

Request for Proposal

Selection of System Integrator for Implementation of e-Governance in Urban Local Bodies and Department of Local Government, Punjab

Volume I: Functional, Technical and Operational Requirements



**Department of Local Government
Punjab**

July 2017



Disclaimer

- This RFP is not an agreement and is neither an offer nor invitation by the Purchaser to the prospective Bidders or any other person. The purpose of this RFP is to provide interested Parties with information that may be useful to them in the formulation of their Proposals pursuant to this RFP.
- This RFP includes statements, which reflect various assumptions and assessments arrived at by the Purchaser in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require.
- This RFP may not be appropriate for all persons, and it is not possible for the Purchaser, its Employees or Advisers to consider the objectives, technical expertise and particular needs of each Party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct their own investigations and analysis and should check the accuracy, reliability and completeness of assumptions, assessments and information contained in this RFP and obtain independent advice from appropriate sources.
- Information provided in this RFP to the Bidders is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The Purchaser accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on the law expressed herein.
- The Purchaser, its Employees and Advisers make no representation or warranty and shall have no liability to any person including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or arising in any way by participating in this Bid process or otherwise, including accuracy, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this selection process.
- The Purchaser also accepts no liability of any nature whether resulting from negligence or otherwise however caused arising from reliance of any Bidder upon the statements contained in this RFP.
- The Purchaser may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumption contained in this RFP.
- The issue of this RFP does not imply that the Purchaser is bound to select a Bidder or to appoint the selected Bidder, as the case may be, for the Project and the Purchaser reserves the right to reject all or any of the Proposals without assigning any reasons whatsoever.
- The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Proposal including but not limited to preparation, copying, postage, delivery fees, expenses

associated with any demonstrations or presentations which may be required by the Purchaser or any other costs incurred in connection with or relating to its Proposal. All such costs and expenses will remain with the Bidder and the Purchaser shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an Bidder in preparation of submission of the Proposal, regardless of the conduct or outcome of the Selection Process.

List of Abbreviations

ADF0	: Assistant Divisional Fire Officer
AG	: Advocate General
AME	: Assistant Municipal Engineer
API	: Application Programming Interface
ASLG	: Additional Secretary, Local Government
ATP	: Assistant Town Planner
ATPHQ	: Assistant Town Planning Head Quarters
BPEL	: Business Process Execution Language
BSUP	: Basic Services to Urban Poor
CAA	: Constitutional Amendment Act
CCTNS	: Crime & Criminal Tracking Network System
CDE	: Common Desktop Environment
CE	: Chief Engineer
COTS	: Commercial Off the Shelf
CSC	: Citizen Service Centre
CTI	: Computer Telephonic Integration
CTP	: Chief Town Planner
DBOOT	: Design Build Operate Own and Transfer
SDC/DC	: State Data Center/Data Centre
DDR	: Deputy Director Regional
DHCP	: Dynamic Host Configuration Protocol
DLG	: Directorate Local Government
DLPFC	: District Land Price Fixing Committee
DNS	: Domain Name Services
DR	: Disaster Recovery Site
DTV	: Digital Television
EMS	: Enterprise Management Software
E-Tender Portal	: https://etender.punjabgovt.gov.in/
EO	: Executive Officer
EQMS	: Electronic Queue Management System
EWS	: Economically Weaker Section
F&CC	: Finance and Contract Committee
FIFO	: First In First Out
FIR	: First Information Report
FSO	: Fire Station Officer

G2B	: Government To Business services
G2C	: Government To Citizen services
G2G	: Government To Government services
Gbps	: Gigabits per second
GIS	: Geographical Information System
GOI	: Government of India
H/W	: Hardware
HOD	: Head Of Department
HQ	: Headquarter
HTTPS	: Hyper Text Transfer Protocol Secure
IAFIS	: Integrated Automated Fingerprint Identification System
IAS	: Indian Administrative Service
ICT	: Information and Communication Technology
IEEE	: Institute of Electrical and Electronics Engineers
IMAP	: Internet Message Access Protocol
IPSEC	: Internet protocol Security
ISO	: International Organization for Standards
ITIL	: Information Technology Infrastructure Library
ITSM	: Information Technology Services Management
IVRS	: Interactive Voice Response System
JE	: Junior Engineer
JPEG	: Joint Photographic Experts Group
Kbps	: Kilobits per second
LAC	: Land Acquisition Committee
LAN	: Local Area Network
LDAP	: Lightweight Directory Access Protocol
LGM	: Local Government Minister
Mbps	: Megabits per second
ME	: Municipal Engineer
MIS	: Management Information System
MLLN	: Managed Leased Line Network
MPLS	: Multiprotocol Label Switching
MTP	: Master of town Planning
N/W	: Network
NCF	: Non Construction Fee
NFS	: Network File System
NIS	: Network Information Service

NMS	: Network Monitoring System
NOC	: No Objection Certificate
O & M	: Operations & Maintenance
OVF	: Open Virtualization Format
PCS	: Punjab Civil Services
PDA	: Personal Digital Assistance
PIDB	: Punjab Infrastructure Development Board
PKI	: Public Key Infrastructure
PKCS	: Public-Key Cryptography Standards
PMIDC	: Punjab Municipal Infrastructure Development Company
POP	: Post Office Protocol
PSLG	: Principal Secretary, Local Government
PAWAN	: Punjab State Wide Area Network
Q & A	: Question & Answer
RFP	: Request for Proposal
RKE	: Record Keeping In English
RTI	: Right To Information
RTS	: Right To Services
S/W	: Software
SDM	: Sub Divisional Magistrate
SDO	: Sub-Divisional Officers
SIC	: State Implementation Consultant
SLA	: Service Level Agreement
SLG	: Secretary Local Government
SLLAB	: State Level Land Acquisition Board
SLNA	: State Level Nodal Agency
SMS	: Short Messaging Services
SMTP	: Simple Mail Transfer Protocol
SOA	: Service Oriented Architecture
SOAP	: Simple Object Access Protocol
SP	: State Portal
SPG	: Specific Purpose Grant
SSDG	: State Service Delivery Gateway
SSL	: Secure Socket Layer
SSO	: Single Sign On
STP	: Senior Town Planner
SUDA	: State Urban Development Authority

TCP /IP	: Transmission Control Protocol/ Internet Protocol
TIFF	: Tagged Image File Format
TP	: Town Planning
UDDI	: Universal Description, Discovery and Integration
UID	: Unique Identification
ULB	: Urban Local Bodies
ULCRA	: Urban Land Ceiling And Regulation Act
UML	: Unified Modeling Language
VP	: Vice President
VM	: Virtual Machine
WAN	: Wide Area Network
WFMC	: Workflow Management Coalition
WSDL	: Web Service Definition Language
XINS	: XML Interface for Network Services
XML/ OpenXML	: Extensible Markup Language

Table of Contents

1. Introduction	10
2. Bid Data Sheet.....	12
3. Project Objectives & Desired Outcomes	14
3.1 Project Objectives.....	14
3.2 Desired Outcomes	15
4. Organizational Structure of Punjab Local Government Department.....	17
4.1 Municipal Corporations.....	17
4.2 Municipal Councils / Nagar Panchayats	17
4.3 Improvement Trusts	18
4.4 Directorate & Regional Deputy Director Local Government.....	19
5. Functional Areas and Services	21
6. Envisaged System for Punjab Local Government	32
6.1 Overview.....	32
6.1.1 Portal	32
6.1.2 Back Office System	32
6.1.3 Centralized Application	32
6.1.4 Mobile-enabled Service Delivery	33
6.2 Salient Design Features.....	33
6.3 Service Oriented Framework	34
7. Functional Architecture & Requirements.....	35
7.1 Key Design Requirements.....	35
7.2 Functional Architecture.....	37
7.3 Modular Interactions.....	38
7.4 Processes behind Functions & Services	38
7.5 Benchmarks & Timelines for delivery of G2C and G2B Services.....	49
7.6 Benchmarks & Timelines for Management Functions.....	60
8. Technology Architecture & Requirements	61
8.1 Overview.....	61
8.2 Solution Architecture.....	65
8.3 General Requirements from the Portal	68
8.4 Specific Requirements from the Portal	71
8.5 Requirements from Application Solution.....	73
8.6 Requirements from Mobile Application	76
8.7 Requirements of Back Office	77

8.8	Requirement from Punjab Local Government Gateway	78
8.9	Deployment Architecture	80
8.9.1	Application Server & Web Server	80
8.9.2	Database Server	80
8.9.3	Hardware Security Module (HSM)	81
8.9.4	Mailing & Messaging Server	81
8.9.5	DNS & DHCP Server	81
8.9.6	Directory Server	82
8.9.7	Management Server	82
8.9.8	Backup Server	82
8.9.9	Anti-Virus Server.....	82
8.9.10	Storage Area Network (SAN) & Tape Library.....	82
8.9.11	Firewall & Intrusion Prevention System in HA (High Availability) mode.....	83
8.10	Infrastructure Requirements	83
8.10.1	Data Center	83
8.10.2	Near Disaster Recovery (NDR) Site	84
8.10.3	Disaster Recovery Site.....	85
8.11	Network Requirements.....	89
8.12	Helpdesk Toll Free.....	90
8.12.1	Toll Free Helpdesk for Employees	91
8.12.2	Toll free Helpdesk for Sewa Kendra Operators	92
9.	Security Architecture & Requirements	93
9.1	General Requirements.....	93
9.2	Security Requirements from the Portal.....	95
10.	Operational Requirements	99
10.1	Application Solution Management	99
10.2	Infrastructure Management	100
10.3	Information Security	101
10.4	Project Management.....	102
10.5	Change Management & Training Requirements.....	103
10.6	Qualification & Skills of Resources to be deployed	105
10.7	Maintenance of Physical Security at DC and Near DR	107
10.8	Facility Management & Administration	107
10.9	Requirement for Adherence to Standards.....	115
11.	Data Migration & Digitization.....	116
11.1	Data Migration Requirements	116
11.2	Data Digitization Requirements.....	117

12.	Acceptance Testing, Audit & Certification	123
12.1	Acceptance Criteria.....	124
13.	Phasing, Timeframe and Deliverables	127
14.	Project Governance Structure	135

1. Introduction

- a) With rapid economic development and exposure to global practices, urban citizens today in Punjab expect world class service delivery from government entities. Urban Local Bodies (ULBs) in Punjab are at the forefront of delivering services to citizens. In keeping with emerging realities for service delivery from ULBs, Punjab has adopted the twin strategies of bolstering its urban infrastructure even as it attempts to strengthen its service delivery. Adopting e-Governance is an undisputed pre-requisite for the latter.
- b) The Punjab Local Government Department is at a very significant crossroads where it has embarked on ambitious plans to deliver end-to-end services to its stakeholders (citizens and businesses) in a user-centric way bringing about high levels of accountability and transparency in its service delivery supported by a high degree of efficiency and effectiveness in the department's internal operations. Interventions to be made are not merely at the surface of service delivery but go deeper in such a way that there is a close integration of the service delivery with the department's internal operations.
- c) Punjab Local Government Department extends its services to citizens and businesses through a galaxy of Urban Local Bodies (ULBs), the service delivery arms of the department, that include 10 Municipal Corporations, 155 Municipal Councils/Nagar Panchayats and 28 Improvement Trusts with the last mentioned catering to a classified set of services. Together they constitute the ULB landscape of Punjab as of today.
- d) Urban Local Bodies (ULB) means, for the purpose of this RFP ("RFP"), the service delivery arms of the Punjab Local Government Department including the Secretariat, the Directorate in Chandigarh, PMIDC office, offices of Regional Deputy Directors, Municipal Corporations, Municipal Councils, Nagar Panchayats and Improvement Trusts. Services provided by ULBs connote services provided by one or more of these bodies/offices.
- e) To achieve this project's objectives & outcomes, following building blocks have been envisaged:
 - i. Centralized Infrastructure & Application: This would include:
 - Web-enabled Centralized Application for Citizen services & Back-office operations
 - Hardware, Software, Network for setting up DC, and NDR
 - Mobile apps for delivery services to citizen
 - Helpdesk Facility (for Employees, Service operators and Citizens)
 - Operation & Maintenance of hardware, software and networking including Application
 - Cloud Services for DR on Cloud
 - ii. Back Office Support: This would include:
 - Manpower to facilitate system implementation and technology enhancements as continuous process.
 - Change Management interventions to ensure proper & sustained use of the envisaged system

- f) To deliver the services directly to Citizen, the state Government will provide required front end channels separately including Unified Service delivery center (USDC or Sewa Kendra). These channels will use the front-end interface developed by the selected Supplier to accept the applications and deliver the services.
- g) To implement the above recommendations, Punjab Municipal Infrastructure Development Company (PMIDC), referred to as the "Purchaser" or "Client", on behalf of Punjab Local Government Department intends to engage a Professional Agency, referred to as the "Supplier" or "System Integrator (SI) or Implementation Vendor", that will implement the envisaged system in all its dimensions as specified in this RFP as well as operate & maintain this system as specified in this RFP.
- h) It is to be emphasized here that Punjab Local Government Department is looking at this engagement as a set of complete integrated services to be provided through Sewa Kendras (which will be setup by State Government). To that end the specifications laid out in this RFP are given as the indicative requirement whereas the Supplier is expected to focus on the objectives of this project and formulate their solution offerings in a manner that enables achieving those objectives both in letter as well as spirit. Towards achieving the stated objectives, the Supplier will be required to deploy additional IT infrastructure and services as felt necessary and not be restricted to indicative bill of material provided in this RFP. Further, the payment accruing to the supplier is tightly linked to achieving the service delivery outcomes as specified in this RFP document.

2. Bid Data Sheet

S.No.	Information	Details
1.	Name of the Assignment	Implementation of e-Governance in Urban Local Bodies (ULBs) and Department of Local Government, Punjab
2.	About the Assignment	To provide end-to-end System Implementation Services (software supply & deployment, supply & installation of hardware) followed by 5 Years of O&M Support.
3.	Name of the Tender Inviting Authority	Punjab Municipal Infrastructure Development Company (PMIDC) on behalf of Punjab Local Government Department
4.	Cost of this RFP Document (through e-Payment Gateway)	Rs. 15,000/- (Rupees Fifteen thousand only).
5.	Date of Publishing RFP on e-tender portal	July 13, 2017 RFP can be downloaded from the e-tendering portal free of cost
6.	Date of Publishing of Notice Inviting Tenders (NIT) in English Newspaper viz. 'Economic Times', 'Hindustan Times' and 'Tribune-Chandigarh'	July 14, 2017
7.	Last Date and Time for submission of Queries	July 24, 2017 By 03:00 PM Bidders will have to pay the cost of this RFP online through the portal before submission of queries through email at egov.dolg@gmail.com . The queries can be sent to PMIDC through email in .xls or .xlsx format carrying details like S. No., referred clause, query/suggestion. Queries not sent in the required format shall not be entertained. Refer Attachment 1 of Volume 1 of this RFP.
8.	Date and Time for Pre-Bid Meeting	July 27, 2017 at 2:30 PM Punjab Municipal Infrastructure Development Company (PMIDC), Punjab Municipal Bhawan, 5th Floor, Plot No. 3, Dakshin Marg, Sector 35-A, Chandigarh-160022
9.	Last Date and Time for Submission of Bids	August 17, 2017 By 03:00 PM
10.	Place, Date and Time for opening the Bids and Pre-Qualification	August 18, 2017 at 3:00 PM Punjab Municipal Infrastructure Development Company (PMIDC), Punjab Municipal Bhawan, 5th Floor, Plot No. 3, Dakshin Marg, Sector 35-A, Chandigarh-160022

S.No.	Information	Details
11.	Bid Security / Earnest Money Deposit (EMD)	Rs. 2,00,00,000/- (Rupees Two Crore only) in the form of Bank Guarantee (as per format given in Volume II of the RFP)
12.	Validity Period for Bid Security	180 days (One Hundred & Eighty days) from the last date of submission of the bid.
13.	Validity Period for Proposal	180 days (One Hundred & Eighty days) from the last date of submission of the bid.
14.	Presentation of the Technical Proposal	To be notified later
15.	Results of Technical Evaluation and opening of Commercial Proposal	To be notified later
16.	Method of Selection	Three stage evaluation on Least cost basis
17.	Consortium & Sub-Contracting,	Allowed (Please refer related clauses of Vol. II & Vol. III of RFP),
18.	Term of Contract	5 years from the Go-Live of Phase I
19.	e-Procurement Help Desk details	<ul style="list-style-type: none"> a. Portal: http://etender.punjabgovt.gov.in b. Office Address: Punjab Infotech, (e-Procurement Helpdesk), S.C.O - 101, 2nd Floor, Sector – 47 C, Chandigarh. c. Visiting Hours: 8 AM to 8 PM (Monday to Sunday except Public Holidays) d. Contact Details: <ul style="list-style-type: none"> Tel : 0172-3953764 Fax : 0172-3934665 (Fax) Mobile : 09257209340, 08054628821 E-mail : etenderhelpdesk@punjabinfotech.in, etender.helpdesk.pictc@gmail.com

3. Project Objectives & Desired Outcomes

- a) Punjab Local Government Department has ambitious plans to reach out to the citizens by providing integrated, end-to-end services using a comprehensive State-wide Service Delivery Infrastructure, constituted by a chain of State owned and managed Sewa Kendras and by utilizing advanced ICT tools for citizen-facing service delivery and back-office computerization.
- b) The idea is to provide integrated services to citizens in a transparent, effective and efficient manner to bring about high levels of citizen-satisfaction.
- c) Primary goal of this project is to provide Local Government services to citizens through online / Single Window service delivery channel and ensure accessible, convenient, transparent and timely delivery of services. These service delivery channels (Sewa Kendras) will be established by state separately.
- d) The proposed project is also envisaged to provide an 'assisted online' mechanism for enabling the citizens and businesses to transact with the Punjab Local Government through Sewa Kendras (established, owned and managed by State separately).

Sewa Kendras are aimed to assist the citizens, not having the requisite skill sets and access to facilities for performing the G2B & G2C transactions involving large documentation requirements, physical verification requirements, etc. online using the portal.

- e) This initiative is to be driven by the following Vision statement:

"Bring about high levels of citizen satisfaction through integrated service delivery on an anytime, anywhere basis, in a transparent, effective and efficient manner."

3.1 Project Objectives

- a) Following are the broad objectives of the envisaged Project:
 - i. Provide online access to the current, complete and accurate information related to functions and services provided by Punjab Local Government Department through its constituent ULBs to citizens, Businesses and Government
 - ii. Achieving internal efficiency & effectiveness of the ULBs by automating and optimizing their back-office processes.
 - iii. To provide citizens and businesses with access to information such as expected service fulfillment times for the Government services, business processes, applicable rules and legislations, etc.
 - iv. To facilitate secure, instantaneous and online payment options for the utility bill payments, taxes and statutory fees associated with services
 - v. To reduce the administrative burden and to be a cost-effective service delivery channel for Punjab Local Government Department
 - vi. To enable the Punjab Local Government Department to focus on their core functions and responsibilities by freeing them from the routine operations (like collection of taxes & fees,

- issuing of certificates, etc.) and thereby enhance the overall productivity of the administrative machinery
- vii. Bring the ULBs closer to the citizens through "Anywhere Anytime Service Delivery"
 - viii. Deliver services to the stakeholders in minimum turnaround time and minimal physical interaction with the ULBs
 - ix. Develop interface of ULBs with other Departments to facilitate seamless sharing of information for better administration and governance.

b) From the perspective of different participating stakeholders, following are the project objectives:

For Citizens & Businesses	For ULBs & the Government	For Supplier
<ul style="list-style-type: none"> Enhanced quality of service Minimizing the number of visits to the ULBs Increased number of service platforms Reduction in time taken to deliver service Easy availability of desired Information 	<ul style="list-style-type: none"> Process efficiency & effectiveness Enhancing existing revenues Setting up new revenue streams Reducing processing cost Boosting own image in front of citizens and businesses 	<ul style="list-style-type: none"> Proficiency in service delivery.

3.2 Desired Outcomes

Following are the desired outcomes from this project:

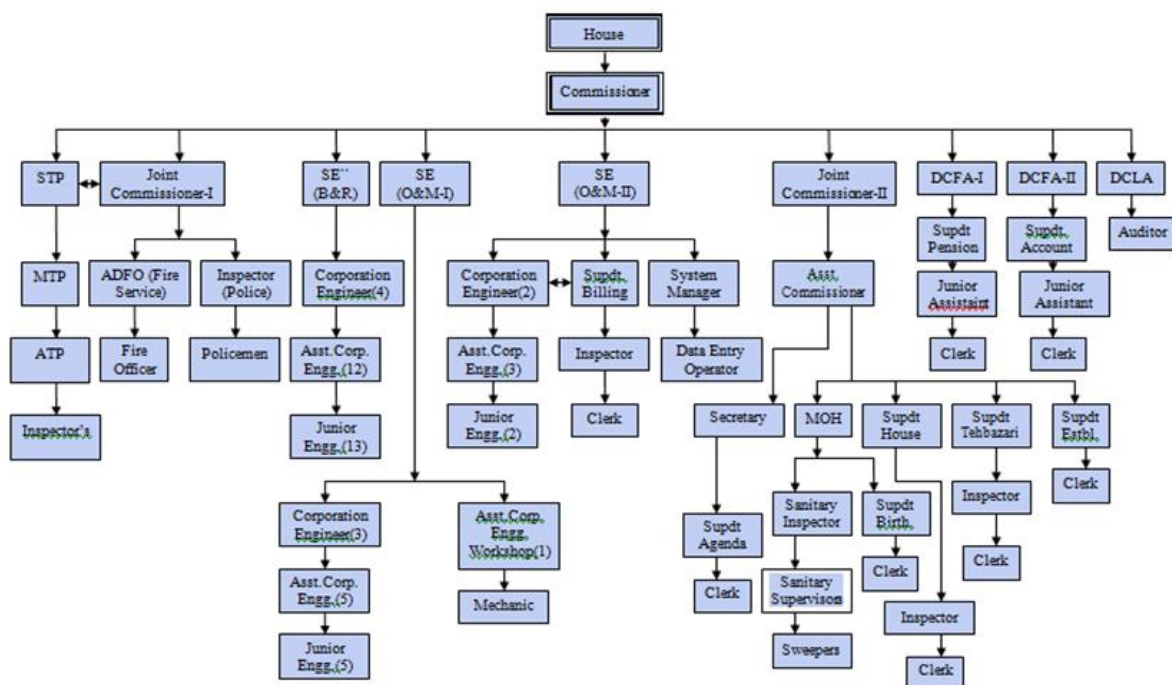
For Citizens & Businesses	For ULBs & Government	For Supplier
<ul style="list-style-type: none"> Anywhere, Anytime Services via multiple Delivery channels& mechanism. Delivery of all Services within pre-defined timelines Ease of availability of all Local Government-related information online 	<ul style="list-style-type: none"> Uniform and well-defined work procedures Rationalized work norms and clear accountability for performance Recognition to efficient employees 	<ul style="list-style-type: none"> Improved service delivery to citizens Standardized practices and procedures across all ULB offices Centralized decision support system to monitor and evaluate the performance of

For Citizens & Businesses	For ULBs & Government	For Supplier
<ul style="list-style-type: none"> • Real-time status tracking • Ease of payment of fees for the services received • An effective Grievance Redressal Mechanism • Transparency in availing services 	<ul style="list-style-type: none"> • Trainings for requisite skill enhancement • High growth opportunity in areas of value-added services, on account of outsourcing of non-core activities • Better work environment 	<p>all ULB offices across Punjab.</p> <ul style="list-style-type: none"> • Capability to handle increased demand • Better utilization of Government resources in areas of value-added services, on account of outsourcing of non-core activities

4. Organizational Structure of Punjab Local Government Department

4.1 Municipal Corporations

- a) Municipal Corporations have deliberative and executive wings. In general, deliberative wings of Municipal Corporations comprise the Corporation Council, Standing Committee and the Mayor, whereas the executive wings comprise the Municipal Commissioner, the Deputy/Assistant/Joint Municipal Commissioner, the Municipal Engineer and subordinate administrative staff.

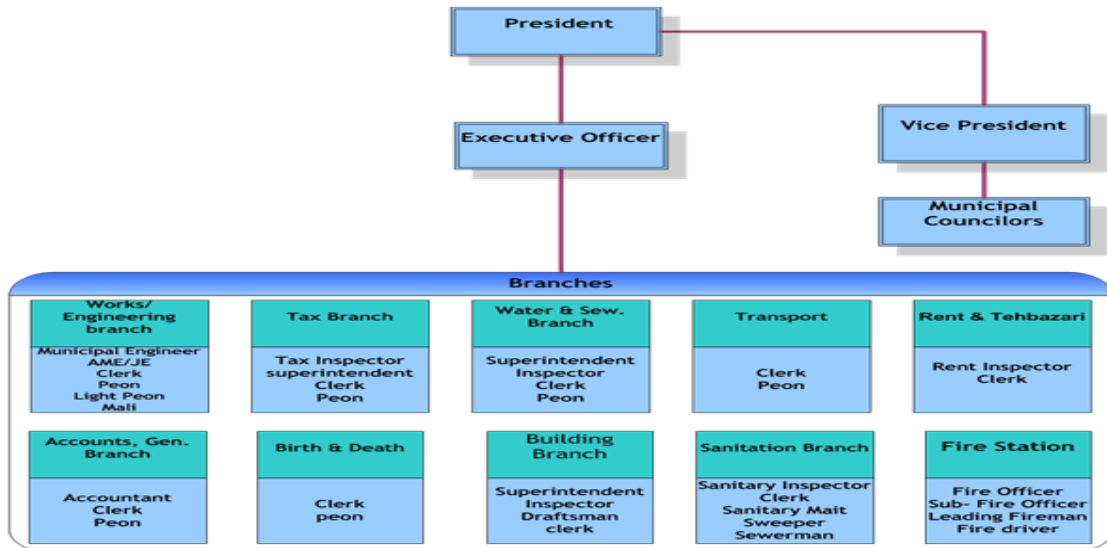


- b) Figure shown above brings out typical organization chart for a Municipal Corporation. In Punjab there are 10 Corporations at Amritsar, Ludhiana, Jalandhar, Patiala, Bhatinda, Mohali, Pathankot, Moga, Hoshiarpur and Phagwara. However, there may be certain variations from one Corporation to other, and in course of time there may be changes in areas under their jurisdictions and the departmental positions/officials. Also, it may be noted that there may be addition in the number of Municipal Corporation in future as per policies of the State Government.

