Components are checked for accuracy, correctness, uniformity, and compliance with standards of practice.

The various tiers of the review cycle are detailed below:

- The Service provider’s Project Manager shall review project products for adherence to the standards of care common to the profession.
- The Service provider’s Project Manager shall be responsible for assigning qualified professionals to check all work products for accuracy, uniformity, and clarity. Responsibility for interface, control, and integration of disciplines into a uniform and coordinated document set is also included in this role.
- The Senior Technical Staff Member and individuals assigned as technical discipline leaders within the Service provider team shall provide another review. The reviews shall be initiated by the Project Manager and shall focus on a technical discipline review of selected project products.
- PBMS will provide a final review. This review will occur only after the Service provider’s internal review cycles have been completed. When review comments result in a change to any technical document, the Service provider’s Project Manager shall be responsible for change coordination and document back-check. In addition to the formal and ongoing quality control review, timely coordination meetings with all project staff shall be held to provide for interdisciplinary liaison and interface coordination. These meetings shall be utilized to schedule work assignments, identify and resolve coordination issues, and track progress associated with any problems encountered and their resolution.

**Document Management**

Due to the substantial amount of documentation involved in this project, Service provider shall work with PBMS’s Project Manager to develop and submit to PBMS a Documentation Management System. The Document Management System shall include an organized electronic library of all versions of all submittals and a log of the contents. This shall be completed within 30 days after Notice to Proceed. PBMS and the Service provider shall mutually agree on a documentation file index that shall provide an overall methodology for referencing documents generated in the course of the project. File type and organization of electronic versions of documentation shall be mutually agreed on by PBMS and Service provider. All subsequent documentation shall be referenced to the file index, and Service provider and PBMS shall mutually maintain the file index in current condition so as to show all documents that have been generated and their status.

Documentation in the DMS should be readily available to PBMS’s Project Manager, designated personnel within the Service provider’s organization, ITM Consultant, and PBMS-designated additional personnel. Security methods shall be available to restrict access by others.

**System Components**
The Service provider shall conduct regular inspections and audits in accordance with guidelines defined by the QA Program Plan. The Service provider’s Project Manager shall establish a quality assurance process and be responsible for assigning qualified professionals to check all system Components for compliance with the ITM Specifications and consistency in production quality. This quality assurance program shall supplement the formal testing requirements to verify that:

- Prior to installation, all System Components delivered by the Service provider shall pass rigorous screening that complies with standards of practice.
- All delivered System Components shall be tested after installation. Testing shall include hardware and software interface tests.

Manufactured Products

The Service provider shall utilize products manufactured by companies that utilize formal, documented quality assurance practices that meet or exceed the standard of care established by the industry. The Service provider shall proactively monitor each supplier’s quality system. Quality systems that conform to ISO/CMMI practices are preferred.

x) MANUALS

This section identifies the manuals to be provided to support training and give on-going documentation needed for PBMS staff to manage, maintain, and expand the ITM.

GENERAL REQUIREMENTS FOR MANUALS

Development Process

The Service provider shall prepare a complete plan for providing the manuals described herein.

The plan shall include at least the following:

- Service provider shall submit for approval the outline of each manual as a part of the Preliminary Design Review.
- Service provider shall develop and submit a draft version of each manual submitted with the Final Design Review.
- Service provider shall deliver one complete set of manuals prior to the start of the acceptance testing.
- Service provider shall incorporate information gathered during installation and acceptance testing, throughout the maintenance and warranty period into the manuals for the updated and final submittals.

Content

Manuals shall contain all of the information material required to support the area of activity.

All Manuals

All manuals shall:

- Be in concise form, with minimal redundancy.
- Be organized in clear, logical fashion, and indexed and tabbed for rapid access.
- Be in English.
- Be written for comprehension by persons with a high school education.
- Contain table of definitions for all abbreviations and special terms.
All Operations Manuals
All operations manuals shall contain:

- Instructions on navigation from one function to another.
- The meaning of all display symbols and labels.
- The meaning and interpretation of all alarms and messages, and the recommended remedial action for each alarm and message.
- A reference card defining each cursor command, control key, and status indication.

All Equipment Maintenance Manuals
All Equipment maintenance manuals shall contain:

- A section on safety procedures and precautions necessary to prevent damage to equipment, injury to personnel, and unsafe operational conditions.
- A section with an overview of the test equipment and tools necessary to troubleshoot and maintain ITM equipments.
- Wiring diagrams and physical layout drawings for all equipment
- A section addressing the intervals and procedures for all preventive maintenance including level adjustments and cleaning.

Medium and Formats for Delivery

Hardcopy
The Service provider shall deliver to PBMS the manuals for all sub-systems in hardcopy form, with appropriate binding and labeling.

- Manuals shall be designed for continuous, long-term service in a maintenance shop or vehicle environment.
- Manuals shall lie flat when opened
- Pages shall be printed on both sides.
- Manuals shall permit adding and replacing pages.
- Covers shall be oil, water, and wear resistant.

Softcopy
In addition, the Service provider shall deliver to PBMS in electronic form all manuals and manuals components that are developed by the Service provider, or by vendors in response to the requirements of this Contract.

- The electronic form shall consist of two good copies of each final manual on an electronic storage medium (CD-ROM or other approved media).
- The format of the storage medium shall be one that is widely used and easily available to PBMS.
- The manuals shall be stored as MS Word, Portable Document File, or other PBMS-approved format.

BUS OPERATORS MANUAL
The Service provider shall provide a manual for bus operators. The manual shall provide a clear and concise description of operator interface with ITM and related PBMS operating policies and procedures. It shall include:
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Overview of the ITM System
- On-Bus Subsystem Description
- How the Bus Operators are to perform all communications and bus fleet management functions provided at the Bus Driver Console.
- Procedures for wireless calls.
- Procedures for sending canned messages and receiving text messages.
- Procedures for SOS.
- Procedures for logon/logoff.
- Help guide for functional failures and problems.
- Pocket size Reference Card.