4.2 Municipal Councils / Nagar Panchayats

- a) A Council is a body constituted by the incorporation of the inhabitants of a city or town. Normally, Municipal Councils cover smaller areas than the Municipal Corporations. The State Government can, by notification, propose an area, except a military cantonment, to be a municipality, define its territorial limits and make alterations in them. The Municipal Council President, the Committees and the Executive

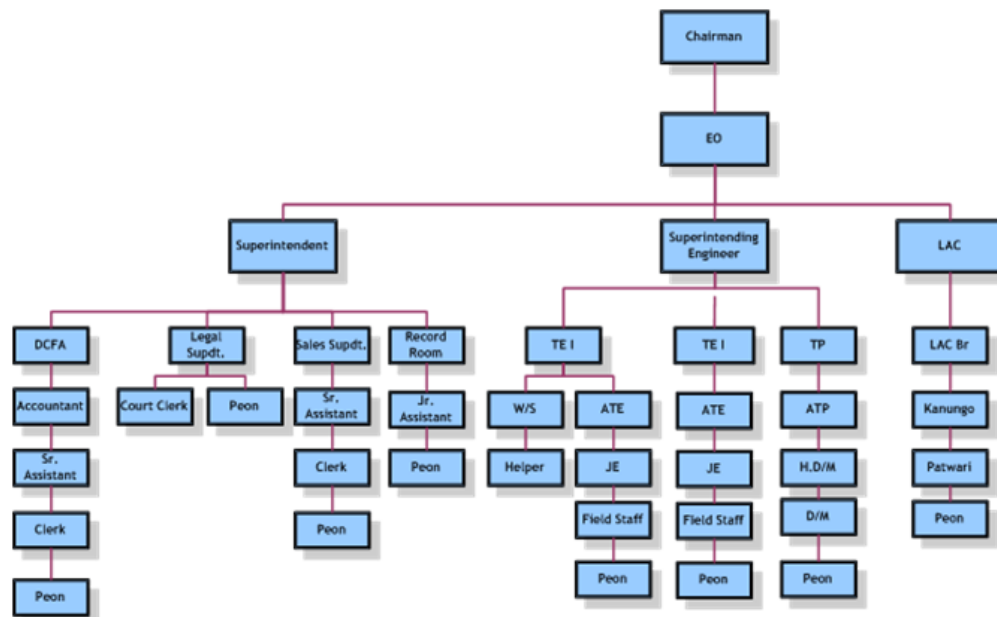
Officer constitute the main components of the structure of municipal government. The Municipal Council makes laws that are called bye-laws within the framework of the municipal act for the civic governance of the city or town.



- b) The figure shown above brings out the typical organization chart for a Municipal Council / Nagar Panchayat. However, there may be certain variations from one Council/Nagar Panchayat to the other and in course of time there may be changes in the areas under their jurisdictions and the departmental positions/officials as shown in this figure. Also, it may be noted that there may be addition in the number of Municipal Council / Nagar Panchayat in the future as per the policies of the State Government.

4.3 Improvement Trusts

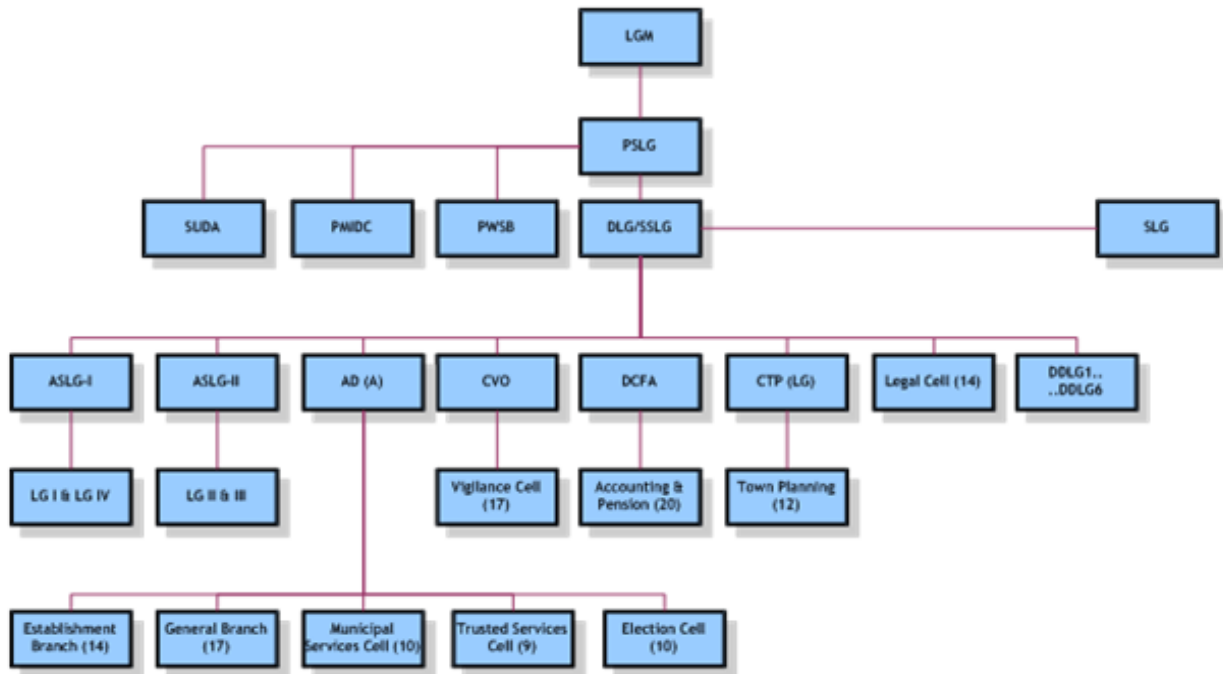
- a) Improvement Trusts are bodies entrusted with land planning and acquisition and are responsible for infrastructure such as roads, streetlights, drainage & sewerage systems and public utilities to meet the diverse needs of the citizens. As per the Provisions of the act, Improvement Trust is empowered to plan and execute various development schemes. An improvement scheme shall be one of the following types or may combine any two or more of such types, or any of the special features thereof, that is to say, a general improvement scheme, re-building scheme, re-housing scheme, street scheme, deferred street scheme, development scheme, housing accommodation scheme, future expansion or improvement scheme and a drainage or drainage including sewage disposal scheme.



- b) The figure shown above brings out the typical organization chart for an Improvement Trust. There are 29 Improvement Trusts in Punjab. However it may be noted that there may be certain variations from one Improvement Trust to the other and in course of time there may be changes in the areas under their jurisdictions and the departmental positions/officials as shown in this figure.

4.4 Directorate & Regional Deputy Director Local Government

- a) Director is the Chief Controlling Authority and the main function of the Directorate is to have an effective co-ordination with the ULBs as well as with the Deputy Directors on the one hand and the Secretariat in the Government on the other hand. The Directorate has responsibility to supervise the functioning of the municipalities, work out suitable HR policies, exercise disciplinary control over the staff of municipalities, monitor the tax collection of ULBs, lay down policies for transparency in expenditures, and hear appeals against decisions of municipalities.
- b) Directorate also releases Government grants to ULBs, to implement schemes of state and central government. The Directorate also collects statistics from ULBs and helps in the preparation of municipal statistics. The proposals submitted by the ULBs through the Deputy Directors and of respective District in the matters of Administration, Execution of works and schemes are examined by the Directorate under the provision of Act & Rules and also on the instructions and guidelines of the Government, issued from time to time.
- c) All proposals sent by the ULB for release of funds, sanctions, approvals, disciplinary matters are routed through Deputy Directors. After examination of the case by concerned Officers file is put up to the Director for suitable decision. The decision taken is communicated to the concerned through a letter/email. Joint Directors supervise all the works carried out by the lower level officers and staff.



- d) Figure shown above brings out the overall organization chart for the Department of Local Governance, Punjab. In addition to ULBs, there are external stakeholders, who are involved directly or indirectly with various wings of the Punjab Local Government Department. Examples of external stakeholders include Hospitals, Nursing homes, Department of Social Security etc. SUDA, PMDC and PWSSB are the other organizations which come under Principle Secretary Punjab Local Government.

Secretariat, Local Government is entrusted with the responsibilities of all policy making and amendment of rules/acts for the welfare of the urban citizen. As shown in the previous diagram, the Secretary is assisted by Additional Secretary, Local Government (ASLG). The administrative functions of Secretariat is divided to four branches namely LG I, LG II, LG III and LG IV. Superintendents, Assistants and Clerks of LG I & LG IV report to ASLG I and that of LG II & LG III reports to ASLG II.

5. Functional Areas and Services

This Chapter contains the various Functions and Services provided by Municipal Corporations / Councils, Improvement Trusts and at the Head Quarter. These services are Government to Citizen (G2C), Government to Business (G2B) and Government to Government (G2G) and other internal management/administrative functions.

The list below is an overview of the various services being offered currently. However the bouquet of services as well as the related policies/ rules may be modified and/or amended by Punjab Local Government from time to time. The scope of this assignment includes all the services being provided to citizens and businesses as well as all internal management functions of the ULBs.

The provision for information services such as enquiry about policy & procedure, contact details, availability of application forms and other pieces of information that the Department can provide is being treated as an umbrella requirement that ought to be met by the proposed system. Informational details to be provided by the portal, for example, are expected to be finalized during the course of implementation and this document does not attempt to bring any finality in such specifications.

Minimum functional requirements have been provided in Attachment-2 of this RFP. Further, the requirements should be read in conjunction with the As-Is Status and To-Be requirements as mentioned in this RFP. The requirements to be captured and finalized in the FRS (Functional Requirement Specifications) and SRS (System Requirement Specification) are expected to be in much greater detail as compared to what is contained in this RFP.

a) Services and Management Functions of Corporations, Councils and Nagar Panchayats are given below:

Functional Area	Name of Service		Type of Service
Birth & Death Certificates	1.	Registration of Birth	G2C
	2.	Issue of Birth Certificate	G2C
	3.	Late Registration of Birth	G2C
	4.	Name-correction in Birth Certificate	G2C
	5.	Name Entry for Birth Registration	G2C
	6.	Registration of Death	G2C
	7.	Issue of Death Certificate	G2C
	8.	Name-correction in Death Certificate	G2C
	9.	Late Registration of Death	G2C
Water Supply & Sewerage	10.	New Water Connection	G2C
	11.	Payment of Water Bill	G2C
	12.	Change of Title in Water Bill	G2C
	13.	Approval of Water Disconnection	G2C
	14.	Water Reconnection	G2C
	15.	New Sewerage Connection	G2C
	16.	Payment of Sewerage Bill	G2C
	17.	Change of Title in Sewerage Bill	G2C

Functional Area	Name of Service		Type of Service
	18.	Approval of Sewerage Disconnection	G2C
	19.	Sewerage Reconnection	G2C
	20.	Assessment of Disposal Charges	G2C
	21.	Water & Sewerage Bill Amendment	G2C
Licenses & Permits	22.	License for setting-up a Commercial Unit	G2B / G2C
	23.	License for a Mule Cart	G2B / G2C
	24.	License for Slaughterhouse	G2B / G2C
	25.	License for a Rickshaw	G2B / G2C
	26.	License for setting up Communication Tower on Private Property	G2B / G2C
	27.	License for setting up Communication Tower on ULB Property	G2B / G2C
Sanitation & Public Health	28.	Collection & disposal of Solid Waste	G2C
	29.	Challan for dumping dirt / garbage	Management Function
	30.	Sterilization of stray dogs	G2C
	31.	Spray / fogging for prevention of Air-borne Diseases	G2C
	32.	Penalty for Stray Cattle	Management Function
	33.	Appointment of Vendors for collection & disposal of Solid Waste	Management Function
	34.	Monitoring performance of Vendors appointed for collection & disposal of Solid Waste	Management Function
	35.	Details regarding ULB properties available for rent / lease	G2B / G2C

Functional Area	Name of Service		Type of Service
Rent & Fee Collection	36.	Renting / leasing of ULB properties	G2B / G2C
	37.	Collection of rent / lease	G2B / G2C
	38.	Removal of Temporary Encroachment	Management Function
	39.	Collection of Tahebazari Fees	G2B / G2C
	40.	Annual Fee for Communication Towers on ULB Property	G2B / G2C
Fire Safety Services	41.	Conducting Fire Rescue Operations	G2C / G2B
	42.	Issue of NOC for Fire Safety	G2C / G2B
	43.	Issue of Fire Call Report	G2C / G2B
Advertisement & Hoardings	44.	Approval for Hoardings / Adv. Boards on private properties	G2B / G2C
	45.	Information on ULB Sites available for Hoardings / Adv. Boards	G2B / G2C
	46.	Contracting of Advertisement Sites with Relevant Media	G2B / G2C
	47.	Contracting / renting of Govt. Sites for Hoardings / Adv. Boards	G2B / G2C
Property Tax	48.	Assigning a Unique ID to each Property	Management Function
	49.	Assessment and collection of Property Tax	G2C
	50.	Issuance of TS-1 Certificate	G2C
Transport	51.	Issue of Bus Pass (for buses operated by the ULB)	G2C
	52.	Fleet management	Management Function
Library Management	53.	Information regarding books available in Libraries managed by the ULBs	G2C
	54.	Issue of Membership Card for Libraries managed by the ULBs	G2C

Functional Area	Name of Service		Type of Service
	55.	Library Management (including issue / return of books)	Management Function
Miscellaneous Functions	56.	Verification of widows, elderly, handicapped, etc. for inclusion in appropriate Scheme	G2C
	57.	Management of Parks & Plantations managed by the ULBs	G2C
	58.	Management of various Civil Works of ULBs	Management Function
	59.	Resolution of Complaints & Grievances received from citizens	G2C
	60.	Supply of information under RTI Act	G2C

b) Services & Management Functions at Improvement Trusts

S.No.	Functional Area	Related Services	Service Type
1.	Land Acquisition	Land Acquisition Process	Management Function
		Approval of Enhanced Compensation	G2C/G2B
		Approval of Development Schemes	Management Function
2.	Sale of Plots / Flats	Information regarding available Plots/ Flats	G2C/G2B
		Draw of Lots	G2C/G2B
		Conducting of Auction	G2C/G2B
		Refund of Earnest Money	Management Function
		Finalization of Sale Agreement	G2C/G2B
		Payment of Regular Installment	G2C/G2B
		Payment from Defaulters	G2C/G2B
		Issuance of Possession Letters	G2C/G2B
		Issuance of Allotment Letters	G2C/G2B
		Issuance of NOC for allotted plots	G2C/G2B
		Finalization of Sale Deed	G2C/G2B
		sanction of change of land use	G2C/G2B
3.	Property Management	Sanction of Building Plan/Completion Plan	G2C/G2B
		Transfer of Property	G2C/G2B
		Permission for Mortgage of Property	G2C/G2B
		Approval for time extension	G2C/G2B

S.No.	Functional Area	Related Services	Service Type
		Penalty for violation of approved Plan or construction without Plan	G2C/G2B
4.	Works Management	Estimating and tendering for development works	Management Function
		Payment of development work	Management Function

c) Administrative Functions at ULBs (Corporations, Councils, Nagar Panchayats and Improvement Trusts)

S.No.	Functional Area	Brief Description	Related Services	Service Type
1.	Secretarial Functions	This represents various secretarial functions of the ULBs	Executive Management of Meetings (Agenda preparation, recording Proceedings, etc.) Preparation of Resolutions Maintenance of Records for various Business Matters of the ULBs	Management Function Management Function Management Function
2.	Legal Matters	This area includes all details related to the different legal cases that apply for the Urban Local Bodies.	Handling of court cases	Management Function
3.	RTI	This refers to the requests received at the ULBs under RTI Act	Supply of information under RTI Act	G2C
4.	RTS	This refers to the requests received at the ULBs under RTS Act	Supply of information under RTS Act	G2C
5.	MIS	This refers to decision support systems that are made available to the ULBs (to help them arrive at informed decisions)	Dashboard & MIS at various level	Management Function

S.No.	Functional Area	Brief Description	Related Services	Service Type
6.	Double-Entry Accounting	This refers to the accounting system to be implemented in the ULBs.	Entry of collections into Account books	Management Function
			Entry of expenditure of ULBs	Management Function
7.	Budget Management	This refers to process of budgeting at ULBs	Budget Preparation	Management Function
8.	Employee Services	This refers to career-related details (appointment, promotion, punishment, performance appraisal, trainings undergone) for the employees of ULBs.	Promotion of Staff	Management Function
			Transfer of Staff	Management Function
			Sanction process of the Leaves	Management Function
			Assured Career Progress Scheme	Management Function
			Employment in case of the death	Management Function
			Recruitment of Staff	Management Function
			Punishment of Staff	Management Function
			Maintenance of Annual Confidentiality Report	Management Function
9.	Payroll & Pension	This area refers to salary and pension related details for the employees of the ULBs.	Payment of Salary	Management Function
			Sanction of Staff Retirement Benefits (Pension)	Management Function

d) Complaints & Grievances

S.No.	Functional Area	Brief Description	Related Services	Service Type
1.	Complaints & Grievances	This refers to details related to the complaints and grievances filed with ULBs and their subsequent disposal	Resolution of Complaints & Grievances	G2C / G2B

e) Management Functions at Secretariat, Headquarter & Regional Deputy Director Office

S.No.	Functional Area	Related Services	Service Type
1.	Secretariat & Headquarter	Approval of resolution of Municipal Councils	Management Function
		Technical Sanction of Project Estimates at ULBs	Management Function
		Implementation & Monitoring of GoI sanctioned / State sanctioned project by PMIDC	Management Function
		Appointment of staff of ULBs / Dept.	Management Function
		Promotion of staff of ULBs / Dept.	Management Function
		Leave and NOC for Passport/foreign travel and other schemes for staff of ULBs / Dept.	Management Function
		Technical sanction of plan by CTP	Management Function
		Complaints and disciplinary actions on the staff of ULBs / Dept.	Management Function
		Fund withdrawal and Distribution (Finance & Account Branch)	Management Function
		Preparation of response and attending of court cases	Management Function
		Conducting Election to notify president and members	Management Function
		Approval of Resolutions and other matters of Corporations	Management Function
		Establishment works of ULBs	Management Function
		Amendment / Relaxation of building bye laws / TP Schemes / Change of land use	Management Function
		Amendment of Acts, Rules, building bye laws of corporations	Management Function
		Facilities and powers of Mayors, Senior Deputy Mayor, Deputy Mayor and Councilors	Management Function
		Approval of schemes/Plots/Reserve Price/Resolutions	Management Function
		Notification of new development schemes	Management Function
		NOC from FCR for new schemes	Management Function
		Permission for Issuing allotment letter/ Confirmation of draw/ auction	Management Function
		Change of land use (Residential to commercial)	Management Function
		Waiving of non-construction fees (NCF) of plots	Management Function
		Maintenance of information for Court cases	Management Function

S.No.	Functional Area	Related Services	Service Type
		Providing Answers to the Questions / Queries raised in the Vidhan Sabha	Management Function
		Record keeping of files	Management Function
		Complaints & actions against President, VP, Councilors	Management Function
		Approval of Policies of MC matter	Management Function
		Approval of TP schemes	Management Function
		Appellate Authority of staff of MC and NP	Management Function
		Meetings-Preparation and Participation	Management Function
		RTI Coordination	Management Function
		RTS Coordination	Management Function
		Coordination for training	Management Function
		Rent Act Constitution implementation and amendment	Management Function
		Establishment work of Directorates and DDRs	Management Function
		Establishment work of sewerage board	Management Function
		Establishment work of PMIDC	Management Function
		Providing Information for FM speech in budget session	Management Function
		Statistics and administrative report	Management Function
		Land acquisition for STP/Solid Waste	Management Function
		Approval of installation of tube well in committees	Management Function
		Enhancements/Exemption/Rebate of water and sewerage board charges	Management Function
		Empanelment of lawyers	Management Function
		Audit and accounts of sewerage board	Management Function
		Sanction of project fund from the state Govt.	Management Function
		Coordination of other works of LG department	Management Function
2.	Regional Deputy Director Office	Approval of Budget Estimates of ULBs	Management Function
		Approval of minutes of the meeting of ULBs	Management Function
		Administrative Approval of Estimates of ULBs	Management Function

S.No.	Functional Area	Related Services	Service Type
		Approval under Section 52(2)(L) of Punjab Municipal Act 1911	Management Function
		Recovery of arrears of ULBs	Management Function
		Approval of Bye Laws of ULBs	Management Function
		Approval / disbursement of Pension to the retired employees of ULBs	Management Function
		Approval of Medical Reimbursement Expenditure of employees of ULBs	Management Function
		Recording of the Annual Confidential Reports of the employees (Provincialized Cadre) of ULBs	Management Function
		Performing the function of Collector under PP Act, 1973	Management Function

The provision for future integration of services of other Departments / MMPs should be kept in the proposed solution.

6. Envisaged System for Punjab Local Government

6.1 Overview

It is to be emphasized that PMIDC, through this Project, is seeking a complete set of integrated and comprehensive services to be provided by the selected bidder (Implementation Vendor) and is not merely looking for a supplier of hardware & software. Bidder is required to assess the requirements as provided in the RFP and do the sizing of entire solution and accordingly, propose the bill of materials. Proposed items should be equivalent or better in terms of technical specifications and performance taking into consideration the nature, size, criticality, scalability, security, service levels and objectives of the Project. Bidders are encouraged to propose latest technology addressing the requirements as given in RFP like virtualization, and unified/converge systems.

6.1.1 Portal

- a) Portal shall be the interface and delivery channel for citizens, Department and other stakeholders to access various services rendered by Department of Local Government, Punjab. Users shall have direct access to this portal from their office/homes/other locations. Citizen will use State Government portal where SSO feature is already available. Department's internal users may also use same portal or there may be separate login mechanism. This will be finalized during Inception/Design phase.
- b) Service-transactions that are initiated either directly or via Sewa Kendras shall be routed to the Back Office System (which shall be implemented as a part of this project) through a secure and reliable messaging infrastructure.
- c) Portal is a critical element in the System Architecture of Punjab Local Government and would act as the "Gateway" between the Sewa Kendras and the Back Offices of the Punjab Local Government.

6.1.2 Back Office System

Back Office System shall provide the user interface to the Employees of Punjab Local Government for processing the transactions submitted through various service delivery channels including Sewa Kendras. Direct access to Back Office system shall be restricted only to the Employees of Punjab Local Government.

Total number of employees in the Department is approximately 32,279.

The Back Office System shall also contain all administrative and management functions related to Punjab Local Government and to enable the same, the Supplier shall have to provide suitable and adequate human resources.

6.1.3 Centralized Application

- a) The Supplier shall configure and deploy a Centralized Application for delivering all the services and management functions of Punjab Local Government as identified in this Volume of the RFP. This Application may be a COTS or Be-Spoke Solution.

- b) This Centralized Application shall be hosted at the Punjab State Data Centre.
- c) This Centralized Application should also be compatible and will be integrated with various e-Governance Systems under the NeGP/Digital India (such as Mobile Service Delivery Gateway, Digital Signature, e-Pramaan, etc.), with Aadhaar and also with various e-Governance Systems (already implemented or envisaged in near future) of Punjab Government (such as e-District, CCTNS, SP (Date Portals) and SSDG)

6.1.4 Mobile-enabled Service Delivery

Rapidly increasing levels of mobile penetration and networking, and requirements of accessibility and citizen convenience must prompt the Supplier to offer more and more services over mobile devices. The Supplier must build strong interfaces, technologies, applications, etc. for mobile devices. Supplier is required to provide SMS and/or USSD based services to citizens. Supplier needs to administer SMS gateway available with Department and integrate relevant services with SMS gateway.

In order to maximize citizen convenience and bring about business process improvements, the supplier must continuously innovate, upgrade and incorporate such new technologies that emerge. It is also assumed that Suppliers will attempt to include as many services over mobile devices as possible, beyond the ones mentioned in this RFP such as collection of taxes/payments/tehbazari through mobile application including integration of receipt through SMS, updation of accounts, etc. For this purpose, the Supplier should also integrate the Mobile Services Application (that is proposed for this project) with Mobile Service Delivery Gateway as envisaged under the NeGP/Digital India and MMPs.

Supplier needs to comply with mGov standards of Government of India.

Mobile applications should have provision of payment through payment gateway. Its payment workflow will be designed during preparation of SRS/design documents.

System should support Users to register and avail mobile enables services. However, select services may be availed without registration. This requirement will be finalized at the time of finalizing design document.

6.2 Salient Design Features

- a) Interfacing with Citizen: The proposed system is designed to establish an extremely smooth citizen interface. The focus in the design has been on maximizing citizen convenience in applying for various Punjab Local Government services, visiting the ULB facilities and in obtaining the services with speed and certainty. These design features are described below:
 - i. Multiple Channels for Service delivery: Citizen shall be allowed to submit their requests for various services through the Portal, Mobile Devices, via the Sewa Kendras or any other existing or future front-end delivery centers established by the State for service delivery.
 - ii. Availability of Portal: It is proposed to establish a Punjab Local Government Portal that can provide guidance to citizens on the procedure and forms, besides enabling them to transact with Punjab Local Government for a variety of services, including filing applications online, tracking status and registering grievances. This portal would serve as the common interface

- for all the users across all ULBs. The system will have provision for ULB-specific portals and information when a choice for a particular ULB is made.
- iii. Helpdesk for Citizens/Sewa Kendra Operators with Toll free number: In addition to the portal, a Helpdesk (i.e. Call Center (In-bound and out-bound)) shall be established by the Supplier to provide IVRS enabled voice-based assistance to the citizens/Sewa Kendra Operators pertaining to various services. Citizens should be able to make enquiries, register their complaints and grievances, and track their application/ complaint status via this Helpdesk.
- b) **Processing of Services**: In order to meet the requirements of the specified service levels, the backend offices of the Punjab Local Government, mainly the ULBs will be reorganized in terms of the processes followed. The following are the salient features of the proposed system of processing of services:
- i. Back Office Processing: All the citizen service related input data will be entered into the system through front-end application at the Sewa Kendras/Portal/Mobile Apps//etc. and back-end related processing of services and management functions will be carried out at Punjab Local Government Offices through back-end centralized integrated application system.
 - ii. IT Infrastructure: In order to achieve & maintain the desired productivity levels, it is necessary to provide appropriate IT infrastructure and related services in the Punjab Local Government Offices. Punjab Local Government proposes to revamp the IT infrastructure at Punjab Local Government Back Offices, in a phased manner, in tandem with the rollout of the proposed system across different locations and functionalities.