SUPERVISOR MANUAL

The Service provider shall provide a manual for supervisors. The manual shall provide a clear and concise description of supervisor interface with ITM and related PBMS operating policies and procedures. It shall include:

- Overview of the ITM System
- On-Bus Subsystem Overview
- Procedures for radio calls using mobile and portable radios.
- Procedures for sending and receiving text messages.
- How the supervisors are to perform all communications and bus fleet management functions provided at the CCS.
- Help guide for functional failures and problems

DISPATCH CENTER DISPATCHER AND SUPERVISOR MANUAL

The Service provider shall provide a manual for Dispatch Center dispatch supervisor, dispatchers, and supervisors performing dispatch duties. The manual shall provide a clear and concise description of the ITM operator interface for Dispatch Center dispatchers and supervisors for all console functions provided, including normal call, messaging, and schedule and route adherence functions. It shall include:

- ITM Overview
- On-Bus Subsystem Overview
- CAD Subsystem Description
- How the dispatchers and supervisors are to perform all communications and bus fleet management functions provided at the dispatcher consoles.
- How the Dispatch Supervisor can assign work assignments.
- How to manage work assignments, the work queue, and incident reports at their various stages.
- How to perform rudimentary remedial action for limited-scope failures, including: shutting down and restarting console processors, shutting down and restarting console-based software processes, and replacing printer paper, restarting printers, restarting printer queues.

VEHICLE COMMUNICATIONS MAINTENANCE MANUAL
The manual shall provide a logical structure and organization for the maintenance manuals provided by the manufacturers of the On-Bus subsystem communication equipment, and shall provide any necessary information to supplement them to fulfill the requirements of this section. Manuals shall include the following topics, as a minimum:

- **ITM Overview**,  
- **On-Bus Subsystem Description**  
- **Communication Subsystem Description**  
- **How to identify the source of a problem to a specific replaceable element. Provide a logical procedure for isolation a problem.**  
- **How to replace an element. Provide detailed procedure, or reference to a manufacturer manual detailed procedure, for removal and replacement of each on bus subsystem element. This shall include setting and verification of options, programming, and testing of the replaced unit and associated equipment to verify correct On-Bus subsystem operation.**  
- **Verification of correct operation of the repaired on-bus subsystem.**

**FIXED COMMUNICATIONS MAINTENANCE MANUAL**

The fixed communications and radio subsystem maintenance manual shall complement the maintenance training provided. The manual shall supplement the maintenance manuals provided by the manufacturers of the fixed radio subsystem equipment. The manual shall provide a logical structure and organization for the maintenance manuals provided by the manufacturers of the On-Bus subsystem radio equipment, and shall provide any necessary information to supplement them to fulfill the requirements of this section. Manuals shall include the following topics, as a minimum:

- **ITM Overview**  
- **Radio Subsystem Functional Description**  
- **System diagnostic procedures**  
- **Identification of the source of a problem to a specific replaceable element, provide a logical procedures for isolating a problem. Provide a description of self-diagnostic features and system administrator reports.**  
- **How to replace an element. Contain detailed procedure, or reference to a manufacturer manual detailed procedure, for removal and replacement of each fixed radio subsystem element.**  
- **Verification of correct operation of the repaired radio subsystem. Include instructions for setting and verification of options, programming, and testing of the replaced unit and associated equipment to verify correct operation.**

This requirement shall apply only if the Service provider provides the fixed data radio system.

**IN-VEHICLE EQUIPMENT MAINTENANCE MANUAL**

The manual shall focus on guiding technicians in verifying the presence of a failure and performing first echelon replacements. Manuals shall include the following topics, as a minimum:

- **ITM Overview**  
- **On-Bus Subsystem Functional Description**
• Identification of the source of a problem to a specific replaceable element, provide a logical procedures for isolating a problem. Provide a description of self-diagnostic features.

• How to replace an element. Contain detailed procedure, or reference to a manufacturer manual detailed procedure, for removal and replacement, and verification of first echelon replaceable elements.

• Verification of correct operation of the repaired On-Bus Subsystem. Include instructions for setting and verification of options, programming, and testing of the replaced unit and associated equipment to verify correct operation.

DISPATCH CENTER AND Depot WORKSTATION MAINTENANCE MANUAL

The manual shall focus on guiding technicians in identifying the source of a problem to a specific replaceable element, replacement of the element, and verification of correct operation of the repaired subsystem. Manuals shall include the following topics, as a minimum:

• ITM Overview

• CAD Subsystem Functional Description

• Depot Subsystem Functional Description

• Identification of the source of a problem to a specific replaceable element, provide a logical procedures for isolating a problem. Provide a description of self-diagnostic features and reports.

• How to replace an element. Contain detailed procedure, or reference to a manufacturer manual detailed procedure, for removal and replacement or repair of an element.

• Verification of correct operation of the repaired ITM Workstations and Dispatch Center equipment. Include instructions for setting and verification of options, programming, and testing of the repaired unit and associated equipment to verify correct operation.

COMPUTER SYSTEM ADMINISTRATOR MANUAL

The Service provider shall provide a system administrator’s manual that provides a clear, organized description of all of the configurable computers of ITM, the tools and procedures for managing their configuration, and for diagnosing their performance and problems. It shall contain at least the information described below.

y) Fleet Management Reporting

This section shall provide details on the standard reports that are automatically generated by ITM and instructions on how to perform custom queries to generate ad-hoc reports.

ITM Computer Configuration

The configuration section shall contain at least:

• A high level and detailed description of computer configurations and interfacing equipment at the Dispatch Center, bus depots, fixed communication site(s), mobile units, configuration of ITM LAN/WAN logical and physical entities, and connections to PBMS LAN/WAN.

• Description of operation of interfaces to connected systems (PBMS LAN/WAN, Vehicle Health System, depot Subsystem.)

• A listing and functional description of software components for each computer.
Configuration Management and Operation

The Configuration Management and Operation section shall contain at least:

- Procedures and tools for defining ITM users, function access and privileges, and console function assignments.
- Computer startup, interconnected systems communications restart, and shutdown procedures.
- Overview and details of procedures and tools for installing and verifying new software and rolling back old software for Dispatch Center, Computer Subsystem, Depot Subsystem, fixed communication site(s), and mobile units.
- Monitoring, maintaining, archiving, and restoring the ITM database and DMZ.
- Maintaining, updating AVLS databases.
- Procedures for modifying the Route and Stop databases.
- Procedures for importing updated route and schedule databases.
- Monitoring, analysis, and optimization of computer/LAN/WAN performance

Manual shall include procedure for configuring ITM for each separate fleet, setting access privileges for PBMS personnel and PBMS service provider personnel.

2) Diagnostics and Troubleshooting

The Diagnostics and troubleshooting section shall contain at least the following:

- Equipment and operating system error messages and diagnostics, with remedial action for each.
- Tools and procedure to troubleshoot equipment and software problems on all ITM equipment
- Procedures to manage and diagnose interfaces with connected systems.

aa) COMPUTER SOFTWARE MAINTENANCE MANUAL

The Service provider shall provide a programmer’s guide for each of the programmable computers in ITM. For each, the guide shall:

- Provide an overview of software organization.
- Define external interfacing data format, semantics, and protocols.
- Define internal modules, data interfaces, tasking, considerations for timing, priorities, and resource use.
- Provide complete source code listings.
- Identify and detail use of programming and database maintenance tools used to create the software.
- Include complete documentation of non-application components such as operating system, communications handlers, database, and report generators.
- Detail the procedures for building and managing software configuration.
- Describe the metrics embedded in ITM to evaluate its performance.
- Identify the error conditions detected within the software, and the messages or indications for those conditions.
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

- Identify parameters used to adjust ITM operation

Annexure 1:

Urban Bus Specifications – II, Ministry of Urban Development, Government of India
Refer UBS-II and subsequent addendum issued by MOUD at www.moud.gov.in
## Annexure 2:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Standard/Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety of information technology equipment, including electrical business equipment.</td>
<td>EN 60950-1:2006</td>
</tr>
<tr>
<td>Power Transformers</td>
<td>IEC 60076, EN 60076</td>
</tr>
<tr>
<td>Protection Class for Components</td>
<td>As specified for individual equipment in this document.</td>
</tr>
<tr>
<td>Surge Protective Devices</td>
<td>IEC 61643 – 1</td>
</tr>
<tr>
<td>EMC – Immunity</td>
<td>IEC 60801, EN 60801</td>
</tr>
<tr>
<td>EMC – Emission</td>
<td>VDE 0875, IEC 60555, EN 60555</td>
</tr>
<tr>
<td>Electromagnetic compatibility Testing and Measurement Techniques</td>
<td>IEC 61000-4, EN 61000-4, BS EN 50121</td>
</tr>
<tr>
<td>RFI Suppression</td>
<td>EN55022A or VDE 0878</td>
</tr>
<tr>
<td>Level measuring systems utilizing ionising radiation with continuous or switching output</td>
<td>IEC 60982</td>
</tr>
<tr>
<td>Sound Level of Noise Source</td>
<td>ISO 3746, BS 4196–6</td>
</tr>
<tr>
<td>Flammability Tests</td>
<td>IEC 60707</td>
</tr>
<tr>
<td>Valve Regulated Sealed Lead Acid Rechargeable Single Cells</td>
<td>IRS: S93-96, DOT: TQS10G 92</td>
</tr>
<tr>
<td>Low-voltage Switchgear and Control gear Assemblies</td>
<td>IEC 60439 – 1, EN 60439–1</td>
</tr>
<tr>
<td>Low-voltage Switchgear and Control gear</td>
<td>IEC 60947, EN 60947, IEC947-3, IEC 60898 or EN 60898</td>
</tr>
<tr>
<td>Specification for contactors</td>
<td>IEC60947 – 4, EN 60947-4</td>
</tr>
<tr>
<td>Code of practice for Earthing</td>
<td>IEEE1100, NFPA 780, IEC1024</td>
</tr>
<tr>
<td>Transient Protection</td>
<td>MIL-STD-7041A</td>
</tr>
<tr>
<td>Lightning Protection</td>
<td>BS-6651</td>
</tr>
<tr>
<td>Quality</td>
<td>ISO9001</td>
</tr>
</tbody>
</table>
### ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

<table>
<thead>
<tr>
<th>Specification</th>
<th>BS EN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification for Safety of Information technology equipment including electrical business equipment.</td>
<td>60950-1:2006</td>
</tr>
<tr>
<td>Electromagnetic Compatibility (EMC) : Generic standards immunity for Industry environments.</td>
<td>61326 (Annex A)</td>
</tr>
<tr>
<td>Specification for safety requirements for equipment to be connected to telecommunication networks.</td>
<td>41003:1999</td>
</tr>
<tr>
<td>Safety requirements for electrical equipment for measurement, control &amp; laboratory use. Part 1: General requirements.</td>
<td>61010-1:2003/A2:1995</td>
</tr>
<tr>
<td>Secondary protectors for Communication Circuits.</td>
<td>Underwriters Laboratory safety std 497A</td>
</tr>
</tbody>
</table>
Annexure 3:

A. Service Level Agreement

1. Management of Services/General principles

Definitions

In this Agreement, unless the context otherwise requires:

“Account Manager” means the IT ITMS Service Provider employee designated by ITMS Service Provider to deal with the Customer’s account as notified from time to time to the Customer;

“Call Close Time” means in respect of any Fault the time at which that Fault is cleared and notified to the Customer

“Call Open Time” means the date and time which is recorded by the ITMS Service Provider Representative as the time the Fault Call is logged;

“Customer” means an artificial person created under the law(PBMS) whose order for Services is accepted by ITMS Service Provider in accordance with the Terms of Service Provider Agreement;

“Customer Components” means such of the Components as are delivered to the Customer;

“Customer Representative” means the individual nominated by the Customer from time to time to represent the Customer in all matters relating to the Customer’s and the End User’s use of the Services;

“ITMS Service Provider Representative” means any employee of ITMS Service Provider or its sub-contractors nominated by ITMS Service Provider from time to time to be responsible, in liaison with the Customer Representative, for delivering the Services;

“Fault” means any recorded failure of any part(s) of the Services;

“Fault Call” means any telephone call, fax or e-mail from the Customer to the ITMS Service Provider Representative;
“Fault Duration” means the length of time between the Call Open Time and the Call Close Time for a Fault or, if any Fault is re-opened after the Call Close Time, the length of time between the Call Open Time and the final Call Close Time;

“Hours of Cover” means the hours of cover specified in Appendix A below;

“Response Time” means the length of time between the Call Open Time and the time at which an engineer arrives at the Customer’s premises or any other premises agreed between the parties with the aim of restoring the normal operations of the services to the customer including rectifying any Fault;

“Service(s)” means the service(s) provided by ITMS Service Provider

“Time to Restore” means the target time to restore specified for each Component;

“Technical Helpdesk” means those ITMS Service Provider Representatives available to respond to Customers’ requests for assistance from time to time;

“Terms of Business” means ITMS Service Provider’s standard terms and conditions in force from time to time.