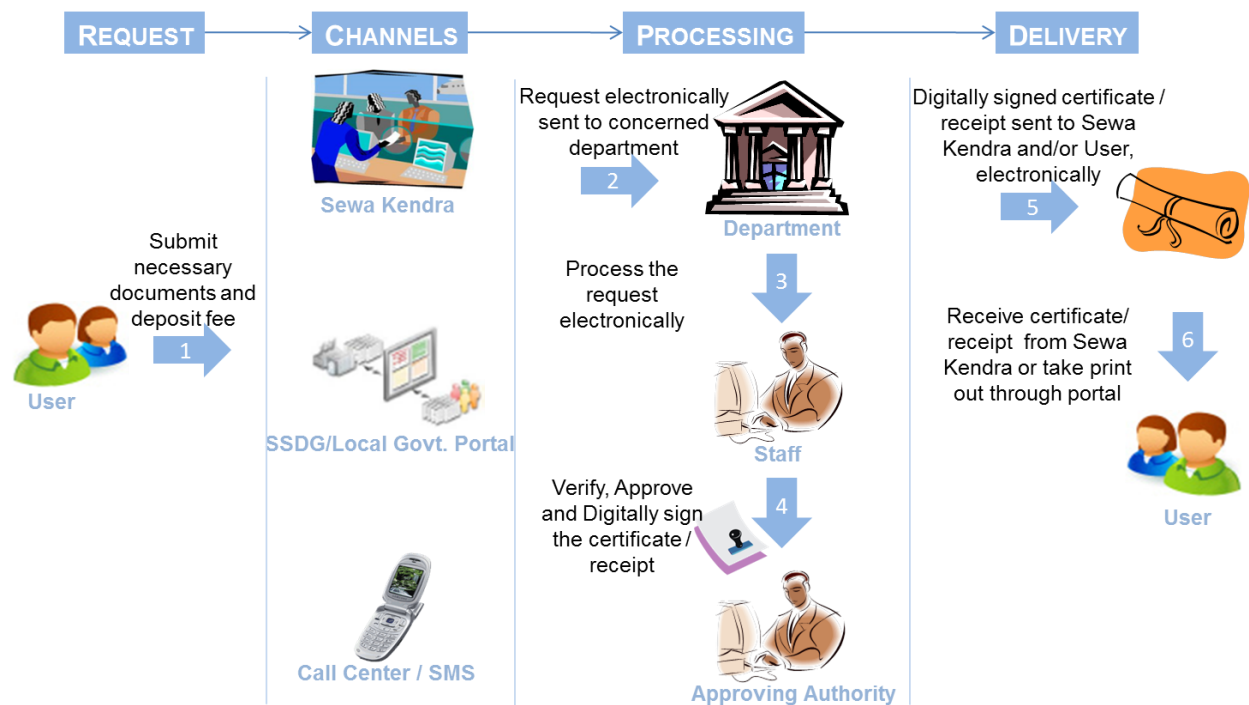
6.3 Service Oriented Framework

- a) Punjab Local Government aims to implement this project on a Service Oriented Approach.
- b) Punjab Local Government is not merely interested in establishing State Data Centers and Service Centers laden with hardware, software and networks. It is interested in the Outcomes i.e. citizen services delivered in compliance with the Service Level Agreements (SLAs) as defined in Attachment 11 of this volume of RFP. The payments to the Supplier would be linked tightly to the compliance with the SLAs as specified in this RFP.
- c) It is essential to recognize that Punjab Local Government intends to implement the project, wherein primary responsibility of delivering quality and efficient services falls upon on the Supplier.

7. Functional Architecture & Requirements

7.1 Key Design Requirements

- a) Supplier is required to design suitable solution architecture to support the functional requirement. Minimum functional requirements have been provided in Attachment-2 of this RFP. Further, the requirements should be read in conjunction with the As-Is Status and To-Be requirements as mentioned in this RFP.
- b) Supplier shall do the detailed assessment of the various services/management functions. The assessment by the Supplier may result in identification of business process re-engineering areas. Supplier shall also the design/customize the existing forms for delivering the services. Supplier shall discuss with the Purchaser and its stakeholders for such business process re-engineering areas & forms and take the sign-off from Purchaser.
- c) Supplier shall prepare detailed FRS (Functional Requirement Specifications) and SRS (System Requirement Specification). The requirements to be captured and finalized in the FRS and SRS are expected to be in much greater detail as compared to what is contained in this RFP.
- d) Typically a service delivery workflow would be like diagram given below:



1 Centralized Infrastructure

- i. The System for Punjab Local Government shall be centrally hosted at the SDC which will be the hub of all applications and transactions.

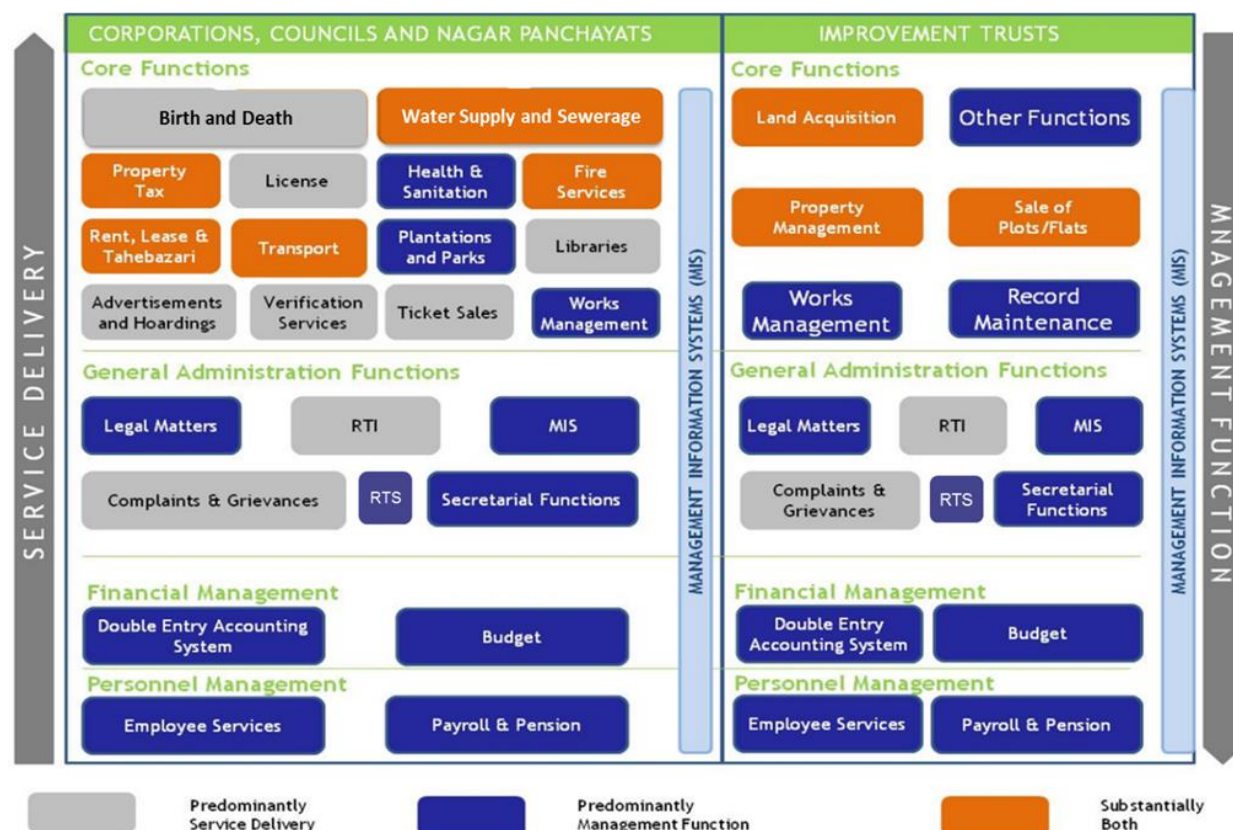
- ii. It should be possible to install any new application or enhanced version of an existing application at the SDC and make it available to all user sites instantaneously
- iii. Portal should allow for online filling up and submission of forms as well as downloading the form, filling up the same offline to be later uploaded on the portal.
- iv. The complete database of ULB transactions shall be maintained at the SDC.
- v. There shall be a fully equipped Disaster Recovery (DR) cloud services.
- vi. This system should be scalable, secure, reliable and manageable as required and specified in this RFP.
- vii. There would be a Helpdesk for the employees, citizen and Sewa Kendra Operators for handling their technical issues, complaints and to provide them with assistance as necessary.

2 Back Office System

- i. Existing ULB Offices will perform the back-end processes identified above as well as for catering to other functions like public grievance hearing, approval, policy, etc. Also, the ULBs will perform their normal management functions through the Centralized Back Office Application System.
- ii. The user should be able to select a particular location/ULB and the page pertaining to that location/ULB should pop up.
- iii. The ULB shall also perform their routine administrative and management functions using the envisaged automated system.

7.2 Functional Architecture

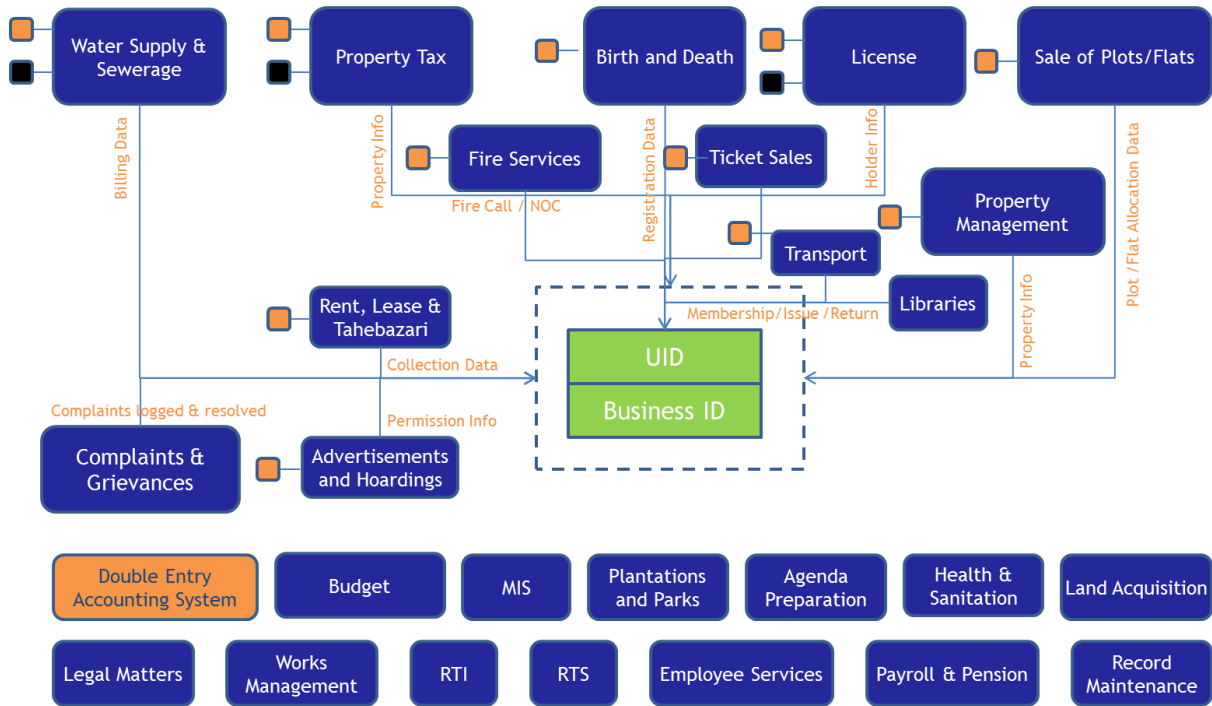
Envisaged system for Punjab Local Government would have the architecture as shown below:



- Corporation and Council Management System: This shall cover all the Services and Management Functions of Municipal Corporations, Municipal Councils and Nagar Panchayats as described in this Volume of the RFP.
- Improvement Trust Management System: This shall cover all the Services and Management Functions of Improvement Trusts as described in this Volume of the RFP.
- General Administration System: This would include all the administrative functions of the Department and the ULBs under it as described in this Volume of the RFP.
- Grievance Management System: This shall be a centrally-shared system for delivering the services related to complaints and grievances of citizens as described in this Volume of the RFP.

7.3 Modular Interactions

- e) Modules and services/functions constituting them do not operate in isolation but have substantial interfaces where they overlap and interact with other modules. The following figure illustratively suggests how different modules would interact amongst themselves.



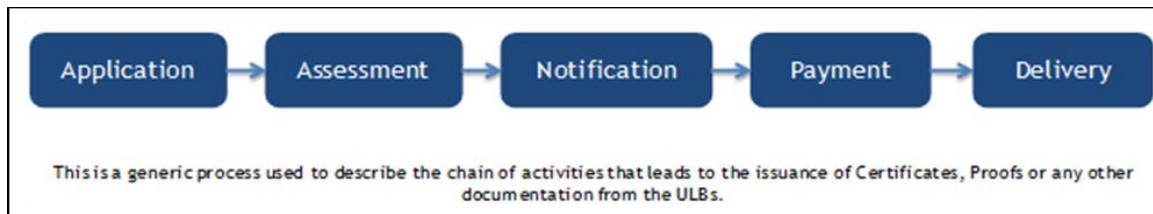
- f) A comprehensive study of the services and functions of the Local Government reveals that there is a remarkable amount of similarity between the processes followed for similar activities in different business units of the Urban Local Bodies; for example, the process of getting a certificate is the same regardless of the department or business unit the certificate is being taken from. Otherwise, too, making this process work on similar lines will be in line with the requirements of standardization of processes, a key tenet of Business Process Re-engineering.
- g) Building Regulation module is being implemented separately by the Department. Supplier shall integrate this module with proposed solution as per Purchaser's requirements to be identified during design phase.

7.4 Processes behind Functions & Services

A Service-oriented Information Architecture demands that the process components be available as reusable objects. Following shall be the different types of processes in the envisaged system:

- a) Core Processes: Core Processes are those that can be considered as specific cases of more generic processes. For example, issue of a Certificate as a core process can be applicable to a TS1 Certificate, each of which could be seen as specific instances of the same Core Process. Following shall be the Core Processes:

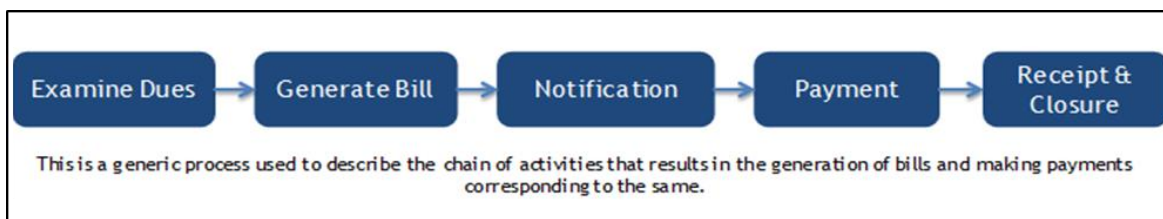
i. Issue of Certificates



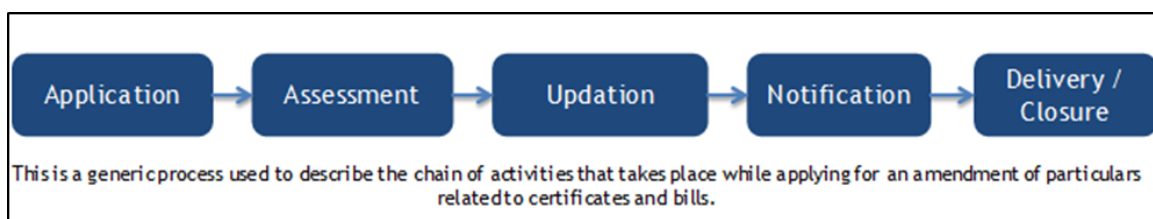
ii. Action on a Report



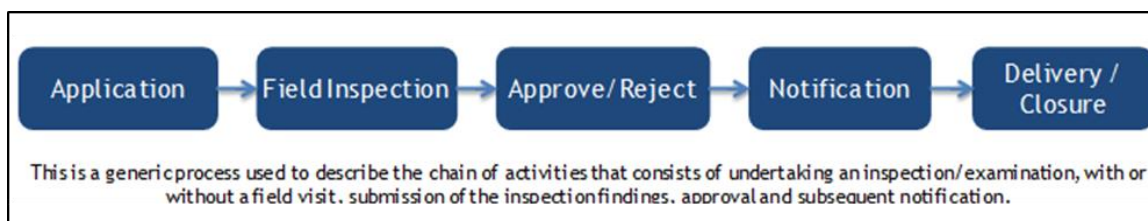
iii. Bill Generation & Payments



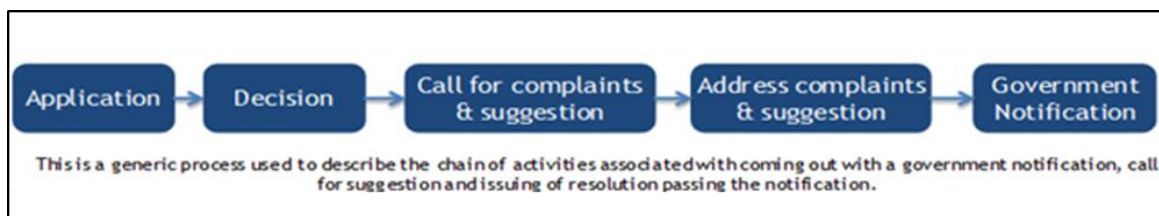
iv. Amendment & Correction



v. Inspection & Approval



vi. Issue of Government Notification



- b) Custom Processes: These are completely specific to the service or the function to which they relate. For example, the issue and return of books is a process that is completely specific to service which it relates to. Custom Processes are those that are specific processes related to services and functions and have limited re-usability.
- c) Common Processes: Common Processes are those that are same across multiple entities. For example personnel management processes that are followed will be same across all ULB entities under consideration. Common Processes are standard processes and are applicable across multiple departments without any significant change in their steps.

The following table summarizes what has been discussed above and presents the linkage between the different systems, modules, services and processes.

S.No.	Functional Area	Related Services	Common Sub-Processes
Corporations, Councils & Nagar Panchayats			
1.	Birth/Death	Registration of Birth	Issue of Certificates
		Registration of Death	Issue of Certificates
		Issuance of Birth Certificate	Issue of Certificates
		Issuance of Death Certificate	Issue of Certificates
		Name correction in Birth Certificates	Amendment & Correction
		Name correction in Death certificate	Amendment & Correction

S.No.	Functional Area	Related Services	Common Sub-Processes
		Late Registration of Birth	Inspection & Approval
		Late Registration of Death	Inspection & Approval
		Name Entry for Birth Registration	Inspection & Approval
2.	Water Supply & Sewerage	New Water Connection	Inspection & Approval
		New Sewerage Connection	Inspection & Approval
		Water reconnection	Inspection & Approval
		Sewerage reconnection	Inspection & Approval
		Water Disconnection	Inspection & Approval
		Sewerage Disconnection	Inspection & Approval
		Payment of Water & Sewerage Bill	Bill Generation & Payments
		Change of Title in Water & Sewerage Bill	Amendment & Correction
		Assessment of Disposal Charges	Amendment & Correction
		Water & Sewerage Bill Amendment	Amendment & Correction
3.	Licenses	License for Commercial Unit	Issue of Certificates
		License for erecting Communication Tower	Issue of Certificates
		Annual Fee for Communication Towers	Bill Generation & Payments
		Issue of License for a Slaughterhouse	Issue of Certificates
		Issue of License for a Mule Cart	Issue of Certificates
		Issue of License for a Rickshaw / Rickshaw Driver	Issue of Certificates
4.	Health & Sanitation	Challan for unauthorized dumping of dirt	Action on a Report
		Lifting of Garbage	Action on a Report

S.No.	Functional Area	Related Services	Common Sub-Processes
		Spray / Fogging for Prevention of Diseases	Action on a Report
		Penalty for Stray Cattle	Action on a Report
		Sterilization of Stray Dogs	Action on a Report
		Appointment of Vendors for Solid Waste	Custom Process
		Monitoring performance of the Vendors	Action on a Report
5.	Fire Services	Conducting Fire Rescue operations	Custom Process
		Issuance of Fire Call Report	Inspection & Approval
		Issuance of NOC for Fire Safety	Issue of Certificates
6.	Rent, Lease & Tahebazari	Information on properties available for rent	Custom Process
		Payment of Rent and Lease	Inspection & Approval
		Removal of Temporary Encroachment	Custom Process
		Collection of Tahebazari Fees	Inspection & Approval
7.	Transport	Issue of Pass for Buses operated by the ULBs	Issue of Certificates
		Fleet Management	Custom Process
8.	Library Management	Issue of Library Membership Card	Issue of Certificates
		Information on books available in Library	Custom Process
		Issue & Return of Books	Custom Process
9.	Plantations and Parks	Setting up new Parks / Plantations	Custom Process
		Management of existing Parks	Custom Process
10.		Approval for Hoardings on Private Sites	Inspection & Approval

S.No.	Functional Area	Related Services	Common Sub-Processes
	Advertisements & Hoardings	Information on Sites available for Hoardings	Custom Process
		Contracting / renting of Govt. Sites	Custom Process
11.	Verification	Verification of Widows / Elderly / Handicapped	Inspection & Approval
12.	Works Management	Estimating and tendering for development works	Custom Process
		Payment of development work	Inspection & Approval
13.	Property Tax	Assigning a Unique ID to each Property	Inspection & Approval
		Assessment and collection of Property Tax	Bill Generation & Payments
		Issuance of TS-1 Certificate	Issue of Certificates
Improvement Trust			
14.	Land Acquisition	Land Acquisition Process	Custom Process
		Approval of Enhanced Compensation	Inspection & Approval
		Approval of Development Schemes	Inspection & Approval
15.	Sale of Plots / Flats	Information regarding available Plots/ Flats	Custom Process
		Draw of Lots	Custom Process
		Conducting of Auction	Custom Process
		Refund of Earnest Money	Custom Process
		Finalization of Sale Agreement	Inspection & Approval
		Payment of Regular Installment	Custom Process
		Payment from Defaulters	Custom Process
		Issuance of Possession Letters	Issue of Certificates
		Issuance of NOC for allotted plots	Issue of Certificates

S.No.	Functional Area	Related Services	Common Sub-Processes
		Finalization of Sale Deed	Custom Process
16.	Property Management	Sanction of Building Plan	Inspection & Approval
		Transfer of Property	Custom Process
		Permission for Mortgage of Property	Inspection & Approval
17.	Works Management	Estimating and tendering for development works	Custom Process
		Payment of development work	Inspection & Approval
18.	Water Supply and Sewerage	sanction of water/sewerage connection	Inspection & Approval
Administrative Functions at ULBs			
19.	Secretarial Functions	Executive Management of Meetings	Custom Process
		Preparation of Resolutions	Custom Process
		Maintenance of Records for Business Matters	Custom Process
20.	Legal Matters	Handling of court cases	Custom Process
21.	RTI	Supply of information under RTI Act	Custom Process
22.	RTS	Supply of information under RTS Act	Custom Process
23.	MIS	Dashboard & MIS at various level	Custom Process
24.	Double-Entry Accounting	Entry of collections into Account books	Custom Process
		Entry of expenditure of ULBs	Custom Process
25.	Budget	Budget Preparation	Custom Process
26.	Employee Services	Promotion of Staff	Action on a Report
		Transfer of Staff	Action on a Report
		Sanction process of the Leaves	Inspection & Approval

S.No.	Functional Area	Related Services	Common Sub-Processes
		Assured Career Progress Scheme	Custom Process
		Employment in case of the death	Action on a Report
		Recruitment of Staff	Action on a Report
		Punishment of Staff	Action on a Report
		Maintenance of Annual Confidentiality Report	Custom Process
27.	Payroll & Pension	Payment of Salary	Custom Process
		Sanction of Staff Retirement Benefits (Pension)	Action on a Report
Complaints & Grievances			
28.	Complaint/Grievance	Resolution of Complaints & Grievances	Custom Process
Management Functions at Head Quarter & Regional Deputy Director Office			
29.	Head Quarter	Approval of resolution of Municipal Councils	Inspection & Approval
		Technical Sanction of Project Estimates at ULBs	Inspection & Approval
		Implementation & Monitoring of GoI sanctioned / State sanctioned project	Custom Process
		Appointment of staff of ULBs / Dept.	Action on a Report
		Promotion of staff of ULBs / Dept.	Action on a Report
		Leave and NOC for Passport / foreign travel, etc.	Inspection & Approval
		Technical sanction of plan by CTP	Inspection & Approval
		Complaints and disciplinary actions on ULB staff	Action on a Report
		Fund withdrawal and Distribution	Custom Process
		Preparing response and attending court cases	Custom Process

S.No.	Functional Area	Related Services	Common Sub-Processes
		Election to notify president and members	Custom Process
		Approval of Resolutions and other matters	Inspection & Approval
		Establishment works of ULBs	Inspection & Approval
		Amendment / Relaxation of building bye laws / TP Schemes / Change of land use	Amendment & Correction
		Amendment of Acts, Rules, building bye laws of corporations	Amendment & Correction
		Facilities and powers of Mayors, Senior Deputy Mayor, Deputy Mayor and Councilors	Custom Process
		Approval of schemes/Plots/Reserve Price/Resolutions	Inspection & Approval
		Notification of new development schemes	Government Notification
		NOC from FCR for new schemes	Inspection & Approval
		Permission for Issuing allotment letter/ Confirmation of draw/ auction	Inspection & Approval
		Change of land use (Residential to commercial)	Inspection & Approval
		Waiving of non-construction fees (NCF) of plots	Inspection & Approval
		Maintenance of information for Court cases	Custom Process
		Providing Answers to the Questions / Queries raised in the Vidhan Sabha	Custom Process
		Record keeping of files	Custom Process
		Complaints & actions against President, VP, Councilors	Custom Process
		Approval of Policies of MC matter	Inspection & Approval
		Approval of TP schemes	Inspection & Approval
		Appellate Authority of staff of MC and NP	Custom Process
		Meetings-Preparation and Participation	Custom Process

S.No.	Functional Area	Related Services	Common Sub-Processes
		RTI Coordination	Custom Process
		RTS Coordination	Custom Process
		Coordination for training	Custom Process
		Rent Act Constitution implementation and amendment	Custom Process
		Establishment work of Directorates and DDRs	Inspection & Approval
		Establishment work of sewerage board	Inspection & Approval
		Providing Information for FM Speech	Custom Process
		Statistics and administrative report	Custom Process
		Land acquisition for STP/Solid Waste	Custom Process
		Approval of installation of tube well in committees	Inspection & Approval
		Enhancements/Exemption/Rebate of water and sewerage board charges	Inspection & Approval
		Empanelment of lawyers	Custom Process
		Audit and accounts of sewerage board	Custom Process
		Sanction of project fund from State Govt.	Inspection & Approval
		Coordination of other works of LG department	Inspection & Approval
30.	Regional Deputy Director Office	Approval of Budget Estimates of ULBs	Inspection & Approval
		Approval of minutes of the meeting of ULBs	Inspection & Approval
		Administrative Approval of Estimates of ULBs	Inspection & Approval
		Approval under Section 52(2)(L) of Punjab Municipal Act 1911	Inspection & Approval
		Recovery of arrears of ULBs	Custom Process
		Approval of Bye Laws of ULBs	Inspection & Approval
		Approval / disbursement of Pension	Inspection & Approval

S.No.	Functional Area	Related Services	Common Sub-Processes
		Approval of Medical Reimbursement	Inspection & Approval
		Recording of the Annual Confidential Reports of the employees (Provincialized Cadre) of ULBs	Custom Process
		Functions of Collector under PP Act, 1973	Custom Process

d) Birth & Death Module

Birth & Death” module, which is already developed under e-district project, shall be used by Supplier under this project for Department of Local Govt. including ensuring its service level performances.

e-District is one of the State Mission Mode Project envisioned under the National e-Governance Plan (NeGP) of Ministry of Electronics & Information Technology (MeitY), Government of India. The project focuses on complete backend workflow computerization of various citizen centric services being delivered at District & sub-district level. In Punjab, Punjab State e-Governance Society (PSeGS) is the State Designated Agency (SDA) for the implementation of the Project in Punjab. The project implementation has been planned in two phases. The first phase was the Pilot implementation, which has already been implemented successfully in two Districts namely i.e. Kapurthala & Shahid Bhagat Singh Nagar (Nawanshahr). At present, the Local Area Networking, IT Infrastructure deployment, Bandwidth Connectivity, training of field officials is in progress. The service Go-Live is expected shortly. For more details about e-district project and birth & death module please refer Attachment-9 of this volume of RFP.