2. **Scope**

This SLA describes the target performance levels which ITMS Service Provider shall aim to deliver for the Services, ITMS Service Provider’s procedures for managing unavailability of the Services, and the penalties which will be applied if ITMS Service Provider fails to deliver any service performance targets in accordance with this Agreement.

3. **Targets and availability**

Because of the varying nature of the Components each Component has an individual target set for performance and availability. However PBMS expects ITMS Service Provider to guarantee 99.5% availability of the Services.

4. **Service monitoring**

ITMS Service Provider will put in place a monitoring mechanism to monitor all Components of ITMS. ITMS Service Provider through its monitoring system should provide data which is sufficient to allow analysis and reporting of Component performance and availability to the detail and frequency described in this Agreement.
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

ITMS Service Provider will additionally use data gathered from its monitoring of the Components to inform & take approval from competent authority its decisions in respect of any changes to its infrastructure which it, in its sole discretion, deems necessary to maintain or improve the availability and performance of the services delivered to PBMS.

5. Performance reporting

ITMS Service Provider shall record performance and availability of each of the Customer Components and report this information to the Customer, as described in Appendix B. Where periodic account reviews are agreed by Both parties to be held between the Customer and ITMS Service Provider, these reports will form an agenda for such reviews. If the Customer Components include access to ITMS Service Provider’s service system, ITMS Service Provider will enable the Customer to view the reports via ITMS Service Provider’s service system.

6. Complaints procedure

If the Customer has any complaints about the way in which ITMS Service Provider’s support facilities are being managed, the Customer Representative shall initially contact ITMS Service Provider, in writing.

7. Non-delivery of Services

Planned suspension

ITMS Service Provider will, on occasion, need to suspend part(s) of the Services in accordance with the Terms of Business. In such cases, the unavailability of any part(s) of the Services will not constitute a Fault. Where practical, any such suspension will be arranged to fall outside the Customer’s normal working hours and ITMS Service Provider shall use its reasonable commercial endeavours to see that the following procedure is followed:

ITMS Service Provider should by e-mail or other means give the Customer Representative reasonable notice of the time and duration of the suspension;

After completion of the planned work, ITMS Service Provider will report the outcome to the Customer Representative by updating the call management system on ITMS Service Provider’s website; and

All work at the premises of Customers or End Users will be carried out in accordance with Both local and national health and safety regulations.

8. Service failures

Any Faults arising from failures of components which are not Customer Components or failure of any End Users’ system (for instance, the failure of a local telecommunications
9. **Managing Service failure**

**Fault Calls**

**Notification of faults**

The PBMS Representative will report a Fault during the Hours of Cover by notifying ITMS Service Provider’s Technical Helpdesk by telephone, fax or email or Service System.

**Setting Fault priority**

The priority of a Fault reported by the PBMS will be categorised by agreement between the PBMS and the ITMS Service Provider Representative taking the relevant Fault Call. In the absence of agreement PBMS will determine the Fault priority. Faults will generally be categorised as follows:

**Table 1**

Severity Definition Chart

<table>
<thead>
<tr>
<th>Support Category</th>
<th>Criteria</th>
<th>Resolution</th>
<th>Maximum Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>The system is unable to be used for normal business activities. There is certainty of financial loss to PBMS.</td>
<td>90 Minutes Escalated after this period to – Stage 2 Escalated after 2 hour (cumulative) to - Stage 3 Escalated after 3 hours (cumulative) to - Stage 4</td>
<td>15 Minutes</td>
</tr>
<tr>
<td>Urgent</td>
<td>There is a problem with part of the system, which impacts on PBMS’s decision making. No viable Work around is available. There is a likelihood of financial loss.</td>
<td>3 Hours Escalated after this period to - Stage 2 Escalated after 4 hours (cumulative) to - Stage 3 Escalated after 5 hours (cumulative) to - Stage 4</td>
<td>1 Hour</td>
</tr>
<tr>
<td>High</td>
<td>The efficiency of users is being impacted, but has a viable workaround.</td>
<td>6 hours Escalated after this period to - Stage 2 Escalated after 8 hours</td>
<td>2 Hours</td>
</tr>
</tbody>
</table>
### ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
<th>Escalation Times</th>
<th>Response Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>A low impact problem that affects the efficiency of users but has a simple workaround</td>
<td>Escalated after 9 hours (cumulative) to Stage 3</td>
<td>12 Hours Escalated after this period to Stage 2</td>
</tr>
<tr>
<td>Low</td>
<td>A fault, which has no particular impact on processing of normal business activities.</td>
<td>Escalated after 14 hours (cumulative) to Stage 3</td>
<td>Escalated after 16 hours (cumulative) to Stage 4</td>
</tr>
</tbody>
</table>

### Recording the Fault

The ITMS Service Provider Representative will ask PBMS Representative for information about the Fault to obtain a clear description of its nature and the circumstances in which it occurred and confirm eligibility or non-eligibility of support for the Fault.

**Faults initially reported by ITMS Service Provider**

### Notification of Faults

ITMS Service Provider will notify the Customer Representative, either by e-mail, fax, telephone or other method, within a reasonable period of time of any Fault of which it is aware, unless that Fault is cleared before it can be notified to the Customer Representative.

### Setting the Fault priority

ITMS Service Provider will allocate a priority to any Fault notified by the Customer Representative in accordance with the Fault designations set out in Table 1 above. The Customer should notify ITMS Service Provider’s Customer Services Manager by telephone if it disagrees with the allocated priority.