PSeGS has selected M/s HP India Sales Pvt. Ltd. as System Integrator for implementation of the e-district project in the State. Data digitization of historical data from 2003 to 2013 is the responsibility of e-district vendor and digitized data will be provided to Department of Local Govt.

DoGR/e-district vendor shall handover the birth & death module with source code, System Requirement Specifications, design documents and other relevant documents and data pertaining to this module to Supplier under this project free of cost for its integration with overall solution.

Supplier shall ensure the complete takeover of this module along with all required documents & data to ensure its smooth implementation.

Post-handover of birth & death module, Supplier shall assess the module, technology used, integration compatibility etc. based on the RFP requirements. Based on the assessment, Supplier may use this module

and integrate it with overall solution or re-develop or customize it to meet Functional Requirements as specified in RFP.

Supplier shall also ensure to incorporate any new functionality as finalized during study & design phase of this project. Supplier shall ensure that the integrated solution must meet all RFP requirements including Service Level Agreements.

Supplier shall be responsible for migrating entire data, received from DoGR/e-district vendor including digitized data into database of this project of Department of Local Government.

Data digitization of historical data, pertaining to period from 1989 to 2002 and 2014 to date of go-Live of birth and death related services, will also be responsibility of the Supplier under this project of Department of Local Govt.

Supplier shall provide operation & maintenance support for this module for entire contract duration of this project.

7.5 Benchmarks & Timelines for delivery of G2C and G2B Services

- a) Overall Timelines refer to the time (upper limit) within which the services shall be delivered. The same should be achieved in a phased manner as per the Implementation Plan.
- b) Time Limits for ULBs depict the time which would be required by the ULBs for processing the Service Requests and Time Limit for the Supplier is the difference between Timelines for Service Delivery and the Time Limit for ULB.
- c) During the execution of the Project further process refinements may also lead to changes in the timelines that have been specified. During the execution of the Project the Supplier must also be prepared to revisit the service delivery parameters and effect any improvements that emerge.
- d) Overall timelines of delivery of services will also adhere to Right to Service (RTS) time-lines as defined by Government of Punjab.

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
1.	Birth/Death	Portal: 24 x 7 Access to the System: 24 x 7 Working hours of Service Delivery Center established by State Government	Registration of Birth and issuance of Birth Certificate	2 days	1.5 days	0.5 day
			Registration of Death and issue of Death Certificate	2 days	1.5 days	0.5 day
			Name correction in Birth Certificates	3 days	2 days	1 day
			Name correction in Death certificate	3 days	2 days	1 day
			Late Registration of Birth	Within 1 year: 4 days Otherwise: 15 days	Within 1 year: 3 days Otherwise: 14 days	1 day
			Late Registration of Death	4 days	3 days	1 day
			Name Entry for Birth Registration	2 days	1.5 days	0.5 day

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
2.	Water Supply & Sewerage	100% automatic generation of utility bills	Sanction and Installation of New Water Connection	5 days	4 days	1 day
		Automatic escalation of events to appropriate authority on non-payment of utility bills:	Sanction and Installation of New Sewerage Connection	5 days	4 days	1 day
		1 st escalation within 24 hours after the time limit is over,	Sanction and Installation of Water reconnection	2 days	1.5 days	0.5 day
		2 nd after 6 working days of 1 st ,	Sanction and Installation of Sewerage reconnection	2 days	1.5 days	0.5 day
		3 rd after 12 working days of 1 st	Approval of Water Disconnection	2 days	1.5 days	0.5 day
		Portal / Mobile / ECS: 24 x 7	Approval of Sewerage Disconnection	2 days	1.5 days	0.5 day
		Working hours of Service Delivery Center established by State Government	Payment of Water & Sewerage Bill	15 minutes	No ULB intervention	15 minutes
		100% availability of updated status of all applications online with multiple search options	Change of Title in Water & Sewerage Bill	2 days	1.5 days	0.5 day
			Assessment of Disposal Charges	5 days	4 days	1 day

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
			Water & Sewerage Bill Amendment	2 days	1.5 days	0.5 day
3.	Licenses	100% automatic generation of receipt number Automatic escalation of status of pending license application to appropriate authority : 1 st escalation within 24 hours after crossing specified time limit for ULB processing, 2 nd after 6 working days of 1 st , 3 rd after 10 working days of 1 st 100% Automatic generation of demand notice for renewal of license	Issue of License for Commercial Unit	5 days	4 days	1 day
			Issue of License for erecting Communication Tower	5 days	4 days	1 day
			Collection of Annual Fee for Communication Towers	5 days	4 days	1 day
			Issue of License for a Slaughterhouse	5 days	4 days	1 day
			Issue of License for a Mule Cart	2 days	1.5 days	0.5 day
			Issue of License for a Rickshaw	2 days	1.5 days	0.5 day
			Issue of License for a Rickshaw Driver	2 days	1.5 days	0.5 day
			Issue of Completion Certificate	5 days	4 days	1 day

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
			Sanction of Change of Land Use	45 days	43 days	2 days
			Approval of Additional Construction	5 days	4 days	1 day
			Regularization of Unauthorized Construction	5 days	4 days	1 day
			Approval of Town Planning Scheme	45 days	43 days	2 days
			Public Street Declaration	45 days	43 days	2 days
4.	Health & Sanitation	---	Spray / Fogging for Prevention of Diseases	2 days (in case of a complaint)	1.5 days	0.5 day

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
			Lifting of Garbage	2 days (in case of a complaint)	1.5 days	0.5 day
5.	Fire Services	---	Issuance of Fire Call Report	1 day	6 hours	2 hours
			Issuance of NOC for Fire Safety	4 days	3 days	1 day
6.	Rent, Lease & Tahebazari	---	Information regarding properties available for rent	In Real-time	NA	In Real-time
			Payment of Rent and Lease	15 minutes	No ULB intervention	15 minutes
			Removal of Temporary Encroachment	2 days (in case of a complaint)	1.5 days	0.5 day
			Collection of Tahebazari Fees	15 minutes	No ULB intervention	15 minutes
7.	Transport	---	Issue of Pass for Buses operated by the ULBs	15 minutes	No ULB intervention	15 minutes
8.	Library Management	---	Issue of Library Membership Card	30 minutes	No ULB intervention	30 minutes

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
			Information regarding books available in the Library	In Real-time	NA	In Real-time
			Issue & Return of Books	In Real-time	NA	In Real-time
9.	Advertisements & Hoardings	---	Approval for Hoardings / Adv. Boards on Private Sites	3 days	2 days	1 day
			Information regarding Govt. Sites available for Hoardings	In Real-time	NA	In Real-time
			Contracting / renting of Govt. Sites	3 days	2 days	1 day
10.	Verification Services	---	Verification of Widows / Dependents / Elderly / Handicapped	3 days	2 days	1 day
11.	Works Management	---	Estimating and tendering for development works	45 days	42 days	3 day
			Payment of development work	15 days	14 days	1 day
12.	Ticket Sales	---	Ticket Sale and Challan Entry	In Real-time	NA	In Real-time
13.	Land Acquisition	---	Approval of Enhanced Compensation	15 days	14 days	1 day
			Information regarding available Plots/ Flats	In Real-time	NA	In Real-time

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
14.	Sale of Plots / Flats	---	Draw of Lots / conducting auction / refund of EMD	90 days	85 days	5 days
			Finalization of Sale Agreement	7 days	6 days	1 day
			Payment of Regular Installment	15 minutes	No ULB intervention	15 minutes
			Payment from Defaulters	2 days	1.5 days	0.5 day
			Issuance of Possession Letters	15 days	14 days	1 day
			Issuance of NOC for allotted plots	3 days	2.5 days	0.5 day
			Finalization of Sale Deed	7 days	6 days	1 day
15.	Property Management at Improvement Trusts	---	Transfer of Property	15 days	14 days	1 day
			Permission for Mortgage of Property	7 days	6 days	1 day
16.	Complaints & Grievances	Resolution of all kinds of complaints as per SLA mentioned in the RFP 100% adherence to the response time as per citizen	Resolution of Complaints & Grievances	3 days	2.5 days	0.5 day

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
		charter / statutes of grievance resolution Automatic escalation of events to appropriate authority on non-resolution: 1 st escalation within 24 hours after crossing specified time limit for ULB, 2 nd after 6 working days of 1 st , 3 rd after 10 working days of 1 st 100% public disclosure of the grievances not resolved Portal / Mobile: 24 x 7 Working hours of Sewa Kendras established by State Government				
17.	RTI and RTS	---	Supply of information under RTI / RTS Act	7 days	6 days	1 day

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
18.	Property Tax	100% automatic generation of demand notice	Assessment of Property Tax	7 days	6 days	1 day
		100% updation before start of assessment year				
		Non-regularized Properties: 100% updation on the date of regularization				
		Automatic escalation of events on default to appropriate authority: 1 st escalation within 24 hours after time limit is over, 2 nd after 15 working days of 1 st escalation, 3 rd after 45 working days of 1 st	Collection of Property Tax	15 minutes	No ULB intervention	15 minutes
		Portal / Mobile: 24 x 7				

#	Functional Area	Overall Benchmarks	Services	Timelines		
				Overall (A)	For ULBs (B)	For Supplier C = (A – B)
		Working hours of Sewa Kendras established by State Government 100% availability of updated status of all applications online with multiple search options	Issuance of T.S. 1 Certificate	1 day	6 hours	2 hours

7.6 Benchmarks & Timelines for Management Functions

- a) For the Management Functions listed in this Volume of the RFP, the Supplier shall ensure that updation of relevant data takes place in Real-time.
- b) Overall Benchmarks pertaining to Accounts & Finance functions are as below:
 - i. 100% Updation of ledgers with the receipt of taxes and charges on the same day
 - ii. 100% posting of payments to vendors / Employees to be posted on the same day
 - iii. 100% updation of Receivables online on the same day on which demand is raised
 - iv. 100% updation of the payable on the same day of receipt of goods / services
 - v. 100% generation of automated alerts for delayed payments and receipts
 - vi. 100% reconciliation of subsidiary accounts (monthly) by the 10th day of the subsequent month
 - vii. 100% closure of books / chart of accounts within 30 days of the end of the financial year
- c) Overall Benchmarks pertaining to Establishment Matters are as below:
 - i. 100% coverage in terms of availability of Login Facility to employees
 - ii. 100% online availability of Employee Related updated information
 - iii. 100% online processing of dues within 7 days

8. Technology Architecture & Requirements

8.1 Overview

- a) Supplier shall design the deployment architecture considering scalability, reliability, security, business continuity, optimum performance of the entire solution and based on other requirements as mentioned in the RFP. Minimum Bill of Materials and their minimum specifications are given in Attachment-4 and 5 to this Volume of RFP respectively.
- b) Considering changes in the type of ULBs (e.g. when a Council becomes a Corporation, etc.), including creation of new ULBs and addition of new process, it will be the Supplier's responsibility to develop the new system in such a manner that it is able to accommodate these changes with the help of the User Interfaces alone.
- c) The deployment architecture to be proposed by Bidder should deliberate upon the following key design considerations:
 - i. Multi-tenant Environment: Considering the federal structure and independence of ULBs, the Solution should be designed in a way to provide independence to ULBs to manage their data and environment. There will be a single portal for all the ULBs where the user will have a drop down list to select the respective ULB. After selecting the name of the ULB they will be automatically directed to the ULB specific portal. The ULB specific portal will be customized based on ULB's requirement. Individual access right will be provided based on the requirement. This environment may be based on model driven approach.
 - ii. Service Oriented Architecture (SOA): The Solution must conform to an application development and integration methodology based on a Service Oriented Architecture (SOA), and the integration methodology should be based on XML/OpenXML/XINS/SOAP/ WSDL and Web enabled services technologies. SOA should comply with the OGPL (Open Government Platform) standards defined by DeitY, GoI. The solution must have an orchestrated sequence of messaging, routing, processing, and transformation events capable of processing the rich (XML/OpenXML/XINS/SOAP/ WSDL) documents. The solution must be architected to ensure that current and new applications can be seamlessly integrated (through an application integration solution using XML/OpenXML/XINS/SOAP/ WSDL) within its architecture with minimal impact and changes. Care should be taken to represent the information as metadata in standard XML/OpenXML/XINS/SOAP/ WSDL format. The solution developed should have native Indian language support and should leverage the Unicode support available within the client Operating System.
 - iii. Interoperability Standards: Keeping in view the evolving trends of interoperability, especially the possibility that the Punjab Local Government system would become the focal point of delivery of several sets of services to be offered G2C and G2B, the Punjab Local Government solution should be built on Open Standards. This will enable easy integration and provision of large portfolio of services to citizens with incremental effort. Core components of an open-standards-based interoperability stack are shown below.

Interop Stack	Universal Service Interop Protocols
	Universal Description, Discovery, Integration (UDDI)
	Simple Object Access Protocol (SOAP)
	Extensible Markup Language (XML)
	Common Internet Protocols (HTTP, TCP/IP)

- iv. Scalability: One of the fundamental requirements of Punjab Local Government Architecture is its scalability. The architecture should be proven to be highly scalable and capable of delivering high-performance as and when transaction volumes increase. It is required that application and deployment architecture should provide for Scale-Up and Scale out on Application & Web Servers, Database Servers, Integration Servers, and all other solution components. Scalability of the solution for Punjab Local Government is to be achieved at least along the Dimensions described below:
- Scalability in terms of the volumes of transactions handled: This translates to the facility to enhance the hardware, software and network capacities to maintain the performance levels always in tune with the SLA metrics.
 - Scalability in terms of addition of new services of an existing department: This translates to seamless and effortless integration with the backend application such that new citizen services can be added with relative ease at the SDC level and can be deployed in all the Sewa Kendras simultaneously.
 - Scalability in terms of addition of new departments: This translates to seamless integration with heterogeneous systems at the backend with relative ease of deployment of the applications and services, maintaining the common look and feel and functionality at the front-end.
 - Scalability in terms of addition of new Sewa Kendras: It may be required to increase the number of Sewa Kendras and at the same time provide adequate coverage in the Punjab.
 - Scalability in terms of addition of new channels of delivery: This translates to designing the systems suitably to provide services through other delivery channels like the mobile devices, PDAs, DTV and other devices.
- v. Security: The system for Punjab Local Government should be highly secure, considering that it is intended to handle sensitive applications relating to citizen services. The overarching security considerations are described below.
- The application and database security should integrate with platform and last mile stone security.
 - The solution should provide for maintaining an audit trail of all the transactions.
 - The security services used to protect the information infrastructure shall include: Identification, authorization, Authentication, Access Control, Administration and Audit and support for industry standard protocols like Kerberos 5.x/ NIS/LDAP/tn3270 X, etc.
 - The solution should provide Single-Sign-On features with password encryption and capability to enforce changing the passwords at system-defined intervals.

- The solution should handle errors due to communication failure, transaction leakages, hardware failure, etc. and roll back the changes maintaining the transaction consistency.
 - The solution should ensure guaranteed once only delivery, message routing, queuing and load balancing features and optimize both data-level and process-level integration. Specific capabilities of such a solution should include, but not be limited to, a robust and secure messaging infrastructure, graphical data transformation capability, automated business process integration (both internal and cross-enterprise), workflow management, and powerful business-to-business transaction capability.
 - Punjab Local Government security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
 - Punjab Local Government System will be audited by a third party at the stage of acceptance testing stage and periodically thereafter, at least once a year, to ensure that the security systems are intact and that the security policies are strictly being enforced.
- vi. Portability: The Solution components should support portability and shall be interoperable with multiple platforms like Unix, Linux & Windows.
- vii. Integrated Directory-enabled Design
- The solution should be based on an Industry-standard NIS/LDAP Directory service, for registration and storage of user profile information for authentication purposes and seamlessly facilitates integration of multiple Sewa Kendras & ULBs. The System administrator should have the flexibility of administering the entire directory from a central location using a browser/console.
 - Single Domain
 - Single point monitoring of entire network for monitoring of congestion, server downtime, application downtime etc.
 - Single point administration and delegated administration of centers and users
 - Inbuilt integration with PKI infrastructure. PKI, should be used for the purpose of integrity (digital signing) and confidentiality (encryption). HSM will offload all the digital signing and encryption requirements from the server.
 - The user authentication should be capable of providing in-built support for Smart Card / Aadhaar Card/ Biometric devices so as to enable the use of such devices by the system administrators, counter operators and managerial-level users of ULBs, Participating Departments, Punjab Local Government and the selected Supplier.
- viii. Modular Design: The application for Punjab Local Government should be developed in a modular fashion to enable ease of extension in order to provide a large number of services in the G2C and G2B domains. The following illustrative generic modules are suggested in this regard, for the guidance of the Suppliers:
- Administration module: Through this module, the system administrator should be able to monitor the provision of services at Sewa Kendras and specifically to create Users providing roles and privileges, monitor Transactions of each department, manage and

monitor the services of each department, manage servers and network connectivity and monitor security breaches and control them in time.

- Audit Trail Module: The application should have in-built mechanisms for enforcing security of data. Auditing of transactions is to be provided in this context. Sensitive information should have transaction logs, which will capture the pre-image and post-image of data modifications. Information regarding the users carrying out these sensitive transactions should be captured to ensure accountability at every process level. This module is to be used to monitor all the transactions done by the application. It is also used to manage any transaction conflicts with the departments. It should provide detailed transaction information, Daily/ weekly/ monthly audit reports and Service/ Department based audit reports.
- Reports & Alerts Module: This module should provide various reports and alerts as required by the Punjab Local Government. The module should be available for report generation at all the levels appropriately. These reports should be available on a real-time basis and they include Hourly/Daily/Weekly/Monthly transaction/collection by center, Service collections by center, Daily Bank reconciliation statement, Daily Service/Department vs. Bank account statement, Transaction based alerts and Bank reconciliation alerts

ix. Database Design, Data Transmission, and Data Confidentiality Requirements

- Solution should maintain standard data definitions (Metadata) for data elements.
- Solution should transform data into required format of the target application.
- Solution should intelligently and securely route the necessary information to required location and applications. The complexity of the application integration and messaging should be transparent to the users.
- Solution should be able to track real docs such as bills using XML/ OpenXML/ XINS/ SOAP/ WSDL schema.
- Ownership of Data & Information: The ownership of data and information accessed, generated and stored within the Punjab Local Government system in the course of providing the services to the various stakeholders, shall exclusively vest with the respective ULBs. The selected Supplier is only a trusted custodian of such data and information. To this extent, the selected Supplier should design the database systems so as to maintain the confidentiality of the data and information, deny access to any person or organization that is not specifically authorized by Purchaser to have such an access, take all possible steps to prevent unauthorized access to such data and information, maintain the safety and security of such data and information at all times, handover all transaction-related data and information from time to time as required by Purchaser, including the tools to process such data and information, to Purchaser at the termination of the Agreement and comply with all the legal requirements to protect the privacy and confidentiality of the information, required by the general laws in this regard or the specific terms of agreement relating to this.

8.2 Solution Architecture

- a) This section gives a brief introduction of overall solution architecture. The details of each component are described below. The figure given below depicts the indicative multi-tiered or layered Solution architecture for the Punjab Local Government Project that is built with the key principles of modularity, scalability and manageability. Each layer provides a distinct set of functionalities that is independent of the functionalities provided by the other layers. Individual layers and their functionalities are detailed below.



- i. **CLIENT/ ACCESS LAYER:** The client layer will consist of the required software components to be used by the end user as the front-end to access and use the underlying business applications for carrying out the required business activity. Typically the client layer will be a Personal Computer (PC) running a desktop /Laptop operating system. The component to access the underlying business applications will be a Web browser such as Opera/Internet Explorer /Midori/ Mozilla Firefox or any other commonly prevalent web browser. The client desktops /Laptop will be connected to the servers hosting the business applications either locally within the premises on a LAN (Local Area Network) or over longer distances on a WAN (Wide Area Network)/ VPN.
- ii. **PRESENTATION LAYER:** Those software components that render the results of the business applications in a format that will be viewable by the end user form the Presentation layer components which will be typically web servers and Portal servers. There can be multiple web or portal servers serving different categories of users – Intranet portals or web servers which serve users within an Intranet and Internet portals or web servers which serve the general Internet users.
- iii. **BUSINESS APPLICATIONS LAYER:** Also called the Applications layer, this one will comprise of all relevant business applications of the Punjab Local Government. This container framework and its associated components will form the "Technology stack" for the business components and they together will provide the necessary technology infrastructure to run the business applications. Typically this will consist of, an Application server, Rules engine, Workflow engine, Content Manager, etc.
- iv. **INTEGRATION LAYER:** This layer comprises of systems and software components that will integrate disparate applications to provide a complete business flow. Components deployed in

the Integration layer will aid in smooth end-to-end data transfer and there by complete the business process. The communication between the disparate applications will happen by passing data in the form of synchronous or asynchronous messages. Integration layer is also called "Middleware".

- v. **DATA BASE LAYER:** The data layer is where all business critical data are stored in the form of databases and files. This layer will consist typically of the Database servers. Once the data is processed in the application layer, the same will be stored permanently in this layer. Since this layer contains data which is critically important to the business of Punjab Local Government, it should be secure and direct access to servers on this layer should be highly restricted to allow only authorized users.
- vi. **INFRASTRUCTURE LAYER:** The infrastructure layer will consist of all the physical systems that form part of the entire solution. They will comprise servers, storage subsystems, network devices, communication links, etc. In addition, this layer will also consist of software components that provide Directory services, Mail and messaging services, Document Management services, etc., in general.
- vii. **SECURITY LAYER:** Multitier security components form part of this layer. This will include Internet and Intranet firewalls, Network IDS/IPS devices, 2-factor authentication systems, sign-on systems, etc. Components in this layer will encompass and govern all other layers.
- viii. **MANAGEMENT LAYER:** Like the Security layer, the Management layer will also encompass and govern all other layers. It will consist of software components and systems that will be required to manage and monitor all components deployed in each of the layers described above. It can be used to manage and monitor both software and hardware components. Thresholds and limits will be set for those components that are required to be monitored and the Management layer components continuously monitor and alert the administrators of any changes so that immediate corrective actions can be taken. The components deployed in this layer will help to correctly assess and monitor the Service levels of the business systems (hardware and software) that will be deployed for Punjab Local Government.

b) The representative Overall Solution Architecture of the new system is shown below:

- i. **Enterprise Portal:** Enterprise Portal will provide a secure unified access point in the form of a web-based user interface, and will be designed to aggregate and personalize information through application-specific portlets/ webparts.
- ii. **Application Modules:** The various application modules and their Functional Requirement Specifications are given in Attachment-2 to this Volume of the RFP.
- iii. **Secure Gateway Service:** This will include Web Gateway, WebSEAL, EWS, , and SMTP Gateway with authentication options including SSO with Active Directory or eDirectory and even using captive portal for shared systems or mobile devices.. The role of the Gateway would be to

- provide a focal point for processing outgoing and incoming requests for web application services to and from external entities. For outgoing requests, the gateway would be responsible for receiving requests from the application, forwarding them to third parties systems and receiving and disposing of the response. For incoming requests, the gateway would be responsible for receiving requests from external systems, invoking the necessary Adaptors to perform the business logic, and finally for composing a response and sending it back to the requesting system. Supplier should compliance norms of cyber security as per guidelines of GOI and Punjab state IT /Cyber Security Policy.
- iv. DNS Services: This service should support features like: support conditional DNS forwarders e.g. forwarding based on a DNS Domain name in the query, allow clients to dynamically update resource records secure and non-secure, Support incremental zone transfer between servers, provide security features like access control list, support new resource record (RR) types like service location (SRV), etc. and to support Round robin on all resource record (RR) types.
 - v. DHCP Services: DHCP would be assisting the System administrators for dynamic IP allocation to devices/ users. Furthermore, the key users, who would be connecting using remote access, would be requiring a valid IP address after successful authentication.
 - vi. Directory Services: These services will be directories are designed with namespaces as Subscribers, Services, Devices, Entitlements, Preferences, Content and so on. Directory Services design process is highly related to Identity management, register, authenticate and manage users and their security privileges. These services will authenticate the Punjab Local Government users and find out user specific privileges. LDAP (Lightweight Directory Access Protocol) is an Internet protocol that Punjab Local Government portal users use to look up information from a server. User password validation will be done from LDAP. Authentication should be conducted using the standards based LDAP meta-directory server. The user directory capable of providing a unified view of all user profiles. Directory services shall be able to define centralized authentication & authorization mechanisms for all network users.
 - vii. Web Application Services: The Web Application Services would be a container to manage the presentation and application logic. It will provide transactional integrity, scalability and availability services. In addition it manages the session, the requests and responses to and from its clients and resources. Supplier should compliance of GOI for web application Services and design.
 - viii. Indexing & Search Services: This tool would be used for indexing and searching all the repositories of knowledge repository maintained across the portal infrastructure.
 - ix. Workflow: SOA (Service Oriented Architecture) Infrastructure would provide work-flow functionality and provide integration with SMS, Payment gateway and email services to the concerned stakeholders.
 - x. MIS Reporting: The following types of reports, but not limited to, are required to be generated from this sub module. The report should be generated in standard formats like PDF, XLS, DOC, DOCX, PPTX, XLSX etc.

- Fixed Format Reports: Application should provide robust reporting capabilities. Application should publish reports using tools such as Microsoft Office, open office or Adobe Acrobat and the publishing engine can generate output in multiple formats including PDF, HTML, DOCX, PPTX, XLSX and similar type of formats. The output can also be delivered through email or can be printed or faxed.
 - Ad-hoc Reports: Application should provide business users with ad hoc query & analysis capability. Application should create new analyses from scratch or modify existing analyses in dashboard pages. Business users do not need to understand physical data storage to combine data from multiple enterprise information sources intuitively, quickly, & easily. Tools and utilities should be provided to facilitate design layout using Open office/MsOffice/Adobe Acrobat etc.
 - All reports will be required in Punjabi and English language.
- xi. Payment Gateway: The portal would provide the online payment services (for payment of license fee, etc.) through integration with the payment gateways. The portal solution shall support card payments using all the popular debit and credit cards (Visa, Master card etc.), internet banking, other options such as BHIM (Bharat Interface for Money), Paytm, and MobiKwik. Payment Gateway is provided by Purchaser/Department of Government Reforms.
- xii. Digital Certificate/E-Sign Services: The propose solution by bidder should be capable of integrating with digital certificates and/or e-sign. The system should automatically enable/disable with using of RSA/ElGamal/DSA/HMAC protocol with Digital Signature Certificates (DSCs) of employees depending on the current status of each employee namely, fresh appointment / transfer / suspension / leave/ training / retirement etc. The system should accordingly enable DSC only for an 'active' employee. Digital Signatures and/or e-sign shall be procured by Department as & when required.
- xiii. Mailing & Messaging Services: This would be used for sending the alerts as mail message to the registered users of the Punjab Local Government Portal and will be used for messaging and calendaring services. Mail & Messaging solution of Department of Government Reforms (DoGR) shall be used for this project. Supplier shall administer end-user issues in using the related services and coordinate with DoGR.
- xiv. Anti-Virus: Anti-Virus would be required to keep the other servers and application secure from the attack of virus, Trojans, spam, spyware, rootkits, etc. with state-of-the-art anti-malware protection. The advanced scanning engine shall check for these threats. This will also act as a centralized system for updating the virus definitions on all systems.
- xv. In case of Be-spoke solution, supplier shall not use any proprietary technology for any part of solution unless the same was approved by the Purchaser.

8.3 General Requirements from the Portal

- a) Punjab Local Government Portal is intended to provide online services to the urban citizens of Punjab. Promotion of online services would have the twin advantage of reducing the pressure on the Sewa Kendras and also reduce cost of operations to all the stakeholders.

- b) The portal architecture needs to be designed with loosely coupled components making it extensible. The portal services should be deployed as components to have a potential for re-use in launching future services, without disturbing the existing architecture. The services should also have a potential of having multi-channel access/ integration, as the data returned by the components, would be in XML/OpenXML/XINS /SOAP/WSDL format. Supplier shall conform to GIGW (Guidelines for Indian Government Websites) issued by GoI.
- c) Multi-lingual support: The Punjab Local Government portal must support bilingual versions in English and Punjabi. However, the implementation of Punjabi version of the portal and Customer Service Application shall be completed within 6 months. Receipts/Certificate will however have to be both in Punjabi and English from day one. The Punjabi language implementation needs to be based on Unicode standards.
- d) In addition to the above, the major solution components of the Portal shall be:
 - i. Content Management (CM): The portal is the official information & service delivery interface for Punjab Local Government Department to all the stakeholders and the extreme care shall be taken while designing the portal layout, coloring scheme, taxonomy etc. One of the key requirements for the portal is the content management, which would be the Supplier's responsibility and shall be performed using the CM tools and processes to ensure that the content, form and services delivered through portal are adhering to the uniform standards. To summarize, updation of Static Content shall be the responsibility of the System Integrator (SI)/Supplier and the Transaction Content shall get dynamically updated via the envisaged System.
 - ii. Secure dynamic online self-registration for users: The portal must provide for the ability for users to register themselves in the user directory and then be assigned the related privileges / entitlements based on their preferences and eligibility. This facility should also give the user the ability to edit details about themselves, such as username and password. If this facility is used to store sensitive information, this should not be redisplayed in its entirety to the user, once it has been entered.
 - iii. Advanced authentication (including PKI) support: The portal shall support advanced cloud based authentication techniques, along with username/password, such as PKI with X.509vs certificates, OATH compliant OTP tokens.
 - iv. "Single Sign-On" capabilities across services: Single sign-on facility and single user credentials meaning that users can have one user ID and password, or a digital certificate, which they can use for all online public services.
 - v. Common transaction and routing facility ensuring the reliable delivery of documents and messages. This includes both documents between business and citizens and government, as well as the routing of documents between government organizations.

Secure XML/OpenXML/XINS/SOAP/ WSDL messaging facility enabling secure communication between business, citizens and government organizations.

- vi. MIS Reporting: In addition to the requirement described in Para 8.2 c (X); The Portal shall provide an interface to the ULB to obtain the transaction history, summary and detailed reports on daily transactions, pending applications etc. The portal shall provide a dash-board view, employee wise, location-wise, region-wise to assess the performance in terms of number of applications received, number of applications processed, pending etc. MIS report generated from the portal shall act as a decision support system for the Senior officials of the Local Government Department.
- vii. e-FORMS: The size of the e-forms created for delivering the services through portal shall be kept to the minimum so as to suit bandwidth typical to dial-up Internet connections. The form filling should be easy, user friendly and shall avoid common form filling errors (such as, ensuring all mandatory fields are entered, selecting options by checking boxes where applicable, number entry etc.). The portal shall provide Easy-to-use step-by-step guidance to fill the e-Forms in the form of form-wizards. The e-Forms, as required for the services, must support Digital Certificate based signatures issued by the authorized CAs. e-Forms may have the need to be signed digitally by the users, depending on the service. Portal shall provide the printable formats for all the e-Forms and user, upon filling up the details, can obtain the printout of the same. All the e-forms shall have appropriate field level and form level business validations built into it to ensure that scope for incomplete/ inaccurate information is eliminated and the information is captured for all the mandatory fields. e-Forms should support following features:
- The e-Forms shall be of the format XML/OpenXML/XINS/SOAP/WSDL or an equivalent format (that meets the all the requirements as described)
 - The e-Forms must carry a version identifier and System must ensure use of current version of the form by the users.
 - Users must be able to download the e-Forms and fill them at their convenience, without requiring to be connected to the portal.
 - Users must be able to copy the blank e-Forms with / without the filled-in data in any removable computer media (e.g. diskettes, CDs, Memory sticks etc.), as well as transport them using mechanisms such as email and FTP.
 - The e-Forms must be designed to be user-friendly. For example, mandatory fields should be distinctly identifiable; fields that will be filled automatically by the system should be distinctly identifiable, etc.
 - The e-Forms must be supported for use by the stakeholders on all widely used operating systems such as variations / versions of Windows/ Unix/ Linux or any open source environment, etc., preserving the functionality, look and feel of the form. When printed, the e-Form must preserve the appearance as on the screen.
 - The e-Forms must support attachment of multiple documents. Such attachments must be embedded in the e-Form so that they can be copied/ transported/ uploaded/ downloaded seamlessly together.
 - The e-Forms must have facility to allow authorized ULB employees add notes / notations / comments. The facility should allow saving of such notes separately from the e-Form itself; Display of the original e-Form with data should be possible with or without the notes (as per the access privileges applicable).
 - The e-Forms must preserve the position of the notes for accurate display

- Integrity of the original e-Form and its data content must be verifiable using the PKI digital signatures even after notes/ comments/ water marks are added.
- For ensuring full integrity of transaction, one application comprising both data and documents should be treated as one whole package that will be signed digitally and stored in the database
- The e-Forms must support multiple digital signatures/e-sign.
- The Punjabi and English content required for the portal will be the Supplier/SI's responsibility.

e) The portal requirement is only for the eservices for citizen, ULB and suppliers. Currently integration with social media is not part of scope but may be a future requirement. Solution must be capable of integrating with various social media platforms/tools.

8.4 Specific Requirements from the Portal

The Portal should have the following specific functionalities in order to ensure smooth delivery of the services and functioning of the Department:

- a) Service Requests/transactions initiated by the citizens/operators shall be routed to the designated employees of the ULB, based on the defined workflow, for further processing in the system only if:
 - i. The version of the e-Form is correct
 - ii. Pre-Scrutiny rules for respective e-Form are satisfied
 - iii. Digital Signatures/E-sign are valid
 - iv. Necessary fee has been received
- b) ULB employee handling the service request should be able to optionally validate the above.
- c) System shall facilitate automatic routing of work-items/transactions to the respective ULB employees. Such routing of work-items/transactions shall be based on following, at a minimum:
 - i. Automatic allocation of work-items to the employees based on FIFO mechanism
 - ii. The role and authorization defined in the system
 - iii. Availability and status of employees in the system (e.g. work-items shall not be routed to employees who are on leave or whose ids are temporarily or permanently deactivated)
 - iv. Based on the defined work-flow and the designated employees
- d) System shall have the ability to recognize the current version of the e-Form.
- e) Facility to define the workflow for each type of e-Form / service
- f) Facility to validate Digital signatures. The digital certificates associated with the signatures shall be checked against the current Certificate Revocation Lists (CRLs) of the Certificate Authority,
- g) Facility to capture and to provide the workflow in the Sewa Kendras/ULB in a comprehensive manner for all the services. Both predefined and ad hoc workflows shall be provided.
- h) Facility to automatically provide the status of the work item (for those work items created upon arrival of an e-Form) through response to a request from the Sewa Kendras.

- i) Facility to manually create a work-item (by an authorized officer) and assign to an individual.
- j) Facility to add comments / notes / documents to a work-item during processing. It should also be possible for entering profiling information or metadata needs for a particular document (in cases where applicable) as part of this facility
- k) In-built business process controls to capture the validation rules defined for processing the transactions/work-items
- l) Facility to register, approve or reject documents of specified type (as per applicable Acts & Bye-Laws) by an authorized officer
- m) Facility to view all pending transactions, retrieve the corresponding documents, print the required pages and mark the request as completed. Facility to mark the request as partially processed, with remarks
- n) Facility for an authorized officer to view pending work-items for all individuals in his/her purview.
- o) Facilities for an authorized officer to retrieve a work-item held by an individual (in his/her purview) and reassign it to another individual
- p) Facility to automatically escalate a work-item; if it is held beyond the pre-defined period by an individual. Multiple levels of escalation must be provided. Consequently, it is also necessary to provide a facility to define the threshold time limits for each transaction or service category that will be used for the purpose of escalation. This should be a parameter that can be changed by Punjab Local Government from time to time.
- q) Access to the records / statistics shall be as per the operating span/ geography of control.
- r) Facility to view the archived/stored documents (within the purview of the individual) along with the notes/ comments; if any
- s) After successful completion of the transaction or such other processing by ULB Office staff, make the e-Forms and associated documents as part of the electronic repository, which can be retrieved and verified at a later date
- t) Facility to return an e-Form for clarifications / corrections and keep track the payment for a given period of time; so that the applicant need not be charged for resubmission of the corrected/clarified document/e-Form.
- u) Facility to process complaints filed by individuals, stake holders and businesses through the work flow functions; including ability to integrate them with the compliance management, inspection, punitive and prosecution processes.
- v) Facility to scan documents, convert them to specified format, allow verification / authorization and upload this as part of the electronic records, with the necessary metadata into the appropriate folder hierarchy updating any necessary indices / links consistent with the application needs

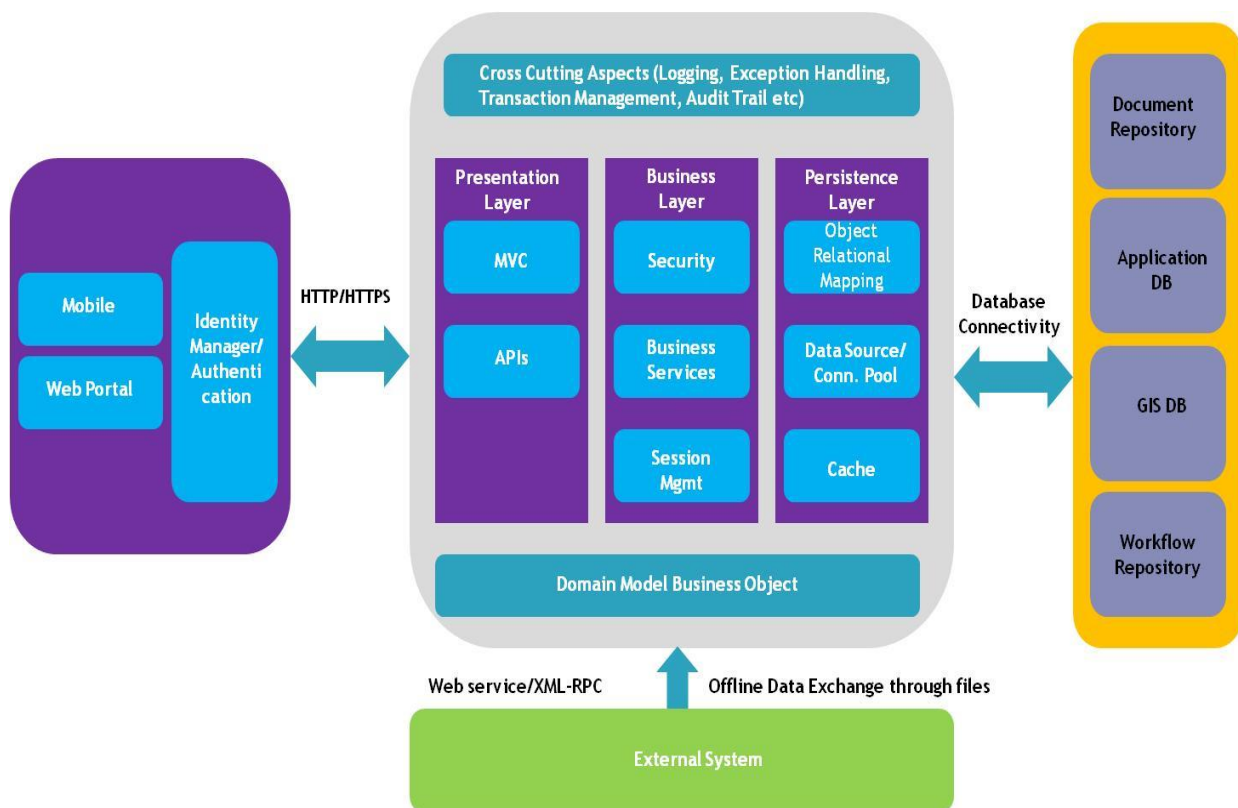
- w) Integrate the email functionality into the rest of the portal system such that all the escalations, e-Form submission, routing activities are notified to the concerned users

8.5 Requirements from Application Solution

The application software components should be simple to use. The total set of software components must be uniform in their user interface, being consistent in their use and meaning of keystrokes and sequences and in their visual presentations to the User. In case of procurement of software, licenses should be enterprise, perpetual and not community based or standard version. The user interface for all kinds of users (Citizen, Business, Government employee, etc.) should be the Local Government Portal, key requirements for which are explained below:

- a) Project Requirements Study: The Supplier shall study and understand the requirements of the project for designing a workable technology solution. Based on the requirements study, Supplier shall submit a Detailed Project-plan for application deployment which should be agreed upon with Purchaser through a formal sign off.
- b) Solution Procurement: The Supplier shall provide a COTS or Be-Spoke Solution, which should include portal solution framework, application software solution, security architecture, network architecture, data flow requirements, data storage requirements, encryption (at various levels of the solution), etc. The Solution should be based on appropriate system standards to enable its interoperability and integration with external solutions. The Supplier will submit System Specifications Document (SSD), Solution Design Document (SDD) and Information Security Plan (in conformity with ISO 27001) to Purchaser and should obtain the sign-off on these before commencing the development/ customization / configuration of the Solution.
- c) Solution Development/ Customization / Configuration: The Supplier would develop/ customize / configure the Solution based on the specifications frozen during the requirement study and design phase.
- d) Solution Testing & Implementation: The Supplier shall identify suitable testing requirements for the Solution and shall design the Test Cases including for Unit Testing, System Testing, Regression Testing, Performance Testing and Acceptance Testing. The Supplier shall obtain the sign-off from Purchaser on the Testing Approach & Plan. The Supplier shall perform the testing of the Solution (based on this Testing Plan), would document the results (in the form of Test Report) and thereafter shall fix the bugs / issues found. The Supplier shall be responsible for implementation of the Solution, which includes its implementation at all ULBs and Sewa Kendras. The Supplier shall also be responsible for defining and implementing ITSM/ITIL based IT Asset Management Policy
- e) Documentation: Post-implementation of Solution, the Supplier shall submit a host of documents to the Purchaser (including Technical Manuals, User Manuals, Operational Manuals, Maintenance Manuals, etc.). The Supplier shall also obtain formal sign-off from Purchaser for all these documents.
- f) Integration with External Systems: The Supplier shall ensure that suitable interfacing / integration is achieved & maintained between the Solution implemented for this project and relevant External Systems. Further the Solution implemented for this project should also be integrated with the 'Aadhaar' Project.

- g) It shall be the responsibility of the Supplier to arrange for the necessary development tools (hardware/software) during customization / configuration, implementation and integration (with External Systems) of the Solution.
- h) During the implementation of the Solution for this project, circumstances may arise when at a ULB, some of the functions get computerized and some remain manual. The Supplier shall state how the ULBs would function in such a scenario and how interfacing would be done between computerized system and manual processes, and vice-versa.
- i) The indicative Application software architecture is depicted below:



- j) It should be designed to provide modular and efficient framework that supports the following:
 - i. Must be multi-user and provide help facility through use of Function keys.
 - ii. Automatic session time out.
 - iii. Prompt facility in searching for the correct code for coded parameters.
 - iv. Ability to discard all data when the transaction is incomplete (Should not save).
 - v. To carry forward data from a previous screen.
 - vi. An audit trail for all transactions must be generated.
 - vii. Procedures for data exchange with interfaced applications
 - viii. Web based GUI for all the business functionality
 - ix. Integrated web based Workflow System

- x. Optimal response time
- xi. Unicode Standard based dual language interface (English & Gurumukhi)
- xii. Highly available, reliable and scalable application
- xiii. Highly transactional as well as MIS capable for all data elements
- xiv. Capability of Integration with third-party authentication devices like Biometrics, etc.

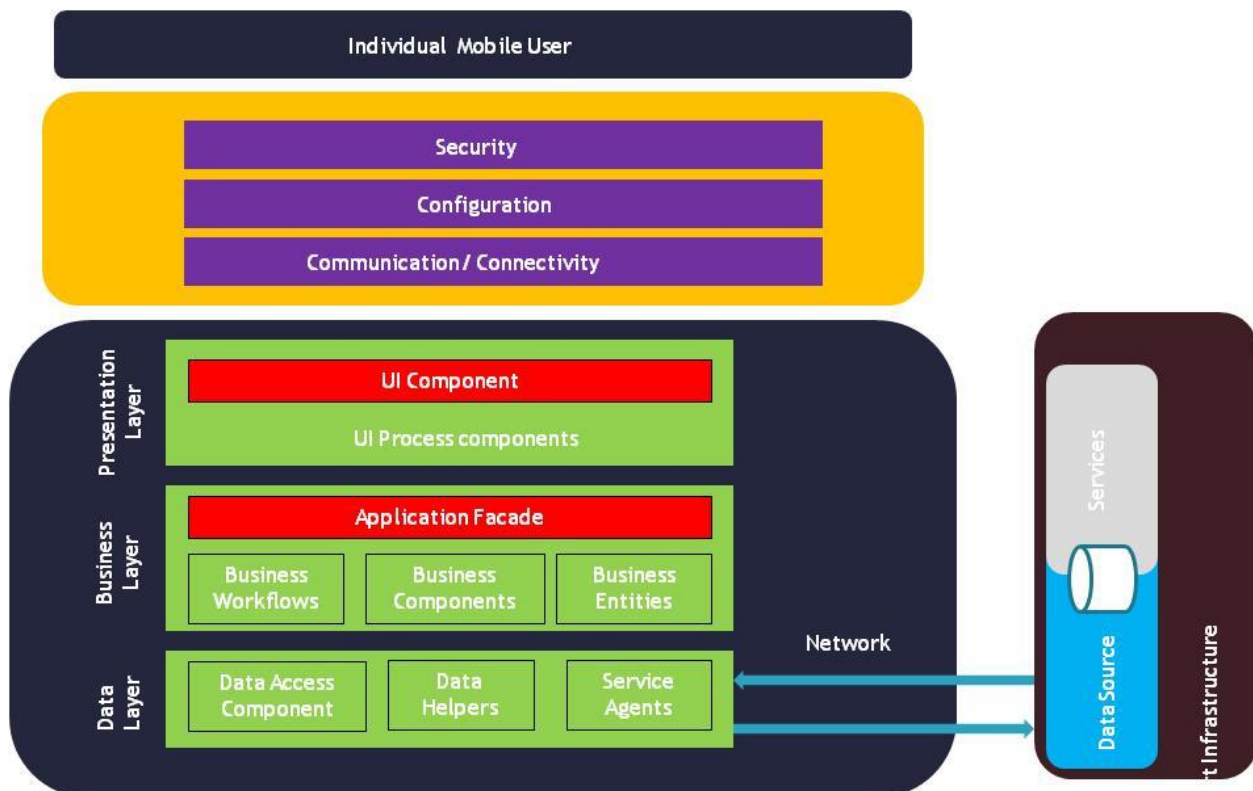
k) Various layers of the Application software architecture are described as below:

- i. Client: Client Application for the Punjab Local Government should be browser based application and should run on all major web browsers (such as Internet Explorer, Mozilla Firefox and Safari Opera). Web browser should be compatible with any mobile device including Android, blackberry and iOS mobile devices.
- ii. Application Container: Punjab Local Government framework may be deployed in any cost effective and robust technology keeping in mind interoperability & portability of system.
- iii. Presentation Layer: Presentation Tier should enforce uniform header, footer and standard side bar items and navigation in each screen to maintain uniform look and feel of the data across various departments and services and is supported by Unicode standard including English and Punjabi for content viewing and entering the data in online forms. In Presentation layer Custom Tag Library and Scripting Language may be used for partial form submission and client side validations.
- iv. Business Layer: Business Layer should implement the process flow and logic that drives the business functionality. Inter-operable and Open Standard/protocols like web enabled services, APIs, A standard framework like UML or Object Rational Mapping should have been used to make this Business Layer a platform-independent application. Application Framework should have been developed using Component based design. This layer should also give functionality for data exchange using web enabled services based component or database synchronization with external agency. Framework should have provision to keeps all the user activity to be audited and logged during the business process.
- v. Persistence Layer: It has been visualized that the Solution for this Project would have to manage very high volumes of data, and would have to store a large amount of data for long-term preservation of records at various repositories. It is mandatory for the Supplier to ensure faster access and better manageability of this data. The Supplier should propose technology which is powerful enough for designing and querying database models at the conceptual level, where the application is described in terms easily understood by non-technical users. The Supplier is expected to use data models which can capture more business rules, and are easy to validate and evolve. It is expected that the Supplier will consider mechanisms which would improve the performance of this layer.
- vi. External System: Punjab Local Government System requires communicating with external applications or legacy systems running in other organizations. Web enabled service interface

should be provided to communicate with external systems. Offline data exchange using files should also be supported by this layer.

8.6 Requirements from Mobile Application

- a) Mobile is an emerging technology with continuous improvement in bandwidth features like 3G, 4G or latest. With rapidly increasing levels of mobile penetration and networking, and requirements of accessibility and citizen convenience, the Supplier must offer more and more services over mobile app including dashboard/reports. The Supplier must build strong interfaces, technologies, applications, Appstore etc. for mobile devices. In order to maximize citizen convenience and bring about business process improvements, the supplier must continuously innovate, upgrade and incorporate such new technologies that emerge. It is also assumed that suppliers will attempt to include as many services over any mobile device as possible, beyond the ones explicitly mentioned in this document.
- b) The following figure depicts the typical mobile application architecture. The mobile application (Apps) must be based on latest HTML5 technology. A mobile application (App) should normally be structured as a multi-layered application consisting of user experience, business, and data layers.