### Recording the Fault report

ITMS Service Provider will record the date and time at which ITMS Service Provider notifies...
10. **Fault rectification**

**Fault handling and escalation**

ITMS Service Provider will allocate to any Fault a Response Time in accordance with the details set out in Table 2 below. Faults which remain unresolved at the end of the Response Time will be escalated as shown in Table 2. Descriptions of the activities associated with each stage are shown in Table 3.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Response Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 1</td>
<td>The ITMS Service Provider Representative on the Technical Helpdesk will acknowledge the Fault Call and advice on tests and actions required in order to resolve the problem, consulting as necessary with other ITMS Service Provider Representatives and third parties. Should the ITMS Service Provider Representative be unable to resolve the problem or provide an action plan suitable to the Customer, the Fault Call will be escalated to ITMS Service Provider’s Operations Team and ITMS Service Provider’s Account Manager will also be informed.</td>
</tr>
<tr>
<td>Stage 2</td>
<td>ITMS Service Provider’s Operations Team will determine a suitable action plan and agree it with the Customer. Where appointed, the Account Manager will be notified. ITMS Service Provider’s Implementation Team may also be involved at this point and third party manufacturers and/or ITMS Service Providers may be contacted for additional technical support.</td>
</tr>
<tr>
<td>Stage 3</td>
<td>If unresolved following Stage 2, the Fault will be escalated to ITMS Service Provider’s Customer Services or Operations Managers, as appropriate. They will involve all necessary resources, both internally and externally, to ensure an acceptable resolution for the Customer. ITMS Service Provider’s Technical Services Director will also be informed.</td>
</tr>
<tr>
<td>Stage 4</td>
<td>If unresolved following Stage 3, then ITMS Service Provider’s Technical Services Director will take responsibility for the call and involve all necessary senior and management resources, both internally and externally, to ensure an acceptable resolution for the Customer. ITMS Service Provider’s Managing Director will be appraised of the situation.</td>
</tr>
</tbody>
</table>

Response Times will start to run at the Call Open Time. The ITMS Service Provider Representative may amend any Fault priority by agreement with the Customer. All telephone calls may be recorded or monitored for training purposes.

Should the same Fault re-occur within 48 hours, the original call will be reopened with the same log number and the same Response Time will apply from the time that the call is re-opened.
ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

ITMS Service Provider reserve the right to ‘stop the clock’ should a third party ITMS Service Provider be unable for any reason to issue or release pertinent details or information.

11. **Progress recording**

**Mechanism for notification of progress, escalations and resolution**

Appendix A sets out how ITMS Service Provider will notify the Customer Representative about Fault progress, escalation and/or resolution. In the event that the Customer Representative cannot be contacted by one of the methods set out in Appendix A, the ITMS Service Provider Representative shall be entitled to use any other method that it deems appropriate for any such notification.

In respect of any priority one Fault, the Customer Representative will, upon request, be updated with regular progress reports during the Hours of Cover. Such progress reports, where issued, will not be produced more frequently than hourly.

12. **General Assistance**

ITMS Service Provider will aim to provide assistance to the Customer in the resolution of difficult “end-to-end” Faults. This will include incidents where the location of a particular Fault is unclear, and may not eventually lie in ITMS Service Provider’s area of supply. Such incidents may require the active co-operation of ITMS Service Provider, the Customer and third parties, in order to undertake the tests necessary for successful Fault isolation and resolution. ITMS Service Provider reserves the right to charge for time and materials where the Fault does not lie within the Service boundaries described in, Appendix B.

13. **Closing a Fault**

Any Fault will remain open until the Call Close Time is notified to the Customer.

In the event that the Customer reports that a Customer Component remains out of operation after the Call Close Time has been noted, then the Fault will be re-opened.

14. **Guaranteeing a Fault Duration Time**

Although ITMS Service Provider will use its reasonable commercial endeavours to clear any Fault within the shortest possible time, the Customer should be aware that it is impossible for ITMS Service Provider to guarantee any time limits.
15. **Recurring and intermittent faults**

ITMS Service Provider will use its reasonable commercial endeavours to record the cause of all Faults and monitor them to try and isolate recurring or intermittent Faults.

ITMS Service Providers Representative may request certain Fault details from the Customer in order to rectify a recurring or intermittent Fault. The Customer may be asked to record certain information relating to recurring or intermittent Faults; the Customer must comply with any such request.

A Fault may be closed by ITMS Service Provider if it is found to be and recorded as “no fault found” or “right when tested,” even if an investigation is ongoing to isolate a recurring or intermittent fault.

**Chart 1: Escalation**

**Escalation Procedure Flow Chart**
Stage 1

Vendor

Technical Helpdesk
Service Level Acceptance (SLA) Matrix and Proposed Penalty Amount for Default/s

a) **Minimum Service levels to be maintained for ITMS system operations by the ITMS Service Provider.**

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Service Parameter</th>
<th>Service Level</th>
<th>Validation</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Project Management Submission of monthly Project Status reports &amp; Conducting Status meetings</td>
<td>100%</td>
<td>Minutes of Meetings Approval of Status reports by Project in-Charge</td>
<td>2% of monthly CCS charges for every default</td>
</tr>
<tr>
<td>2</td>
<td>Helpdesk Resolution of ticket logged as per the Severity definition chart</td>
<td>99%</td>
<td>Generated from Ticket logging system. Measured monthly</td>
<td>95%-99% calls resolved in specified time: 2% penalty on the monthly charges 90% - 95% calls resolved in specified time: 5% penalty on the monthly charges Less than 90%, will form the basis of liquidity damages and may lead to termination</td>
</tr>
<tr>
<td>3</td>
<td>Installation Should be part of Monthly project status report</td>
<td>95%</td>
<td>Report. Installation is not as per agreed installation plan. Deviation in plan because of delay from the service provider side.</td>
<td>For delay between 7 to 30 days INR 2000 per day per station delay. For more than 30 days delay : will form the basis of liquidity damages and may lead to termination</td>
</tr>
<tr>
<td>4</td>
<td>Asset / Inventory Management Provide monthly MIS Asset Inventory</td>
<td>95%</td>
<td>Report. Inventory not maintained to provide agreed service levels</td>
<td>0.2% of monthly charges</td>
</tr>
<tr>
<td></td>
<td>Conduct Annual Physical Asset</td>
<td>100%</td>
<td>Management approval of Physical Asset Verification</td>
<td>0.5% of Yearly Charges</td>
</tr>
<tr>
<td></td>
<td>Verification</td>
<td>Report</td>
<td>1% of monthly charges till 99.9%, 3 % of Monthly Charges till 99% and 5% of monthly charges till 98%</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ITMS Application</td>
<td>Evaluation of ITMS Service Provider Performance On monthly basis</td>
<td>Low performance – 99% to 99.98% of monthly Operations time Critical Less than 98% of monthly Operations time Less than 98% : will form the basis of liquidity damages and may lead to termination</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>99.98%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Desk Side Technical support Services</td>
<td>Resolution of ticket logged as per the Severity definition chart</td>
<td>Agreed report submission to client as per fixed schedule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>95%</td>
<td>0.2% of monthly charges</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Antivirus Management</td>
<td>Rollout of latest anti-virus definition file On workstations and Servers on being made available on AFCS Service Provider's website</td>
<td>Reports generated from Anti -Virus software console</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>98%</td>
<td>1% of monthly charges</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>LAN &amp; local computer administration</td>
<td>Resolution of ticket logged</td>
<td>Reports generated from Ticket logging system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>99%</td>
<td>For down time more than 99% of the operations time penalty calculation : Number of Activities / Items identified X Penalty amount X Number of Hours</td>
<td></td>
</tr>
</tbody>
</table>