- c) These layers are same as described previously. The mobile application (Apps) should be designed in such a manner that it should address the following key issues:
 - i. Authentication / Authorization-Failing to authenticate in occasionally connected scenarios

Caching-Caching unnecessary data on a device that has limited resources

- ii. Communication- Failing to protect sensitive data over any carrier
- iii. Data Access-Failing to implement mechanisms that work with intermittent connectivity

8.7 Requirements of Back Office

Bidder is required to propose entire back-office solution based on their own assessment of technical specifications, performance, SLAs, other RFP requirements taking into consideration the nature, size, criticality, scalability, security, etc. and objectives of the project.

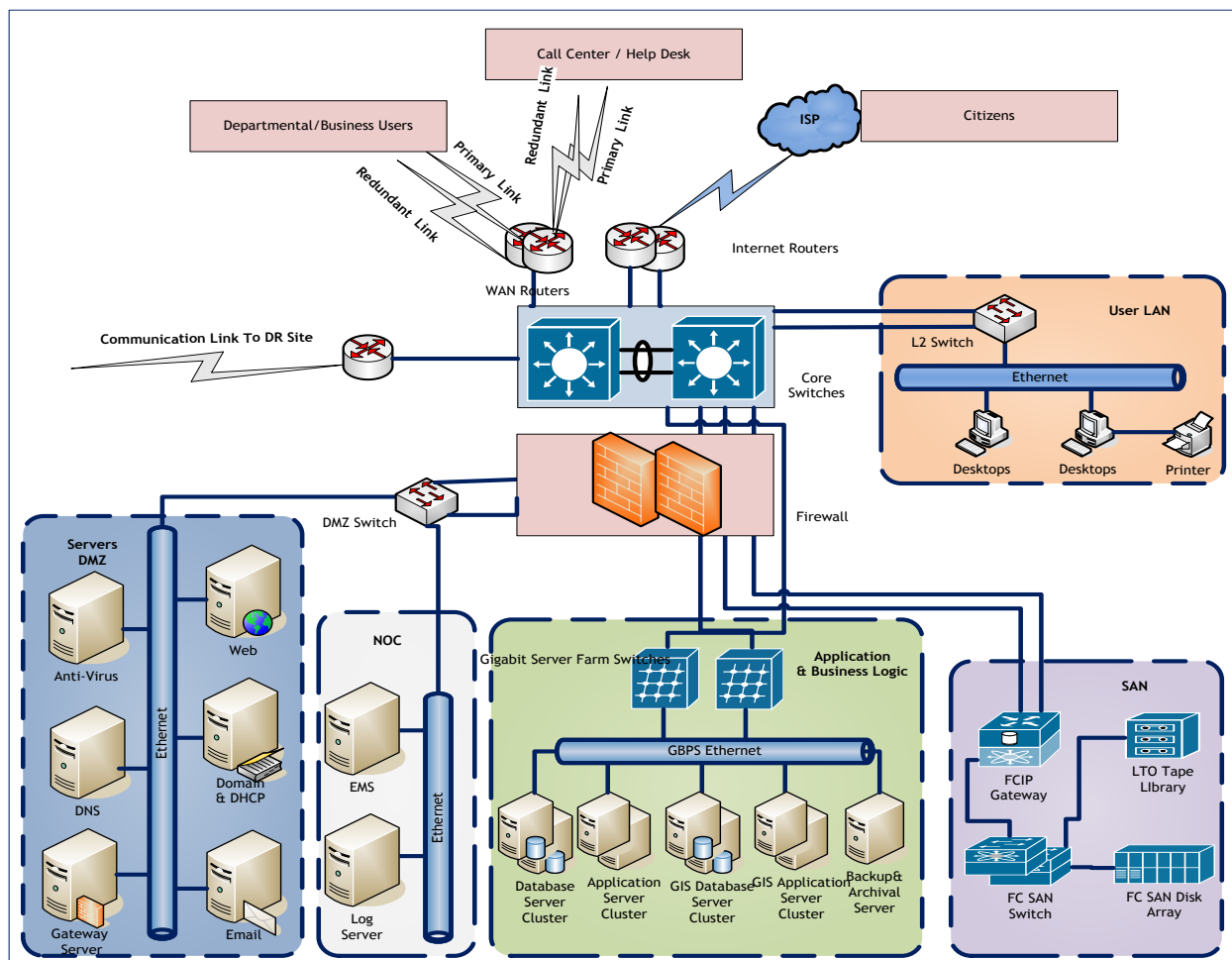
The back office would also be enabled to use all associated software modules as specified in Attachment-2 of Volume-1 of the RFP to perform general administration and management functions at ULB offices.

Supplier will provide adequate resources to assist ULBs in making use of application system.

Based on the assessment of Purchaser's requirement, Supplier shall do the sizing of solution and propose BOM along with specifications required at ULBs/offices of Department of Local Government, Punjab. Supplier shall be responsible for the performance of entire solution including performance of hardware and software sized and recommended by Supplier for back offices. Supplier shall also coordinate with Agency/OEM who will provide the end-user hardware and system software.

Supplier is expected to consider all above factors suitably while responding to this RFP.

8.8 Requirement from Punjab Local Government Gateway



- The gateway shall provide the facility to register the Service delivery channels & users.
- The gateway shall facilitate activation/deactivation of the registered service delivery channels and information users
- The gateway shall facilitate administrative facility to activate any select or all the back office system services (including data query/access) for service delivery channels & users.
- Gateway shall implement multiple verification/authentication mechanisms, at various levels, for ensuring trustworthiness of service delivery channels, information users/providers. For instance verification/authentication shall be implemented at network, transport, application layers etc.
- The authentication mechanism of service delivery channels, information users/providers shall support and implement advanced authentication techniques such as PKI based authentication. The design should be extensible to support newer authentication mechanisms

- f) The authentication mechanism(s) implemented for gateway shall guarantee the highest degree of trustworthiness.
- g) Once a service delivery channel is authenticated, it shall be granted access to services for which it is authorized/ enrolled.
- h) Gateway shall provide a common interface for the service delivery channels, and users, to interact with it using the standard interface.
- i) Gateway shall expose a common messaging interface for the Back Office Services, Gateway Common Services and other Third party Services to interact with it using the standard interface.
- j) While providing this interface, Gateway must be secure from the extranets that it may be communicating with; these extranets may be the Internet/un-trusted networks and or the Government Secure Intranet and or any other different extranets
- k) Gateway shall implement a messaging interface for the back office system, in conformance with IIP/IIS standards, for routing the requests received from service delivery channels and to receive the response from the back office system
- l) Gateway shall transfer messages from the service seekers to a back office system and vice versa in a secure, guaranteed and performance efficient manner
- m) All messages sent shall be delivered in a reliable manner and shall NOT be lost
- n) Any error in sending and receiving the message shall be appropriately logged and the sender/receiver appropriately informed
- o) Message content shall not be consumed / modified by Gateway during receipt, routing process
- p) Provide mechanisms for confidentiality and integrity of the information held on or passing through Gateway
- q) Any errors encountered during message processing shall be logged by Gateway in its logs
- r) Gateway must be able to deliver a message to its right recipient in the right message order supporting synchronous and asynchronous modes
- s) Gateway shall provide an administrative interface for registration, activation, deactivation of the service providers, information users/providers, to generate gateway usage and error reports, performance reports etc.

8.9 Deployment Architecture

- a) To run the application successfully on the network Web Server, Application Server, Database Server, etc. will be required. Some other servers like DNS, Directory Server etc. will be required for their different purposes. Indicative specifications of servers are given in Attachment-5 to this Volume of RFP.
- b) The specifications of servers, provided by the supplier should include following characteristics:
 - i. Scalability: The configuration proposed is expected to have adequate upgrade capability in terms of processors, memory, disk storage, etc. This should be achievable with minimum disruptions to processes and Users with minimum additional investment.
 - ii. Reliability: Installation of equipment manufactured by reputed companies committed to product improvement and new product development.
 - iii. Security: The equipment should have good security features, both physical (lockable, etc.) and operational (security/administration systems).
 - iv. Backup: Appropriate archiving system (i.e. tapes cartridge library, optical backup equipment or better alternative) to be installed at Server sites. In the event of serious failure, backed up data must be restored in quickest possible time to ensure continuity.
- c) The specification of the servers should be designed to ensure high availability of servers (clustering) at the central site. All the major servers should be configured in such a way that there is no single point of failure. This means that RAID technology may be used and configured as a multi-storage system cluster. If there is any requirement of application specific server at any site as per the requirement of the proposed application, the supplier is required to provide the same also. The supplier is to ensure the high availability for these servers (clustering) also. The option of having clustered servers is to allow for redundancy and load sharing for both database management and applications. The followings are description of major servers (but not limited to) required at SDC.

8.9.1 Application Server & Web Server

Application server would be required as middle tier for various web based applications. It would take care of the necessary workflow and Web server would be required for the interfacing with the end user. Both the web and application server would be seamlessly integrated to provide high availability and performance. These servers should be installed and operated in clustered configuration to ensure high availability and reliability.

8.9.2 Database Server

The Punjab Local Government application will be hosted on database which will contain all the data of the application. Since this data will be centralized and is very critical, the server should be installed and operated in clustered configuration in higher security layer, comprising of components such as Firewall and Intrusion Prevention system to ensure high availability and reliability. The data would be physically stored on an External FC based Storage (SAN). These will be Mid/High Range Enterprise servers.

8.9.3 Hardware Security Module (HSM)

Security would be one of the most important aspects of departmental /ULB network i.e. the communication and the information flow will be done in secured way. For that the solution would be integrated with Hardware security module (HSM) which may digitally sign and encrypt critical data, to secure the application, databases, data in transit etc. PKI will be used for the purpose of integrity (digital signing) and confidentiality (encryption). HSM will offload all the digital signing and encryption requirements from the server.

The Server responses to client requests should be digitally signed for ensuring the integrity and non-repudiation. Also the data in the database will remain in encrypted format with usage of HSM.

Wherever in the solution, integrity and confidentiality of the messages is needed, HSM will be used for securing the root keys and will be used for securing the transactions. It will be helpful in fulfilling the compliance requirement as per recent IT amended ACT or ISO as per standard norms or comply update act. For example, the central system will be equipped with HSM and any response sent to the client requests should be digitally signed. This will bring the complete architecture and message flow in line to recent IT amended act.

8.9.4 Mailing & Messaging Server

Mailing & Messaging Infrastructure would provide workflow functionality to ULB Employees. The Messaging Server should provide a highly scalable, reliable, and available platform for delivering secure communication services. PAWAN's Mail messaging solution (through DoGR) will be used by Department for this project. However, Supplier will act as system administrator for Department users and coordinate with DoGR for user related queries/rights. The messaging system implemented under this project shall have provision to use e-Mail facility from the mail servers at PAWAN. All employees will have email facilities.

8.9.5 DNS & DHCP Server

- a) DNS server would be required for various website and web applications hosted for public access. The internet users will query for the domains on the DNS (Public DNS) server deployed at the Server farm. DHCP would be assisting the System administrators for dynamic IP allocation to devices. Furthermore, the key users, who would be connecting using remote access, would be requiring a valid IP address after successful authentication. Domain name registration and ownership will lie with Purchaser.
- b) Following would be the services provided by DNS Server:
 - i. Should support conditional DNS forwarders e.g. forwarding based on a DNS Domain name in the query
 - ii. Should allow clients to dynamically update resource records secure and non-secure
 - iii. Should Support incremental zone transfer between servers
 - iv. Should provide security features like access control list
 - v. Should support new resource record (RR) types like service location (SRV), etc.
 - vi. Should support Round robin on all resource record (RR) types

8.9.6 Directory Server

The Directory Server will be used for authentication and authorization of users. LDAP v3 compliant directory software would be installed on this server.

8.9.7 Management Server

The management server would help in administration of distributed systems at the server farm. The management server would help in efficient and reliable administration of all the distributed computing devices. It would provide Inventory Management, Fault Management and Performance Management and Patch management and it would monitor the availability of Services. EMS will be installed on this system.

8.9.8 Backup Server

Backup server would be required for installation of backup ,Restore and Repository software (to take care of backup and repository activity)

8.9.9 Anti-Virus Server

A separate server for Anti-Virus would be required to keep the other servers and application secure from the attack of virus, Trojans, spyware, etc. This will also act as a centralized system for updating the virus definitions on the systems include last milestone desktop / laptop across Punjab Local Government offices, etc.

8.9.10 Storage Area Network (SAN) & Tape Library

- a) SAN (Storage Area Network) will be required for storage of data from all the locations. This will act as central repository for data, documents and records. The specifications for SAN are given in the RFP. Backup is an important aspect of recovering the lost data due to any loss. A Tape Library is proposed for taking the regular backup of centralized storage (SAN).
- b) The Punjab Local Government setup would be configured with SAN for external storage of data for faster access and would be implemented on RAID 5/6 for redundancy. The Database cluster connects to SAN through a redundant fiber switch to ensure no single point of failure. Tape Library with automatic robotic arm for movement/inventory of tapes for backup.
- c) It is proposed to have incremental backup of data, application logs and full backup of Directory, database and other servers. This can be done through the storage connected to SAN.
- d) The backup solution should address the following:
 - i. Assuring that the production servers' data is available in an offline storage device, and can be restored as and when required.
 - ii. The backup of the production systems to be performed in an LAN free manner for the Database Server, a LAN based backup for other APP and WEB Servers.
 - iii. Online full and incremental backups for database.

- iv. Online full and incremental backup for Mail and file servers
- v. To ensure a policy driven data-protection through scheduled backup and recovery.
- vi. Availability of complete backup data to a remote site, so that in case of any disaster at the Server Farm, the backup may be recovered from the remote site.
- vii. Single, centralized management for data protection and disaster recovery.
- viii. Backup of operating system, database and application as per stipulated policies at the Server Farm.
- ix. Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
- x. Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by User Departments or in case of upgrades and configuration changes to the system.
- xi. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
- xii. Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets.
- xiii. Physical security of the media stored in cabinets.
- xiv. Ongoing support for file and volume restoration requests at the Server Farm.

8.9.11 Firewall & Intrusion Prevention System in HA (High Availability) mode

Firewall with Intrusion Prevention System is a device that stops intrusion attempts before it enters the Punjab Local Government network. The network IPS (sensor) has two interfaces connected to the network; it receives network traffic on one of its interface and then passes that traffic out via the other interface. Any traffic that passes through the IPS (sensor) will then be examined for any malicious / suspicious activity by the sensor's Intrusion Prevention Software. Firewall integrated with Gateway Antivirus/Intrusion Prevention Service can inspect traffic from numerous protocols to identify attacks against the network; by blocking malicious traffic. The Network IPS solution can stop this traffic before it reaches the target system.

8.10 Infrastructure Requirements

8.10.1 Data Center

- a) The Data Center for this project will be based at State Data Centre (SDC). SDC is planned to locate at Plot No D-241, Phase-VIII B Industrial Focal Point, Mohali.
- b) At SDC, space, power, power backup, ACs and other administrative facilities such as physical security, fire extinguishers and access management shall be provided by Purchaser.
- c) Network connectivity shall also be responsibility of Purchaser.
- d) Supplier shall also be provided sitting space for their data centre staffs. However facilities like table, chairs, etc. for their staffs shall be responsibility of Supplier.
- e) It would be the Supplier's responsibility to arrange, and setup the necessary IT infrastructure at SDC. The minimum bill of material and their minimum specifications are given in Attachment-4 and 5 to this Volume of the RFP respectively.

- f) Hardware and software proposed for the Punjab Local Government at SDC should be dedicated for this project and not to be shared by the Supplier for any other purpose.
- g) The overall monitoring will be done with the help of EMS monitoring tools and system logs/counters. Reports and alerts should be auto-generated. Supplier will also monitor performance of network connectivity provided by Supplier.
- h) The system should be designed to remove all single point failures and comply to prevent information, system etc. and match requirement. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The agency shall perform various tests including network, server, security, DC/DR fail-over tests to verify the availability of the services in case of component/location failures. This shall also verify the availability of services to all the ULB users/Citizen/Employees in the defined locations/department and state governance forum
- i) The routers should be configured in high availability (HA) at State Data Centre.

8.10.2 Near Disaster Recovery (NDR) Site

- a) The near DR centre shall be located at Mahatma Gandhi State Institute of Public Administration Institutional Area, Sector 26, Chandigarh, 160019. Supplier shall ensure that NDR should immediately come up in case of SDC failure. This site would be connected with SDC by Department of Government Reform.
- b) Data will be replicated from DC to NDR at storage level in a synchronous mode.
- c) In case of DC failure, application should be accessed from Near DR location.
- d) NDR drill will be carried out by Supplier quarterly in non-business hours with prior permission of purchaser.
- e) List of software hardware resources required at NDR, but is not limited to, is provided in Attachment-4 and Attachment-5 to this Volume of the RFP.
- f) The network setup at NDR should have multiple security Layers.
- g) Supplier shall provide Business continuity plan.
- h) At NDR, space, power, power backup, ACs and other administrative facilities such as physical security, fire extinguishers and access management shall be provided by Purchaser.
- i) Network connectivity shall also be responsibility of Purchaser.
- j) Supplier shall also be provided sitting space for their data centre staffs. However facilities like table, chairs, etc. for their staffs shall be responsibility of Supplier.

- k) It would be the Supplier's responsibility to arrange, and setup the necessary IT infrastructure at NDR.

8.10.3 Disaster Recovery Site

General

- a) Disaster Recovery Site will be hosted on cloud.
- b) In case of DC failure, application should be accessed from Near DR location. In case both DC and Near DR fail, applications shall be accessed from DR within 3 hours of failure of Near DR (NDR). The replication of DC to DR should be such that to meet RTO and RPO. RTO should be 3 hours and the RPO should be nearly zero (but more than 15 minutes).
- c) DR drill will be carried out quarterly in non-business hours with prior permission of purchaser.
- d) Cloud Service Provider (CSP) should be one of 11 agencies empaneled by Ministry of Electronics and Information Technology (Meity). Please refer website www.meity.gov.in for more details.
- e) Supplier shall ensure that the guidelines issued by MeitY should be followed. Please refer www.meity.gov.in for guidelines on procuring cloud services.
- f) Preferred service model for the cloud services will be platform as service (PaaS)/ Disaster Recovery as a Service (DRaaS). There should be flexibility to scale up/down and the ability to provision virtual machines, storage and bandwidth dynamically.
- g) Supplier shall ensure the replication of data between DC, DR and NDR. Any tools to be used for backup, other than the mentioned in BOM, are to be provisioned by Supplier.
- h) Network Connectivity for the connectivity between PAWAN and DR will be provided by Supplier.

Security

Supplier shall ensure that CSP should be certified to compliant to the following standards:

- a) ISO 27001 - DR cloud services should be certified for the latest version of the standards.
- b) ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.
- c) ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds.
- d) ISO 20000-9 - Guidance on the application of ISO/IEC 20000-1 to cloud services.
- e) PCI DSS - Compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud.

- f) The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard.
- g) The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC

Privacy and confidentiality

- a) For classified and sensitive data, Supplier has to ensure that data is encrypted as part of a standard security process choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to the application and may choose from multiple key management options.
- b) Supplier should notify department promptly in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively.
- c) Supplier shall ensure that all the storage blocks or multiple copies of data if any are unallocated or zeroed out by the CSPs, that data cannot be recovered. If due to some regulatory reasons if it is required to securely decommission data, Supplier has to ensure that data is irrecoverable.
- d) Supplier shall report forthwith in writing of information security breaches to the Department by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.
- e) Supplier undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Purchaser.

Location of Data

- a) The location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the Supplier for processing, storage or hosting by the Cloud services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the Cloud services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider.

Audit

- a) The Cloud services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines as and when published).

- b) The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service Provider.

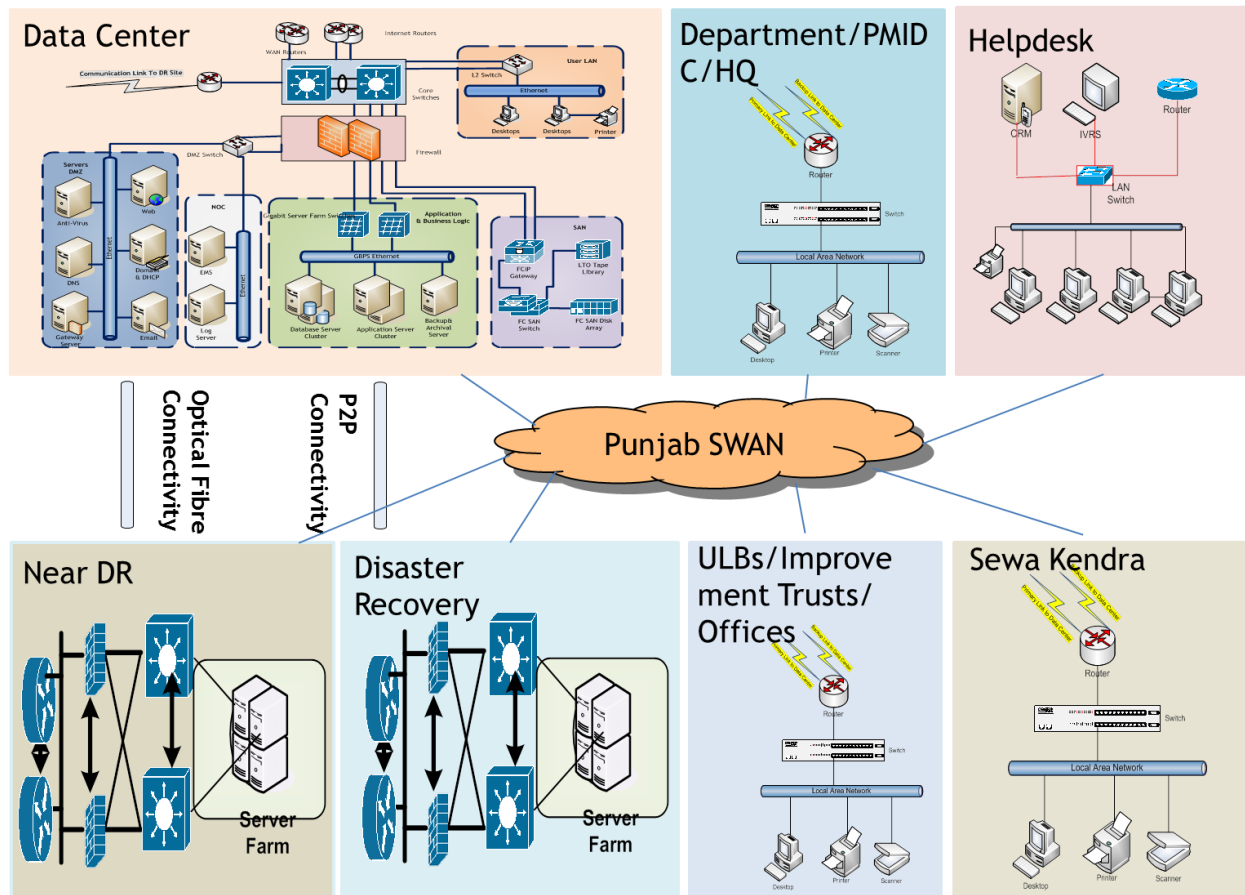
Transition/ Exit

- a) Supplier shall ensure that any data not to be deleted at the end/ termination of the agreement (for a maximum of 45 days beyond the expiry/ termination of the Agreement) without the express approval of the Department. Any cost for retaining the data beyond 45 days shall be paid to the Service Provider based on the cost indicated in the commercial quote.
- b) Supplier shall be responsible for providing the tools for import / export of VMs & content and preparation of the Exit Management Plan and carrying out the exit management / transition
- c) The Supplier shall provide the Department or its nominated agency with a recommended exit management plan or transition plan indicating the nature and scope of the CSP's transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement:
 - i. Transition of Managed Services
 - ii. Migration from the incumbent cloud service provider's environment to the new environment
- d) The Supplier is responsible for both Transitions of the Services as well as Migration of the VMs, Data, Content and other assets to the new environment.
- e) The Supplier shall carry out the migration of the VMs, data, content and any other assets to the new environment created by the Department or any other Agency (on behalf of the Department) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure.
- f) The format of the data transmitted from the cloud service provider to the new environment created by the Department or any other Agency should leverage standard data formats (e.g., OVF) whenever possible to ease and enhance portability. The format will be finalized by the Department.
- g) Transitioning from the cloud services including retrieval of all data shall be in formats approved by Department
- h) The Supplier shall ensure that all the documentation required by the Department for smooth transition (in addition to the documentation provided by the Cloud Service Provider) are kept up to date and all such documentation is handed over to the Department during regular intervals as well as during the exit management process.
- i) The Supplier will transfer the organizational structure developed during the Term to support the delivery of the Exit Management Services. This will include:
 - i. Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures.

- ii. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Department or its nominee in the use and operation of security controls.
- j) Some of the key activities to be carried out by Supplier for knowledge transfer will include:
 - i. Prepare documents to explain design and characteristics.
 - ii. Carry out joint operations of key activities or services.
 - iii. Briefing sessions on process and process Documentation.
 - iv. Sharing the logs, etc.
 - v. Briefing sessions on the managed services, the way these are deployed on cloud and integrated.
 - vi. Briefing sessions on the offerings (IaaS/PaaS) of the cloud service provider
- k) Transfer know-how relating to operation and maintenance of the software and cloud services.

8.11 Network Requirements

- a) Punjab State Wide Area Network (PAWAN) shall be used for meeting connectivity requirement of the project.
- b) WAN Connectivity shall be provided by Department of Government Reforms including connectivity between DC and Near DR.
- c) It will be the responsibility of the Supplier to assess the existing connectivity and make necessary recommendations to meet the requirements of their proposed solution, for example, whether upgrade of bandwidth is required.
- d) For the connectivity through PAWAN or current WAN availability at Punjab State, the supplier shall be responsible for proactive monitoring, troubleshooting and administration of the connectivity, & would provide issue resolution through coordination with the PAWAN operator or current WAN service provider availability at Punjab State or any other associated stakeholder to ensure high uptime.
- e) Current status of PAWAN is provided in attachment-7 of this volume of RFP.
- f) Network Connectivity of adequate bandwidth (minimum 20 Mbps) between PAWAN (DC and NDR) to DR shall be provided by Supplier.
- g) Network Connectivity of adequate bandwidth (minimum 5 Mbps) between PAWAN and helpdesk shall be provided by Supplier.



8.12 Helpdesk Toll Free

Punjab Local Government requires a helpdesk enabled with IVRS and required software and call management service that will automate processes to consolidate, log, track, manage and escalate incidents and problems. The Service will act as a single point of contact Helpdesk for all employees Punjab Local Government ("Employees") /Operators under Sewa Kendra Project of PSeGS ("Operators") who will record an incident. It will help Punjab Local Government to accelerate detection and problem resolution, maintain accurate configuration details, and minimize the risk caused by any change. It would be based on best practices, such as ITIL, for effective IT Service Management at Punjab Local Government.

Supplier is required to set up, operationalize and run this centralized helpdesk, accessible through telephone, the Local Government web portal, mobile phone where the Employees/Operators can call to register complaints and/or make suggestions.

Punjab Local Government shall provide toll-free number for helpdesk and will pay directly to Service Provider the cost towards its usage. Supplier shall check and verify the usage of toll-free number and submit a verification note every month.

Supplier shall be responsible for arranging necessary space, power, infrastructure, etc. for helpdesk to be set up. This helpdesk shall be separate from Helpdesk being implemented under Sewa Kendra project.

Minimum 10 helpdesk staffs are expected under this project. However, Supplier shall be required to provide satisfactory response to all calls received at helpdesk. Based on number of calls, Department may increase or decrease the number of helpdesk seats. Resources for helpdesk operation shall be dedicatedly deployed on this project for full time basis. Payment to Supplier will be made based on actual number of helpdesk seats.

Supplier can propose helpdesk from its location or through available hosted call centre solution but within the State of Punjab or tricity.

Operational requirements for Helpdesk:

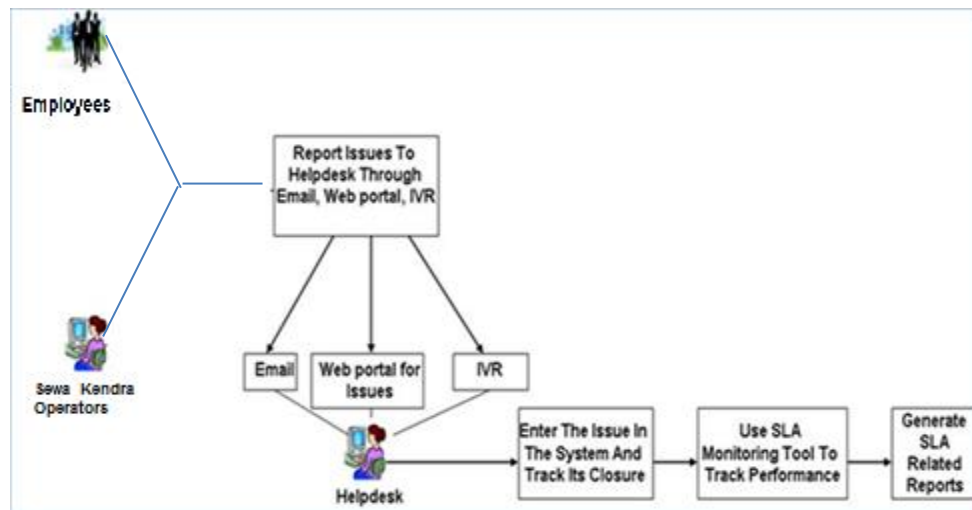
- a) Helpdesk will provide services using toll-free numbers to the Employees/Operators during general shift from 8AM to 8PM except on public holidays declared by Government of Punjab.
- b) Helpdesk should be both IVRS-enabled as well as operator-assisted.
- c) This helpdesk will be connected to PAWAN by Supplier.
- d) Call / Service request received at helpdesk for a specific ULB would be forwarded to them accordingly.
- e) The services shall be rendered across the State. The service shall be accessible in English, Hindi and Punjabi.
- f) The Supplier must periodically solicit user (Employees/Operators) satisfaction levels about the e-Government system, among other things, by conducting surveys.
- g) The menu structure shall provide callers with touch tone shortcuts, that can be used in sequence, which will allow the knowledgeable users to access information more quickly, without having to "drill down" through the menu structure with every call.
- h) The number of operator at helpdesk to be scaled up, if necessary, by the supplier based on transaction growth and to meet the SLAs

8.12.1 Toll Free Helpdesk for Employees

The centralized helpdesk would also facilitate resolution of day to day technical issues faced by the technical coordinators at the ULB level through call ticket management system. Following activities shall be carried out at the Helpdesk:

- i) Log User Calls related to application / IT infrastructure at Data Centre and assign Call ID No.
- j) Assign severity level to each call
- k) Track each call to resolution
- l) Escalate the calls, to the appropriate levels, if necessary as per escalation matrix, which can be defined at the time of award of contract
- m) Escalate the call related to usage of application software to respective application owners
- n) Provide feedback to callers.
- o) Analyze the call statistics
- p) Creation of knowledge base on frequently asked questions to aid users.

- q) Number of operators at helpdesk to be scaled up, if necessary, by the Supplier based on transaction growth and to meet the SLAs.



8.12.2 Toll free Helpdesk for Sewa Kendra Operators

- a) Given the enormity of the importance of this initiative, the Helpdesk is envisioned to be a critical interface between the Sewa Kendra project and project of Local Government, Punjab. This helpdesk shall support Operators of Sewa Kendra ("Operators") etc. across the state of Punjab.
- b) Operational requirements for Helpdesk for Sewa Kendra Operators are as follows:
- i. This helpdesk should be integrated with the helpdesk run by Sewa Kendra Operator/State Government to receive any query/complaint directly from their helpdesk for the issues pertaining to solution provided by Supplier.
 - ii. Helpdesk system should provide ULB wise, service wise and ward wise complaint details.
 - iii. The helpdesk system should have clear classification of complaint type for example O & M related, Building related, Water & Sewerage related and Licenses related, etc.
 - iv. All interactions with Operators will be assigned a ticket number and the number will be made available to the user along with the identification of the agent without the user having to make a request in this regard, at the beginning of the interaction.
 - v. All interactions will be noted on system. Interactions will also be recorded and the records shall be maintained for reference purposes. The transactions shall also be monitored – both on line and off line - on a statistically appropriate sampling basis to assess service level as well as delivery effectiveness and for providing training/ feedback to agents. Operators will be kept informed of the progress of resolution and final resolution.
- c) An IVRS facility, linked with Complaint & Grievances module, must be provided with the following functionality:
- i. Caller should be welcomed with a pre-defined note and must be informed about the estimated hold time.

- ii. Caller should be given option for selecting type of complaints e.g. Dial 1 for "Water & Sewerage Related", for Operation & Maintenance Related dial-2, for Health & Sanitization Related dial-3, for Billing Related dial-4, etc.
- iii. After selecting type of complaint the Caller should be allowed to select the Sub-Type of Complaint e.g. for Type Bill the Customer should be given Sub Options like, for Payment of Bill dial-1, for Correction of Bill dial-2, etc.
- iv. The system should have facility to directly talk to Customer Care Executive.
- v. There should be a facility to generate complaint number as the number which uniquely refers to any particular complaint.
- vi. The system should be able to track the resolution based on complaint number.
- vii. The system should be able to fetch the details of customer from other modules.
- viii. The system should have other standard features of IVRS.
- ix. The system should have SMS enabled services for Employees/Operators.

d) Some other requirements of the Helpdesk facility for Employees/Operators are as follows:

- i. The service shall respond to user errors with an offer to the users to restate or re-enter their selection.
- ii. The service shall allow users the capability of replaying the message they have just heard, restarting their session by returning to the main menu, or by accessing the help menu at any point during the call.
- iii. System shall have capability of presenting a "broadcast" message at the start of every call, if it is required at any point during the stage of regular operations. This message shall be separate and apart from any "static" message regarding service availability.
- iv. The information about status/ grievance shall be provided to the callers after their identification based on the required query. The system must have an authentication mechanism through Application number / reference number
- v. Once the caller initial request has been satisfied, the caller will be prompted whether or not they wish to request additional information
- vi. The system should have SMS enabled services for Employees/Operators.

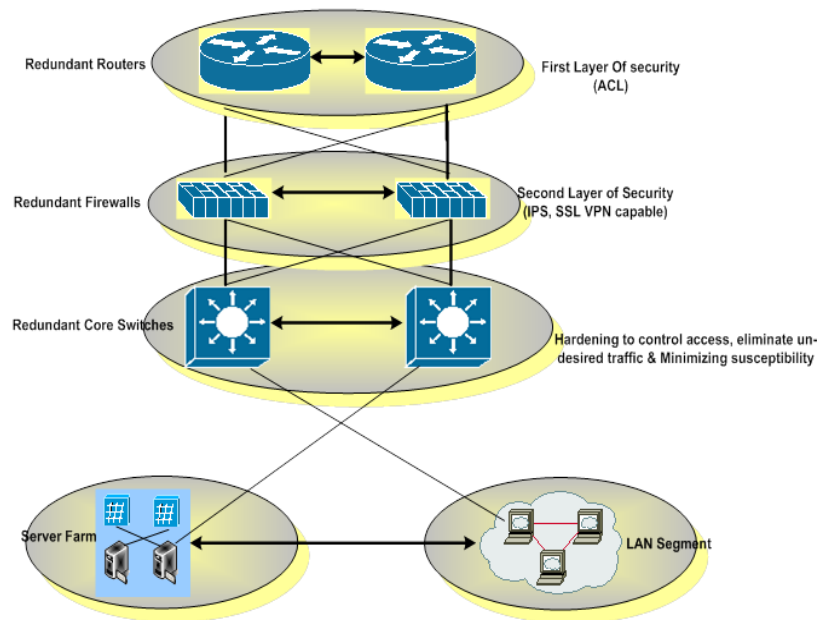
9. Security Architecture & Requirements

Solution should comply with latest Information Technology Act including all amendments thereon. Users shall access to the system must be through a single sign on process, which should involve specification of a user Identification, a password and the applications displayed must be as per the user profile and authority. The system should allow user to change his/her password based on a given time frame as well as give the user the option to change his password at any time. The system should disable the User profile after three unsuccessful log-on attempts. The system should be able to log successful and failed attempts to the system.

9.1 General Requirements

- a) Information, hardware and software must be secured to both internal and external parties (such as through password encryption).

- b) The security measures adopted must be of wide range and of high quality, to create confidence in the systems security and integrity. The system must be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users.
- c) System level and application level authentication between sites and between applications within sites, if any, to ensure against security attacks
- d) The application system should strictly be password protected and access to different modules should be role specific
- e) Audit trails should be provided to allow the activities of users to be monitored.
- f) For the system, security must be available at Functional level, User group/class level, Menu level and Transaction type level. Following figure depicts the hardware level security at SDC.



- g) There should be 3 levels of Security Considerations as described below:
 - i. At User level: This should include at least the following aspects:
 - User authentication
 - Role based access to services, transactions and data
 - Digital Certificate to be used for signing the Documents
 - Unified code
 - ii. At the Network/ Transport level: This should include at least the following aspects
 - Network Link Encryption (IPSEC)
 - Encrypted HTTP session using SSL (HTTPS)
 - iii. At the Application & Database level: This should include at least the following aspects
 - Secure storage of user credentials
 - Firewall to filter unauthorized sessions/traffic
 - Intrusion Prevention System to detect/prevent unauthorized activities/sessions
 - Server –to-server communication encryption secure mode.

- Secured/ encrypted storage of data/ data elements in Database & DB Backups
- Comprehensive logging & audit trail of sessions and transactions

9.2 Security Requirements from the Portal

- ULB Portal should be in compliance with updated amended IT Act Indian Cyber Act and other GOI, State Government and e-Gov standards prescribed by State department of e-Governance Forum and Ministry of Information Technology, Government of India.
- Effective password management controls: The portal solution must have the ability to perform unified code and password management functions including: controlled password expirations, forced password change with optional grace logins, minimum password lengths (eight characters), alphanumeric password standards, minimum number of numeric characters, non-dictionary words, password history logging, and user lockout from failed login attempts.
- Access control to information: The security solution must be facilitating access controls for specific users to only certain resources/services in the portal and at the same time system must provide single sign-on to all functional areas.
- Scalable and portable solution: The security solution must provide scalable access services for the Portal, including scalability in terms of number of users, user groups, resources, and access control policies.
- Secure Communication over the network: The portal shall support the exchange of data through secure channels of communication protected by standards such as the SSL protocol. Such facility shall provide the following functionality, at a minimum:
 - Confidentiality of communication - Encryption of all messages between client and server
 - Authenticity – Digital certificates to authenticate all messages between client and server, confirming the identities of messages/transactions
 - Uniform network code-It has a common set of rules which ensure that competition can be facilitated on network layer level. It governs processes, such as the balancing of the network packet system, network planning, and the allocation of network capacity to last milestone desktop and its services delivery to prevent failures of network.
 - Integrity – Message Authentication Codes (MACs) provide integrity protection that allows recognizing any manipulation of exchanged messages.
 - Secure communication between the user and the portal with SSL and encrypted logon information using algorithms with strong key lengths.
- Uninterrupted security services /automated load balancing to backup services: The security solution must provide for load balancing/high-availability to enable a fully scalable and available solution. It should enable continued service on failure of one or more of its component parts.
- Secure storage of critical items: The security solution must provide for the ability to securely store critical data within the LDAP or other user directory structure or any user related databases so that database administrators or any unauthorized users do not have access to items such as transaction information, passwords, user profiles and other critical items.

- h) Detailed session management abilities: The security solution must provide for session settings such as idle or max session time-outs, concurrent sessions and other session control settings.
- i) Web Access Filtering
 - i. The portal security solution must examine all traffic to all resources of the solution and all access attempts to the portal or directly to any resource managed/access by the portal, should be intercepted by the security solution, and examined for authentication and authorization requirements defined for the resource.
 - ii. At the same time, the performance overhead of examining all web-traffic and performing the authentication and authorization requests should not become the bottleneck in the service delivery process and should not impact on the performance of the portal solution.
- j) Security Monitoring: The security solution implemented for portal must be capable of comprehensive logging of the transactions and access attempts to the resources/applications through the portal. It should be capable of logging transaction history, unauthorized access attempts, and attempts to login that fail. It should also be capable of notifying appropriate parties of suspicious activity.
- k) Security- User profiles
 - i. For the first login by a user, the system should prompt the user to change his password.
 - ii. When a user logs-in, the system should show him the date & time of last login
 - iii. System must restrict user access based on the privileges assigned to the user
 - iv. System should keep a log of all activities carried out by a user (with date & time stamp)
 - v. System must maintain a log of all activities carried out by an administrator.
- l) Other Security Services
 - i. The sensitive and confidential information and documents of the users must be stored in an encrypted format in the database.
 - ii. System should support 64 bit/128-bit encryption for transmission of the data over the Internet.
 - iii. All the systems in solution network should run most up-to-date anti-virus software to avoid malicious programs to cause damage to the systems
 - iv. Any access to end users to database should only be via application/portal authorization
 - v. Physical security for the solution should address securing all information assets from physical access by unauthorized personnel. For example, the Server Infrastructure at SDC should not be physically accessible by anyone other than the persons responsible for on-site maintenance of the systems
 - vi. The technology solution should comply with recent amended ISO27001 standards. Security certification process shall include audit of network, server and application security mechanisms.
- m) PKI Service Requirements: For providing online and real-time transactions to the citizens requiring high degree of user authentication and security, Punjab Local Government system shall be implemented as the PKI based solution. For e.g. the online approval of the Punjab Local Government application shall require approval of the concerned Punjab Local Government officer using his digital signature. Following outlines certain guidelines with respect to implementation of PKI Services:

- i. The security solution implemented for Punjab Local Government portal shall support usage of Digital Certificates and Biometrics based authentication for all the personnel performing critical transactions in the system (as defined/ specified in the RFP).
 - ii. The solution should support digital certificates issued by all licensed CA's in India and should accept digital certificates based on criteria (Issuer, Class, Policy Identifiers).
 - iii. Client digital certificates based authentication should be used for access to the services as identified by the Purchaser.
 - iv. The digital signatures used in for the portal must be compliant to RSA standards as required by recent amended IT-Act of state and GOI norms and any further amendments, if any.
 - v. Automatic validation of digital certificates used for authentication and digital signatures is required. The validation must include check for acceptance criteria (Issuer, Class and Policy Identifiers), validity period, and current CRL based revocation checking.
 - vi. Digital signatures to be used shall be compatible with all platforms without any limitation
 - vii. Digital signing and encryption of attachments (documents) compliant to PKCS standards
- n) Auditing features & Requirements: The security solution for portal must provide the capability to track and monitor successful and unsuccessful transactions with the portal. Accountability for transactions must be tied to specific users. The architecture/systems should facilitate audit of all significant security events including authentication, accessing of services and security administration. Auditing capabilities need to be built into various layers of the portal infrastructure including Application Software, OS, Database, Network, Firewall etc.
- i. Supplier shall implement Intrusion Prevention Systems (IPS) at all the critical network points, both internal and external, for monitoring and addressing the unauthorized access attempts and the malicious activities in the network.
 - ii. Information & Communications systems handling sensitive information must log all security relevant events. Examples of these events include, but are not limited to:
 - Attempts to guess passwords,
 - Attempts to use privileges that have not been authorized,
 - Modifications to production application software,
 - Modifications to operating systems,
 - Changes to user privileges, and
 - Changes to logging subsystems.
 - iii. Detailed audit trail of transactions performed in the system (approvals, rejections, renewals, etc.) which should capture the details of individuals performing the transactions, date & time stamp etc.
 - iv. Stringent security measures shall be implemented surrounding the audit data to ensure that audit records are not modified, deleted etc.
 - v. The portal shall facilitate reporting facilities in a simple and readable manner for the officers to review audit trails for the transactions occurring in the system.
- o) Security Requirements for Punjab Local Government Portal Databases: Database is the critical components of the Punjab Local Government portal, which stores the entire data related to Services & functions. Following outlines the security requirements of the Punjab Local Government database, which at a minimum shall be implemented:

- i. The database for Punjab Local Government portal shall support and implement encryption capabilities while transferring data over networks, and ability to encrypt data stored in the database at the column level
- ii. Shall support PKI based authentication for administrative access to the server
- iii. Comprehensive auditing for inserts/ deletes/ updates / selects to quickly spot and respond to security breaches.
- iv. The critical data and the related documents stored in the portal database shall be stored in encrypted format.

p) Anti-Virus: The following activities need to be performed:

- i. Monitor Anti-Virus tool on daily basis and ensure that latest patches are updated
- ii. Monitor the security console and clean the virus from the systems, which are affected and if necessary, isolate those systems to avoid further spreading of viruses.
- iii. Alert users on new virus breakouts.
- iv. Install, configure and test latest security patches.
- v. Troubleshoot and rectify all virus related problems reported and also escalate if not rectified by the AV tool.
- vi. Monitor client security tools and adhere to security policies as finalized
- vii. Monitoring the efficiency and effectiveness of the Anti-Virus tool.
- viii. Registering and updating the Anti-Virus tool on the server and the clients periodically
- ix. Providing feedback on any new virus detected and alarms the protection systems.

10. Operational Requirements

This chapter outlines the operational requirements of e Governance & Automation project at Punjab Local Government. It should be noted that the Supplier for this project would be engaged on a turnkey basis for implementing the solution and providing operation & maintenance support in its functioning for a period of 5 years from Operational Acceptance of sub-phase 1- pilot. The summary of Operational Requirements is given below. However, it should be noted that operational success of this project is going to be measured in terms of successful service-transactions that take place using the system deployed by the Supplier.

- Supplier shall customise, implement and manage the Solution in accordance with the service level defined for the project.
- Supplier shall coordinate and provide complete support to Purchaser in conducting the solution acceptance testing and certification
- Supplier shall provide operational support and maintenance services for the Term of the Project including but not limited to the overall system stabilization,, Sewa Kendras Solution and IT infrastructure solution maintenance, system administration, security administration, database administration, network administration and end-user problem resolution. The Supplier will have to ensure that the solution is functioning as intended and attending to all problems associated in operation of the application system.
- Supplier is required to train the Purchaser's staff (technical personnel and end-users) to enable them in effectively operating the system. Supplier shall also be responsible for re-training the staff whenever changes are made in the Solution that is implemented for this project.
- Supplier shall prepare and provide to Purchaser documents including User Manuals, Operational Manual, Maintenance Manuals, etc. as per acceptable standards
- Purchaser will provide all types of stationeries (including paper for printout) and toner required for Operation of Department post Operational Acceptance of Solution. Stationary and toner requirements prior to Operational Acceptance of System and for digitization related activities (including printed records to be verified by Department) shall be responsibility of Supplier.

The scope of hardware maintenance and support services will cover supply, installation, on-site diagnosis of hardware faults in response to problem reports. Resolution of hardware problems detected during routine operational support activities will be taken care of by supplier. Supplier should timely install updates / upgrades of the Solution implemented for this project.

10.1 Application Solution Management

- a) The Supplier will provide full support to ensure that the Solution implemented under this Contract shall have no defect arising from development/ customization/configuration or from any act or omission of the Supplier.
- b) This support should also cover adapting the Solution for any additional requirement that might come to the notice of Purchaser at the time of actual use of the same.

- c) During the Project term, the Supplier shall be completely responsible for defect-free functionality of the Solution implemented under this Contract and shall resolve any related issues (including bug-fixing, etc.) within the duration agreed between the Purchaser and the Supplier.
- d) Since it has been considered that application may undergo the changes post-go live of application, hence Supplier shall deploy the required resources during operation & maintenance period. Supplier shall make all the customization in the Application during Operation & Maintenance period as per requirement of Purchaser without any additional cost/change request to Purchaser for all the services/modules mentioned in this RFP. The related cost may be factored-in reasonably under 'Maintenance Charges of Application' in the financial formats.
- e) The Supplier shall provide latest updates, patches/ fixes, version upgrades relevant for the Solution implemented under this Contract.
- f) Release Management: Supplier shall be responsible for Version Management and its documentation reflecting changes or enhancements made in the application including features and functionality. Supplier shall update the Application in form of 'Releases' for any change made post application security audit of sub-phase 1. Each release will be tested thoroughly by Supplier including unit testing, system testing, performance testing and regression testing. Supplier shall submit UAT test cases to Purchaser with Requirement Traceability Matrix (RTM) for UAT by Purchaser. All the releases are subject to security audit by Purchaser.

10.2 Infrastructure Management

The supplier shall be responsible for end to end infrastructure management during the entire project period. To enable IT support and administration, the supplier would need to plan and deploy experienced manpower so as to maintain availability of services and SLAs. Infrastructure Management includes the following activities:

- a) Design of appropriate System Administration policy with precise definition of duties and adequate segregation of responsibilities and obtaining approval for the same from Purchaser.
- b) Overall management and administration of infrastructure solution including servers, networking & security components, storage solution etc.
- c) Performance tuning of the system as may be needed to comply with SLA requirements on a continuous basis.
- d) Security management including monitoring security and intrusions into the solution.
- e) Monitor and track server and network performance and take corrective actions to optimize the performance on a daily basis.
- f) System administration tasks such as managing the access control system, creating and managing users, etc.
- g) Data storage management activities including backup, restore and archival etc.

- h) Attend to Punjab Local Government's user request for assistance related to usage and management of the eGovernance solution.
- i) The Selected Supplier undertakes to ensure that regular back-up copies of data are created and maintained safely.
- j) Network Administration & Management consists of the following activities but not limited to: Administering User IDs, Network analysis and performance optimizing, Continuous monitoring and management of network during the working hours of Sewa Kendras on each working day and restoration of breakdown within prescribed time limits, Ensuring network security and database security at all times.
- k) Design of Network Administration Policy and getting it approved from the Purchaser for effective and efficient management of Network resources. Network Administration would broadly include the activities: Network devices configuration, management and tuning for optimum performance, Tracking the network status, Availability and taking the remedial and preventive actions in case of problems, Network fault isolation and resolution, Monitoring of network performance and escalation of performance deterioration to concerned authorities and take remedial actions to resolve such issues, Implementation/ modification of network routing policies, IP addressing policy as required and Documentation related to network configuration, routing policies, IP addressing scheme etc.
- l) The Supplier shall maintain the adequate stocks of spares to meet the requirements.
- m) Whenever a component has to be replaced because of technical, functional, manufacturing or any other problem, it shall be replaced with a component of same make and configuration. In case the component of same make and configuration is not available, replacement shall conform to open standards and shall be of higher configuration specifically approved by Purchaser
- n) The supplier would also be responsible for resolution of all associated application, infrastructure and technical issues related to the infrastructure of the project. For the same the supplier may position a centralized team at the Data Centre to take care of the day to day technical issues.
- o) Perform SLA Monitoring with the help of NMS and EMS monitoring tools and system logs/counters.
- p) Auto-generation of MIS reports and alerts.

10.3 Information Security

- a) Supplier will be responsible for implementing measures to ensure the overall security of the solution and confidentiality of the data. The Supplier shall monitor production systems for events or activities, which might compromise (fraudulently or accidentally) the confidentiality, integrity or availability of the Services. This monitoring shall be through the security controls including:
 - i. Real-time intrusion detection tools
 - ii. Audit review tools
 - iii. Manual processes
- b) Supplier shall develop and deploy a detailed security policy for the solution implementation & maintenance in adherence to policies and procedures as laid by ISO, PCI, CERT-IN, Govt. of India and

provide automated compliance reports without minimal manual intervention. The security policy developed by the Supplier shall be updated to keep the security recommendations current and the same shall be implemented for the solution. The Supplier with the co-operation of appropriate, appointed representatives of Purchaser and the participating departments will manage the response process to security incidents. The incident response process will seek to limit damage and may include the investigation of the incident and notification of the appropriate authorities. A summary of all security incidents shall be made available to Purchaser on a weekly basis. Significant security incidents will be reported on a more immediate basis

- c) Supplier shall be responsible for application security audit from CERT-In empaneled agencies and STQC during implementation and operation & maintenance period as per requirements given in this RFP and submit 'Certificate of Audit' to purchaser along with detailed report on vulnerabilities.
- d) Supplier shall take approval from Purchaser for the selection of CERT-In empaneled agency. Purchaser shall make the payment for Security Audit separately.
- e) Supplier shall fix all the vulnerabilities as per report of Security Auditor and submit the compliance report.
- f) Supplier shall produce and maintain system audit logs on the system for a period agreed by Supplier and Purchaser, at which point they will be archived and stored at off-site or as desired by Purchaser. Supplier would deploy tools for automated correlation of audit logs for relevant security exceptions in real time or in near real time and take immediate remediation action.