MIS reporting on during Contract Period 95% Agreed report submission to client as per fixed schedule 0.2% of monthly charges

Desk Side Technical support Services Resolution of ticket logged as per the Severity definition chart 95% Reports 1% of monthly charges

Antivirus Management Rollout of latest anti-virus definition file On workstations and Servers on being made available on AFCS Service Provider's website 98% Reports generated from Anti -Virus software console 1% of monthly charges

LAN & local computer administration Resolution of ticket logged 99% Reports generated from Ticket logging system For down time more than 99% of the operations time penalty calculation : Number of Activities / Items identified X Penalty amount X Number of Hours
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 7 | Network Monitoring, Management and Restoring (Connectivity between DC and station, DC and fleet) in a month | SP to monitor the availability of the network link for 99% uptime. SI should measure link availability on a monthly basis. | 99% | Downtime reports
Reports on the network Performance

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
|  |  |  | downtime
Penalty Amount INR 200 per activity per hour|
|  |  |  |  |
|  |  |  | At a stretch in a day network cannot be down for more than 2 hours. Service provider to ensure data is stored locally while the network is down and uploaded as soon as network is up.
DC to Station: After 2 hours, Penalty of 2% of monthly charges per incident per hour up to 4 hours
DC to fleet: After 2 hours, Penalty of 1% of monthly charges per incident per hour up to 4 hours
More than 4 hours of connectivity failure for more than 5 times a month may lead to termination|
<p>| | | | |
|  |  |  |  |
|  |  |  | 99% |
|  |  |  | Reports generated from Ticket logging system|
|  |  |  | 0.2% of monthly charges|
|  |  |  |  |
| 8 | Data Centre Operations | Resolution of ticket logged related to Networks | 99% |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |</p>
<table>
<thead>
<tr>
<th>Controls</th>
<th>95%</th>
<th>Report</th>
<th>0.2 % of monthly charges</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIS reporting of health check-up of all systems &amp; modules installed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Server Administration / Management</td>
<td>98%</td>
<td>Patch update report</td>
<td>0.5% of monthly charges</td>
</tr>
<tr>
<td>Rollout of patches (OS, infra level) on Workstations and Servers after patch being approved on test environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uptime of DMZ servers</td>
<td>99.8%</td>
<td>Report</td>
<td>2% of monthly charges for less than 99.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3% of monthly charges for less than 98%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 % of monthly charges for less than 95%</td>
</tr>
<tr>
<td>10 Database Administration services</td>
<td>99%</td>
<td>Report</td>
<td>0.5% of monthly charges</td>
</tr>
<tr>
<td>MIS report of database scheme, disk space, storage and user role</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Backup/Restore Management</td>
<td>99%</td>
<td>Report</td>
<td>If the negligence is found in monthly audit, the Bidder would be penalized a sum of INR 5,000/- per negligence.</td>
</tr>
<tr>
<td>PBMS would periodically (once a quarter on a random day) request the Service Provider to restore the backup data</td>
<td>100%</td>
<td>Report</td>
<td>INR 5000/- for every restore test failure</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Mail / Messaging System</td>
<td>Uptime of email server</td>
<td>99%</td>
<td>Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide monthly MIS of user account and mailboxes created/delete d.</td>
<td>95%</td>
<td>Report</td>
</tr>
<tr>
<td>Management of PBMS’s EMS (Enterprise Management System)</td>
<td>Daily MIS of server and device health check-up (CPU, disk space, Memory utilization, I/O utilization, Central Storage etc.)</td>
<td>100%</td>
<td>100% Reports generated from EMS system</td>
</tr>
<tr>
<td>Incident management</td>
<td>Resolution of ticket logged in Incident Management tool</td>
<td>99%</td>
<td>Reports generated from Ticket logging system</td>
</tr>
<tr>
<td>Problem</td>
<td>Service Provider shall</td>
<td>100%</td>
<td>Root cause report</td>
</tr>
</tbody>
</table>
### ITMS Technical Specifications for Amritsar BRT

<table>
<thead>
<tr>
<th>Managemen t</th>
<th>Analyse all the incidents and provide a root cause report every month if there are more than 10 incidents of the same type. Service Provider shall take the needed corrective action to prevent further issues due to the same cause.</th>
<th>timely Submission covering all Incidents logged in that month</th>
<th>Incident report stating Problems faced by the users Document detailing Corrective action</th>
<th>Area, if the Service Provider does not submit a problem report for that month. 5% penalty on the monthly charges of that Project Area, if the Service Provider does not perform the corrective action for more than one calendar month.</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Change Management</td>
<td>Resolution of Change Management ticket logged in Change Management tool</td>
<td>99%</td>
<td>Reports generated from Change Management System</td>
</tr>
<tr>
<td>17</td>
<td>Availability Management</td>
<td>Should be part of Monthly status report</td>
<td>95%</td>
<td>Report</td>
</tr>
<tr>
<td>18</td>
<td>Performance Management</td>
<td>Should be part of Monthly status report</td>
<td>95%</td>
<td>Report</td>
</tr>
<tr>
<td>19</td>
<td>Capacity management</td>
<td>Should be part of Monthly status report</td>
<td>95%</td>
<td>Report</td>
</tr>
<tr>
<td>20</td>
<td>Security</td>
<td>Should be part</td>
<td>95%</td>
<td>Report</td>
</tr>
</tbody>
</table>
## ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

<table>
<thead>
<tr>
<th>Managemen t</th>
<th>of Monthly status report</th>
<th>21 Resource Management</th>
<th>Number of shift days for which resource present at the designated location / Total number of shift days</th>
<th>98% Averaged over all Resources designated for SP services – calculated on a monthly basis</th>
<th>Attendance track Call Log Audit calls/ visits Measured on a monthly basis</th>
<th>If the resource availability is less than 95%, then payment shall be deducted based on the pro-rata basis. (Total cost per day divided by nos. of persons deployed) Further deduction INR2,000/- per day per resource/shall also be made on account of loss of service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource provided is not as per specified certification / experiences</td>
<td>100% of the Resource given</td>
<td>Experience certificate of personnel submitted by Service Provider to PBMS</td>
<td>Per day deduction = 0.5 * (Monthly value for that manpower as per SOR) / 30</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Additional Service Levels for critical modules:

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Module</th>
<th>Service Level Description</th>
<th>Measurin g Duration</th>
<th>Measurement</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Minimum</td>
<td>Lower Performance</td>
</tr>
<tr>
<td>1</td>
<td>PIS</td>
<td>Bus Station Display Availability</td>
<td>Daily</td>
<td>98%</td>
<td>98% to 95%</td>
</tr>
<tr>
<td>2</td>
<td>PIS</td>
<td>Replacement of Faulty Displays</td>
<td>Daily</td>
<td>1 Day</td>
<td>2 day</td>
</tr>
</tbody>
</table>
### ITMS TECHNICAL SPECIFICATIONS FOR AMRITSAR BRT

<table>
<thead>
<tr>
<th></th>
<th>Data Centre</th>
<th>CPU utilization must not cross beyond % at any time of processing</th>
<th>Monthly</th>
<th>75%</th>
<th>76% to 80%</th>
<th>&lt; 80%</th>
<th>More than 80% utilization shall be mutually agreed and any failure of system shall lead agreed penalties</th>
</tr>
</thead>
</table>
| 4 | Servers uptime | Monthly                                                      | 100%   | 99.99% | 99.98% | 99.9 % > Availability >= 99.5% : INR 1,00,000/- from monthly payment  
|   |              |                                                              |        |       |           |       | b. 99.5 % > Availability > =98%: INR 1,50,000/- from monthly payment  
|   |              |                                                              |        |       |           |       | c. Availability < 98%: INR 2,00,000/- from monthly payment |
| 5 | Website uptime with all the features | Monthly | 99% | 99% to 98% | <98% | Below 98% , Penalty INR 500 per incident per hour unavailability |

16. **Uptime Calculation for the month:**

\[ \left\{ \frac{\text{Actual Uptime} + \text{Scheduled Downtime}}{\text{Total No. of Hours in a Month}} \right\} \times 100 \]

"Actual Uptime" means, of the Total Hours, the aggregate number of hours in any month during which each equipment is actually available for use.

"Scheduled Downtime" means the aggregate number of hours in any month during which each equipment, is down during total Hours, due to preventive maintenance, scheduled maintenance, infrastructure problems or any other situation which is not attributable to Service Provider’s (or Service provider’s) failure to exercise due care in performing Service Provider’s responsibilities.
The PBMS would provide a maximum of 04 hours of planned downtime for the preventive maintenance (as part of scheduled downtime) per month per equipment/service.

The downtime for scheduled maintenance (patch application, upgrades – OS, Database, etc.) would need to be mutually agreed between PBMS and the Bidder. To reduce this time, various maintenance activities can be clubbed together with proper planning.

"Total Hours" means the total hours over the measurement period i.e. one month (24 * number of days in the month).

**Downtime Calculation:**

The recording of downtime shall commence at the time of registering the call with Service Provider or Service Provider for any downtime situation for the equipment.

Downtime shall end when the problem is rectified and the application/service is available to the user.

Down time will not be considered for following:

1. Pre-scheduled preventive maintenance and health checks (Scheduled Downtime).
2. Failover time (30 minutes) in case of cluster environment. Beyond which the service would be considered to be not available and appropriate penalty shall be imposed on the Service Provider.
3. Bug in any application which causes the non-availability of the service.

If the PBMS elects to continue the operation of the machine/equipment, when a part of the machine is giving problem and leading to downtime, the commencement of downtime shall be deferred until the PBMS releases the machine/equipment to the Bidder for remedial action.

a) The compliance report shall be submitted monthly, by the ITMS Service Provider.

b) These compliance reports shall be verified by PBMS officials or the nominated representatives of PBMS. Any disputes on the compliance report shall be escalated to a nominee of the senior management of PBMS and the decision of that nominee shall be binding on both the parties.

c) Elaborate list of SLA shall be furnished to successful bidder at the time of agreement stage.

d) The compliance to the SLA metrics as listed above shall be monitored on the monthly basis.

e) If PBMS finds that ITMS Service Provider has breached any of the SLA Metrics more than three (3) times in a year then PBMS, in its sole discretion, may terminate the Agreement in accordance with the provisions thereof. Such termination of the Agreement shall be without prejudice to any other rights available to PBMS.

f) The compliance report shall be submitted along with the Monthly invoice by the ITMS Service Provider.
g) These compliance reports shall be verified by PBMS officials or the nominated representatives of PBMS. Any disputes on the compliance report shall be escalated to a nominee of the senior management of PBMS and the decision of that nominee shall be binding on both the parties.

17. **Breach of SLA**

In case the Service Provider does not meet the service levels mentioned in document, for three (3) continuous time-periods as specified in the relevant clause, the PBMS will treat it as a case of breach of Service Level Agreement. The following steps will be taken in such a case:-

1. PBMS issues a show cause notice to the Service Provider.
2. Service Provider should reply to the notice within three working days.
3. If the PBMS authorities are not satisfied with the reply, the PBMS will initiate termination process.

18. **Exclusions**

The Service Provider will be exempted from any delays or slippages on SLA parameters arising out of following reasons:-

Delay in execution due to delay (in approval, review etc) from PBMS’s side. Any such delays will be notified in written to the IT Team.

The network links if provided by a third party, in that case the Service Provider will monitor and report any problems on behalf of third party. If Service Provider notifies and PBMS approves that the delay or fault was due to the third party link services then such loss will not be considered for tracking Service Provider’s SLA parameters (Also reduced from total service time).

19. **Monitoring and Auditing**

IT Team of PBMS will review the performance of Service Provider against the SLA parameters each month, or at any periodicity defined in the contract document. The review / audit report will form basis of any action relating to imposing penalty or breach of contract. Any such review / audit can be scheduled or unscheduled. The results will be shared with the Service Provider as soon as possible. PBMS reserves the right to appoint a third-party auditor to validate the SLA.
20. **Reporting Procedures**

The Service Provider’s representative will prepare and distribute SLA performance reports in an agreed upon format by the 10th working day of subsequent month of the reporting period. The reports will include “actual versus target” SLA performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports will be distributed to the PBMS’s IT Team.

21. **Issue Management Procedures**

**General**

This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between PBMS and Service Provider. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.

**Issue Management Process**

Either PBMS or Service Provider may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

PBMS and the Service Provider’s representative will determine which committee or executive level should logically be involved in resolution.

A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.

Management of PBMS and Service Provider will develop a temporary, if needed, and the permanent solution for the problem at hand. The Service Provider will then communicate the resolution to all interested parties.

22. **SLA Change Control**

**General**

It is acknowledged that this SLA may change as PBMS’s business needs evolve over the course of the contract period. As such, this document also defines the following management procedures:

1. A process for negotiating changes to the SLA.

2. An issue management process for documenting and resolving particularly difficult issues.
3 PBMS and Service Provider management escalation process to be used in the event that an issue is not being resolved in a timely manner.

Any changes to the levels of service provided during the term of this agreement will be requested, documented and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this document and consequently the contract.

**SLA Change Process**

Both the parties may amend this SLA by mutual agreement in accordance. Changes can be proposed by either party. Normally the forum for negotiating SLA changes will be PBMS’s monthly review meetings.

**Version Control**

All negotiated SLA changes will require changing the version control number. As appropriate, minor changes may be accumulated for periodic release (e.g. every quarter) or for release when a critical threshold of change has occurred.

**Management Escalation Procedures**

The purpose of this escalation process is to provide a quick and orderly method of notifying both parties that an issue is not being successfully resolved at the lowest possible management level. Implementing this procedure ensures that PBMS and Service Provider management are communicating at the appropriate levels. Escalation should take place on an exception basis and only if successful issue resolution cannot be achieved in a reasonable time frame.

1. All issues would be raised to the project management team, which is completely responsible for the day to day aspects of the implementation. The project management team shall classify the issues based on their severity level and resolve them within appropriate timelines.

2. If project management team is unable to resolve an issue, the issue would be escalated to the top management with options/ risks detailed for decision. Top management will make decisions based on the options/ risks presented by the IT team.

**Service levels of AVLS and PIS**

**System Availability**

The System could be required to be functional round the clock, and the availability of the System should be in excess of 99.50% of the operations time, shall be calculated monthly basis. Any other service level metrics, as might be appropriately required, would be finalized during the contract signing stage.
Service monitoring

a) AFCS Service Provider will put in place a monitoring mechanism to monitor all Components. AFCS Service Provider through its monitoring System should provide data Which is sufficient to allow analysis and reporting of Component performance and Availability to the detail and frequency described in these Conditions.

b) AFCS Service Provider will additionally use data gathered from its monitoring of the Components to inform & take approval from competent authority for its decisions in respect of any changes to its infrastructure which in its sole discretion, deems necessary to maintain or improve the availability and performance of the services delivered to Authority.

Performance reporting

a) AFCS Service Provider shall record performance and availability of each of the Customer Components and report this information to the Customer. Where periodic account reviews are agreed by both parties to be held between the Customer and AFCS Service Provider, these reports will form an agenda for such reviews. If the Customer Components include access to AFCS Service Provider’s service System, AFCS Service Provider will enable the Customer to view the reports via AFCS Service Provider’s service system.

Complaints procedure

a) If the Customer has any complaints about the way in which AFCS Service Provider support facilities are being managed, the Customer Representative should contact the AFCS Service Provider.

General Maintenance Conditions:

a) The maintenance shall include both Preventive Maintenance and Corrective Maintenance.

b) This Service Level Conditions shall cover each and every part/component of the System. The AFCS Service Provider shall examine, clean, lubricate and adjust various Components /parts of the entire System including all parts and components every month and shall take necessary measures to maintain the units in proper working conditions in accordance with the Specifications in the Service Level Conditions.

c) The AFCS Service Provider shall supply and replace any part/components which are discovered to be potentially detrimental to the safety of the user and/or to the efficient and cost effective operation of the units and which require immediate replacement.

d) In case of need to replace any part/component, the AFCS Service Provider shall provide original make genuine parts/components of similar/higher quality.

e) In case of emergencies, the AFCS Service Provider shall respond immediately to take the necessary actions irrespective of the provisions regarding time limit in these SLCs.

f) The AFCS Service Provider shall be liable for any kind of damage to the user of the units caused by poor maintenance, delay in any repair/maintenance works and shall pay for the damage.

g) Repairs may be carried out generally during non-operational hours.
Nature of Distress, Remedy Periods and Damages payable for Breach

The AFCS Service Provider shall during both the warranty period and the Operation & Maintenance period attain following standards of remedy for each nature of distress specified for flap gates. In the event of the AFCS Service Provider not being able to deliver the services, damages shall be payable by the AFCS Service Provider against default in service as shown as follows.

In addition to the above, for any non-availability of the System below 99% of total operations time in hours, damages shall be recoverable separately on a pro rata basis per every hour of non-operations below 99%.

25. Training Requirements

Training is an important activity for the successful implementation of Work. To make the Work a success, the following training programs shall be arranged by the ITMS Service Provider from time to time depending on the requirement and understanding of the service centre operators, participating users, etc. For all these training programs, ITMS Service Provider shall provide adequate course material documents. The following are the trainings to be imparted by the ITMS Service Provider:

- ITMS Service Provider shall impart training to Authority nominated trainer staff, so that they are aware of the operations of the solution and further impart training to the relevant staff of Authority ensuring smooth running of System at the selected sites.

- ITMS Service Provider shall also be responsible for re-training the Authority nominated trainers staff whenever changes are made in the System and it shall be the responsibility of the ITMS Service Provider to ensure that the operators are familiar with new versions of system and its allied services.