10.4 Project Management

- a) The "e-Governance & Automation for Punjab Local Government" project is an initiative whose implementation is complex and can go out of control unless all the stakeholders, especially the Supplier designs and implements a comprehensive and effective project management methodology. The following requirements are therefore prescribed in this regard:
- b) WORK PROGRAM: The Supplier should design a detailed Project Plan, which should include the following components:
 - i. Project Organization and Management Plan
 - ii. Deployment Plan for envisaged Solution
 - iii. Plan for setting-up necessary Hardware and equipment at SDC
 - iv. Delivery and Installation Plan
 - v. Testing Plan and Methodology
 - vi. Training Plan, Methodology and Training Details
 - vii. Change Management Plan
 - viii. Data Digitization & Migration Plan
 - ix. Resource Deployment Plan
 - x. Any other relevant items related to Program Development
- c) Program Implementation: The Selected Supplier shall:

- i. Assume responsibility of managing and monitoring the project as per the Indicative Time Schedule specified in this RFP, under the agency assigned by Purchaser as Program Manager for the project
- ii. Monitor the progress of Change Management plan and data migrations as given out in the RFP in order to enable smooth transition to the new system
- iii. The Supplier shall submit following Monthly Progress Reports to the Program Manager agency summarizing:
 - Results accomplished during the period
 - Cumulative deviations from schedule of progress on milestones as specified
 - Corrective actions to be taken to return to planned schedule of progress
 - Proposed revisions to planned schedule
 - Other issues, outstanding problems and action proposed to be taken
 - Interventions which the Supplier expects to be made and the actions to be taken before the next reporting period
 - Test results of training

10.5 Change Management & Training Requirements

- a) As the organization goes through changes IT infrastructure will also change from time to time to meet the changing needs of the businesses. Proper change management will ensure that approved changes are implemented efficiently and with acceptable risk to the existing and to the new IT Services with minimal impact on the operations of Punjab Local Government. Training can be used as an effective medium to bring about the necessary change. For this project, training is envisaged to be carried out at all district offices simultaneously.
- b) In addition to the individual trainings conducted centrally for the ULB and the headquarter staff, Supplier may introduce 'Train the Trainer' Concept for effectiveness and continuity of training for future in consultation with the Purchaser. For this purpose he may select potential trainers from various ULB staff/Headquarter staff and grade them as certified trainers. This is a recognition certificate. ULB's may use these selected trainers for conducting their internal trainings.
- c) The Supplier must impart training to the personnel from Punjab Local Government in the operation of the application software, generation of MIS reports, maintenance of User Logins and operations of the backend servers, policies and procedures. All the personnel selected shall be trained on all the modules of the concerned department. For all these training programs the Supplier should provide necessary course material, manuals for troubleshooting and system admin to the trainees etc. Training Room /Premises, whiteboard, furniture for training would be provided by respective Corporations and DDR offices. However any other infrastructure required such as desktops, etc. shall be the responsibility of the Supplier.
- d) Supplier shall take the feedback from trainees at the end of each trainee and submit a report to Purchaser.
- e) Training shall be imparted in English and/or Punjabi.
- f) Supplier will be responsible for:-

- i. Advance Administration training for Data Center Administrators to perform required tasks
 - ii. User Training for officers/employees / Supplier
 - iii. Syllabus and Manual for Training plan for the departmental users to be approved by Punjab Local Government beforehand.
 - iv. Issue supporting documentation such as Training material, User Manuals, feedback form, etc.
 - v. Develop evaluation design and prepare evaluation forms for Pre, in course and post training assessment and evaluations, in consultation with Purchaser.
 - vi. Sign-off from Purchaser on Training.
 - vii. Other Change Management interventions which are required
- g) Supplier shall develop e-contents (maximum 5-15 minutes) and upload on the portal so that users can do self-learning. E-Contents should be prepared for
- i. Registration into application
 - ii. Password change,
 - iii. Application/Portal Navigation
 - iv. Broad functionalities/features of all modules.
 - v. E-Content should be highly interactive to users using infographics. Supplier shall
 - Define Learning Objectives for different set of users.
 - Prepare Instructional Design for the content, including duration, levels and outcomes.
 - Develop the course content such as Audio, Video, Audio-visual, eBooks, Multimedia, and Games.
 - Develop evaluation design and prepare evaluation forms for Pre, in course and post e-learning assessment and evaluations, in consultation with Purchaser.
- h) At the beginning of the project, following trainings shall have to be provided by the Supplier:

S.No.	Training Detail	Staff To Be Trained	Persons per Training Session	Duration
1	General Awareness Training (Basic computer awareness training)	All staff above clerk level of the functionaries (6000 approximately)	30	2 days
2	Functional Training on Application	All staff above clerk level of the functionaries (6000 approximately)	30	3 days
3	System Administration Training	Identified Officials (Approximately 100)	20	10 days
4	Change Management and IT sensitization training for Senior officers	Senior Officials (approximately 200)	20	2 days

- i) Subsequently, the following trainings shall have to be provided by the Supplier every year till the end of the assignment:

S.No.	Training Detail	Staff To Be Trained	Persons per Training Session	Duration
1	General Awareness Training (Basic computer awareness training)	All staff above clerk level of the functionaries (2640 approximately) Every quarter at each district	30	2 days
2	Functional Training on Application	All staff above clerk level of the functionaries (2640 approximately) Every quarter at each district	30	3 days

10.6 Qualification & Skills of Resources to be deployed

- a) The supplier will be responsible for overall implementation followed by 5 years of operations and management of the project. Therefore to meet the implementation and operational requirements as laid down in this RFP, the supplier would be required to deploy experienced and trained manpower for smooth functioning of the project. All the three components of the project, namely – Centralized infrastructure and Application, Back office System and the Service delivery infrastructure, suitable manpower need to be deployed during the project period to successfully implement & operationalize the system and meet the SLA requirements. The cost of manpower at Back office as well as Centralized infrastructure has been sought under Category III cost. These manpower requirements for each of the components are given in this Volume of the RFP.
- b) It is of immense importance for the bidder to understand that it would be required to deploy the actual manpower as per the proposal for the back office locations for which the supplier would be paid on man month basis/actual bases. Apart from the manpower required as above, a Project management Committee (as proposed in Volume III of this RFP) shall be constituted in which individual project managers of purchaser and supplier will also be members.
- c) The wages for the manpower deployed on the project should conform to the Minimum Wages Act, 1948 (along with the applicable amendments)
- d) Qualifications and skills expected at each levels: The supplier would need to deploy the actual number of resources as given in this RFP at the Back office to perform necessary roles/functions as defined in this RFP conforming to the SLA requirements. The following are the qualification requirement for manpower at various levels:

- i. Qualifications for manpower at Centralized infrastructure: The supplier would need to ensure that adequate & sufficiently trained resources are deployed to manage the Centralized Infrastructure components to meet the SLA and functional requirements of the project. Minimum qualifications and skills requirements are given in the table below:

Full-Time Onsite Deployment		
S.No.	Resources	Minimum Qualification & Skills
1.	Database Administrator Lead	<ul style="list-style-type: none"> B.E./B. Tech. / MCA with Certification in Database Administration 5-8 years of relevant experience
2.	System Administrator Lead	<ul style="list-style-type: none"> B.E./B. Tech. / MCA with Certification in Information Security Management 5-8 years of relevant experience
3.	Networking Lead	<ul style="list-style-type: none"> B.E./B. Tech. / MCA with Certification in Network Administration 5-8 years of relevant experience
4.	Security Lead	<ul style="list-style-type: none"> B.E./B. Tech./ MCA with Certification in Network/Security Administration 5-8 years of relevant experience
5.	Support Staff at Data Centre	<ul style="list-style-type: none"> B.E./B. Tech./ MCA 3-4 years of relevant experience

- ii. Qualifications for manpower at Back Office: The supplier would need to ensure that the resources as stipulated in this RFP are deployed at the ULBs to provide support on various activities. This manpower shall directly be reporting to respective ULB (as well as to higher authorities of the Supplier) for all related services.

Minimum qualifications and skills requirements for helpdesk staffs are given in the table below:

Full-Time Onsite Deployment			
S.No	Manpower	Key Responsibility	Minimum Qualification & Skills
1.	Staff at Helpdesk	Responsible for receiving user queries, providing them resolution, maintaining logs of call, etc.	Graduation or 3-year diploma in Electronics/Computer Sciences/Information Technology with more than 2 years of relevant experience

- iii. Qualifications for manpower at Project Management team (Supplier): The supplier would need to ensure that suitable resources are assigned dedicatedly for the project which would also be engaging

with the purchaser for all related matters and escalations. The requirements shall be governed by the governance structure as defined in Volume III to this RFP.

S.No.	Manpower	Minimum Qualification & Skills
1.	Program Manager	<ul style="list-style-type: none"> B.E./B. Tech./ MCA + MBA 15+ years of experience with 5+ years of experience as program/project manager Project Management certification (e.g. PMP, Prince2, etc.)
2.	Project Manager	<ul style="list-style-type: none"> B.E./B. Tech./ MCA + MBA 10+ years of experience with 3+ years of experience as Project Manager Project Management certification (e.g. PMP, Prince2, etc.)
3.	Application Development & Integration Lead	<ul style="list-style-type: none"> B.E./B. Tech./ MCA 7+ years of experience with 3+ years of experience in similar role Knowledge of SOA, ITIL Processes etc. is desirable
4.	Domain Specialist	<ul style="list-style-type: none"> Graduate in any discipline 10+ years of experience in Municipality / Local Government/ Urban Development Department. Large scale IT implementation experience is desirable
5.	Quality Manager	<ul style="list-style-type: none"> B.E./B. Tech./ MCA 7+ years of experience with 5+ years of experience in providing quality management services for large scale system implementations. Knowledge of automated testing tools is also desired.
6.	Service Delivery Infrastructure Lead	<ul style="list-style-type: none"> B.E./B. Tech./ MCA 7+ years of experience with 5+ years of experience in managing large scale geographically dispersed service delivery infrastructure like Sewa Kendras.
7.	Training and Change Management Lead	<ul style="list-style-type: none"> B.E./B. Tech./ MCA 7+ years of experience with 5+ years of experience in Change Management and capacity building

10.7 Maintenance of Physical Security at DC and Near DR

Physical security at DC and Near DR will not be responsibility of Supplier. However, Supplier is responsible for physical access for their staff or the staff of OEM engaged by Supplier to Data Centre, and Near DR.

10.8 Facility Management & Administration

- a) In addition to the management, administration, and security requirements specified in the RFP, the System must also provide for various management, administration and security features at overall system level

- b) System installation procedures should be self-explanatory, menu driven and should require minimum user interaction. Detail on-line help for installation should also be provided. Installation procedure should set all required system parameters for successful installation of the system. The Supplier should take into account ease of deployment for while proposing a solution.
- c) Following table depicts the facility management and administration activities which need to be performed by Supplier:
- i. Centralized Infrastructure and Application

Component	Activity/Responsibility
Facility Management and Administration	<ol style="list-style-type: none"> 1. Configuration of server parameters, operating systems administration and tuning 2. Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of upgrades including migration to higher versions and patches to ensure that the system is properly updated. 3. Re-installation in the event of system crash/failures 4. Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc. 5. Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc. 6. Ensuring that the logs are backed up and truncated at regular intervals 7. Periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measure 8. Ensuring the upkeep of existing systems that would be reused and also incorporate necessary changes for new applications if any during the tenure of the contract 9. Troubleshooting issues in the infrastructure, network and application to determine the areas where fixes are required and ensuring resolution of the same. 10. Identification, diagnosis and resolution of problem areas pertaining to the Server farm infrastructure and application and maintenance of assured SLA levels. 11. Implementation and maintenance of standard operating procedures for maintenance of the infrastructure. 12. Management of the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc. 13. Providing Information on the IT infrastructure to all other processes and IT Management

Component	Activity/Responsibility
	14. Enabling control of the infrastructure by monitoring and maintaining information on All the resources that need to deliver services and Status and history of Configuration Items (CI) or IT Assets and their relationship with other IT Assets
System administration	<ol style="list-style-type: none"> 1. Configuring and apportioning storage space 2. Setting up of working e-mail accounts and mailing lists 3. Management and integration of databases 4. Implementing security on the Internet / Intranet 5. Setting up of firewalls and authorization systems 6. Performing periodic backup of data and automating reporting tasks 7. Executing updates in hardware and Solution as necessary.
Server Management	<ol style="list-style-type: none"> 1. The Supplier shall perform all system administration tasks like server management and operating system administration, user management, device management etc. The vendor shall ensure high availability of System resources to the users and to maximize the uptime of the system by diagnosing, detecting and rectifying the faults in time. 2. The Server Administration for any platform will comprise of the following activities <ol style="list-style-type: none"> a. Starting/Shutdown servers or services at Server Farm b. Monitoring performance of server resources c. Monitoring access logs and application logs d. Purging of files and logs e. Taking data backup and restoration f. Applying service packs, fixes, updates and security patches g. Providing helpdesk related administrative support 3. Server Management operations will comprise of the following – <ol style="list-style-type: none"> a. Monitoring of software licenses and identification of software license procurement or up-gradation b. Providing and maintaining user access controls – creation, modification or deletion of access/authentication and administrative rights on servers as per defined access policy. c. Maintaining data access security d. Deployment, Monitoring and updating of Anti-virus software on servers e. Coordinating with Anti-virus service provider for support for virus attacks and resolution.

Component	Activity/Responsibility
Storage / Database Administration	<ol style="list-style-type: none"> 1. Installation and configuration of the storage system. 2. Management of storage environment to maintain performance at desired optimum levels. 3. Development of storage management policy, configuration and management of disk array, SAN fabric / switches, tape library, etc. 4. Configuration of SAN whenever a new application is hosted at the server farm. This shall include activities such as management of storage space, volume, RAID configuration, zone, security, business continuity volumes, NAS, performance, etc. 5. End-to-end management of database on continuous basis to ensure smooth functioning of the same 6. Management of any changes to database schema, disk space, storage, user roles 7. Review of Code of Conduct and configuration to improve performance of the application or to resolve bottlenecks if any. 8. Performance monitoring and Databases on a regular basis including, preventive maintenance of the database as required. 9. Applying patches and database upgrades as and when required with minimal downtime. 10. Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions. 11. Use of DBA tools related to performing database creation, maintenance, and database monitoring tasks
Network Administration	<ol style="list-style-type: none"> 1. Monitoring and administering the LAN up to the integration points with WAN. 2. Creation and modification of LANs, assignment of ports to appropriate applications and segmentation of traffic. 3. Coordination with vendor for break fixes maintenance of the LAN cabling.
Messaging Administration	<ol style="list-style-type: none"> 1. Administration of messaging servers 2. Troubleshoot and rectify all email-related problems reported. 3. Coordinate with PAWAN mail administration team and provide issue resolution for e-mail related issues. 4. Backup and archival management. 5. Transaction log management.
Security Administration	<ol style="list-style-type: none"> 1. Information, hardware and software must be secured to both internal and external parties (such as through password encryption).

Component	Activity/Responsibility
	<ol style="list-style-type: none"> 2. The security measures adopted must be of wide range and of high quality, to create confidence in the systems security and integrity. The system must be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users. 3. System level and application level authentication between sites and between applications within sites, if any, to ensure against security attacks 4. The application system should strictly be password protected and access to different modules should be role specific 5. Audit trails should be provided to allow the activities of users to be monitored. 6. Overall network environment has to follow a well-defined security policy. The framework needs to ensure the information availability, integrity, and confidentiality of Punjab Local Government infrastructure and data. The security policy should be comprehensive and shall address the security needs of the network and the Network Operations for the Servers kept at State Data Center and for the end-users in various offices. 7. A security audit of the Non Functional Requirements of Applications shall be done after the completion of implementation phase and regularly during the Operations and Maintenance phases on annual basis, to assess whether appropriate security procedures are being followed. 8. Network will be an IP based intranet, therefore strong security infrastructure will be put in place from securing the network from the external network/ internet. 9. Methods of mitigating a security breach from within the intranet or extranet should be addressed by the security policy. The Supplier should design appropriate network solution so that a security breach/ virus do not spread throughout the network if originating at the end-user level. 10. The Network shall have IPS, Firewall, and Anti-virus server to secure the network in conjunction with Access Control List, port monitoring and management from any attacker 11. Security Infrastructure should provide comprehensive identification, authentication, authorization/access control, administration, and audit mechanism in the Hardware and network with relevant technologies, best practices, guidelines, and standards. The security services used to protect the information infrastructure shall include: <ol style="list-style-type: none"> a. Identification – Process of distinguishing individual users b. Authentication – Process of verifying the identity of a user

Component	Activity/Responsibility
	<ul style="list-style-type: none"> c. Authorization and Access Control – Process of establishing and enforcing user rights and privileges d. Administration – Process of managing, and maintaining infrastructure e. Audit – Process of monitoring above mentioned processes, to make sure that suitable security has been established and maintained. <p>15. The security services shall be delivered, and that the technologies implemented, in conjunction with a set of best practices guidelines, and industry standards. The technology solution should comply with BS7799/ISO27001 standard or any other standard adopted as a policy by the Government of India.</p> <p>16. Monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.</p> <p>17. Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies etc.</p> <p>18. Periodic reviews of domain level rights and privileges.</p> <p>19. Maintenance of an updated knowledge base of all the published security vulnerabilities and virus threats for related software, including, but not limited to, operating systems, application servers, web servers, databases, security solutions, messaging solutions, etc.</p> <p>20. Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.</p> <p>21. Responding to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.</p> <p>22. Undertake maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers, desktops from viruses.</p> <p>23. Implementation and periodic updating of the security policy.</p> <p>24. Operating system hardening through appropriate configuration and patch updates.</p>
Backup and restore	<p>1. Backup of operating system, database and application as per stipulated policies at the Server Farm.</p>

Component	Activity/Responsibility
	<ol style="list-style-type: none"> Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies. Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by User Departments or in case of upgrades and configuration changes to the system. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes. Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets. Physical security of the media stored in cabinets. Ongoing support for file and volume restoration requests at the Server Farm.
Change Management	<ol style="list-style-type: none"> Tracking the changes in hard / soft configurations, changes to applications, changes to policies, applying of upgrades / updates / patches, etc. Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.
Technical Troubleshooting	<ol style="list-style-type: none"> Recovery and auto-roll back of data: There should also be re-scheduling capabilities for automatic retries and restart logic (e.g. batch processing) Audit trails and logs maintenance capabilities The Suppliers will provide the backup frequency and recovery plan. The application system should also support the replication of the centralized system to the disaster recovery site, as and when the site comes up. A combination of full (on Tape Media) and incremental (Day-time) backups should be employed to ensure disaster tolerance. The Supplier must provide the backup and recovery plan. The Supplier must provide a BCP/Disaster Recovery plan.
User and Usage administration	<ol style="list-style-type: none"> Only authorized personnel are allowed to access the system; access being restricted via the use of user names/identifications and associated password. Access to each application is restricted to specified authorized users The user in the application system is logged off automatically if the user is idle for more than a specified and variable period, to prevent access to the system, applications etc. by unauthorized third parties when a terminal is left unattended.

ii. Back Office System

Component	Activity/Responsibility
Facility Management and Administration	<ul style="list-style-type: none"> • Providing Information on the IT infrastructure to all other processes and IT Management • Enabling control of the infrastructure by monitoring and maintaining information on All the resources that need to deliver services and Status and history of Configuration Items (CI) or IT Assets and their relationship with other IT Assets
System administration	<ul style="list-style-type: none"> • Monitoring hardware and software updates • Recommendation on hardware and software for ensuring desired performance
Network Administration	<ul style="list-style-type: none"> • Monitoring and administering the LAN up to the integration points with WAN • Coordination with vendors/OEMs for break fixes maintenance of the LAN cabling
Mailing Administration	<ul style="list-style-type: none"> • Install, configure and test client email software on all workstations, desktops and laptops, if any. • Coordinate and follow-ups with email solution provider for all email-related problems reported by users. • Backup and archival management. • Implementation of mail policies as defined by Punjab Local Government, including, but not limited to, user security, access control, encryption, mail box sizes, mail sizes, spam, content filtering, etc.
Security Administration	<ul style="list-style-type: none"> • Information, hardware and software must be secured to both internal and external parties (such as through password encryption). • The security measures adopted must be of wide range and of high quality, to create confidence in the systems security and integrity. The system must be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users. • Security Infrastructure should provide comprehensive identification, authentication, authorization/access control, administration, and audit mechanism in the Hardware and network with relevant technologies, best practices, guidelines, and standards. The security services used to protect the information infrastructure shall include: <ul style="list-style-type: none"> • Identification – Process of distinguishing individual users • Authentication – Process of verifying the identity of a user • Authorization and Access Control – Process of establishing and enforcing user rights and privileges • Administration – Process of managing, and maintaining infrastructure • Audit – Process of monitoring above mentioned processes, to make sure that suitable security has been established and maintained.

Component	Activity/Responsibility
	<ul style="list-style-type: none"> The security services shall be delivered, and that the technologies implemented, in conjunction with a set of best practices guidelines, and industry standards. The technology solution should comply with BS7799/ISO27001 standard or any other standard adopted as a policy by the Government of India.
User and Usage administration	<ul style="list-style-type: none"> Only authorized personnel are allowed to access the system; access being restricted via the use of user names/identifications and associated password. Access to each application is restricted to specified authorized users The user in the application system is logged off automatically if the user is idle for more than a specified and variable period, to prevent access to the system, applications etc. by unauthorized third parties when a terminal is left unattended.
Support to back office Employees	<ul style="list-style-type: none"> Assisting ULB employees in performing their work related to general administration and management functions & back office processing with the use of deployed system. Providing guidance and assistance to the employees time to time for their queries related to features, use of the system etc. Taking feedback time to time for change management related matters at the ULBs.

10.9 Requirement for Adherence to Standards

The following Technology and standards should be used while developing and implementing the overall solution for Local Government.

Application	Standard
Workflow Design	WFMC /BPEL or Equivalent Standard
Portal Development	W3C Specification
Information access/transfer Protocols	SOAP, HTTP/HTTPS, UDDI, WSDL
Interoperability	Web enabled Services, Open Standard
Photograph	JPEG(minimum resolution 640 X 480 Pixels
Scanned Documents	TIFF (Resolution of 600 X 600 dpi)
Finger print scanning	IAFIS specification
Digital signature	RSA standards
Document encryption	PKCS specification
Information Security	ISO 27001 certified System (amended)
Operational Integrity & Security Management	ISO 17799 certified System (amended)
Operation	ISO 9001 Certified (amended)

Application	Standard
IT Infrastructure management	ITIL/ EITM specification (As per GOI Norms)
Service Management	ISO 20000 specifications or latest (as per GOI Norms and e-Governance policy from GOI)
Project Documentation	IEEE/ISO Specifications for documentation
Data Standards	All important data entities should be in line with standards published by DIT. These can be accessed at http://egovstandards.gov.in
Localization Standards	Localization standards, like Font standards are notified, and available at http://egovstandards.gov.in . All Applications should comply with these standards to ensure common look and feel.

11. Data Migration & Digitization

Supplier would be responsible for the digitization of the data currently available in manual form and / or migration of the data available in the databases of the existing IT systems to the new Database implemented for the proposed project. The procedure for Data digitization and Migration activities is covered in subsequent paragraphs.

11.1 Data Migration Requirements

The responsibility of data migration from existing databases to new database would lie with the supplier. The supplier will ensure that the data migration task is completed before shifting to the new application. For the data migration activity the Supplier will:

- Procure and maintain any hardware, software, tool or plug-in required for performing data migration and related tasks at no additional cost to Purchaser.
- Design data migration plan including acceptance methodology and get it approved from Purchaser. Data Migration plan should also highlight the prioritization for data migration based on locations, modules and/or sub-phase.

- c) Develop a separate schema for data migration or as agreed in data migration plan.
- d) Data migration for each sub-phase/module to be implemented must be completed atleast one week prior to start of its pilot implementation. Migration of location/ULB specific data must be completed atleast one week prior to start of implementation in that location/ULB.
- e) Purchaser will provide the available data to the supplier for migration purposes in the format as available with Purchaser. Supplier will convert the format, if required and migrate the existing data. Supplier will provide the **print outs and /or on-line view access** of the migrated data to Purchaser for verification purposes. Cost towards printer, paper, cartridge, etc., will be borne by Supplier.
- f) Supplier will provide checklists for migrated data to Purchaser for verification, including number of records, validations (where possible) and other controls.
- g) The supplier will submit a report on the quality assurance/control and the process adopted duly ensuring the accuracy in the migrated data (100% accuracy is required). Further, the purchaser will verify the data digitization on random sampling basis within a period of 10 working days from the day of submission of print outs and/or online view access to the Purchaser.
- h) Any corrections as identified in the migrated data during Data Quality Assessment and Review shall be addressed by supplier at no additional cost to Purchaser. Supplier shall be required to make corrections as identified as soon as possible and maximum in a week from date of notifying by Purchaser or timeline as agreed with Purchaser.

11.2 Data Digitization Requirements

The Supplier will be responsible for the data entry and/or digitization of the existing paper based records / physical files. The supplier will also be responsible for developing the software application for the data entry and digitization of the existing paper based records / physical files. The supplier shall procure and maintain all the hardware/tool/plugin required for the purpose of digitization/scanning of documents as appropriate. The Supplier will formulate the data digitization plan and the resource plan, in consultation with the Purchaser, based on the guidelines & statistics provided in this Chapter. The wages for the manpower deployed on the project should conform to Minimum Wages Act, 1948 (along with applicable amendments).

- a) Guidelines for Data Digitization Work
 - i. Data would be digitized in reverse order i.e. first complete most recent year's data for specified services, before digitizing data of previous years.
 - ii. Data Digitization task must be completed atleast one week prior to Supplier's request to Purchaser for issuing certificate of 'Operational Acceptance' for all concerned modules and locations. For instance, in case of 'Operation Acceptance' for a particular module and ULB, data digitization related to that module and ULB must be completed atleast one week prior to request to Purchaser for issuing certificate of its 'Operational Acceptance'.
 - iii. Supplier should have completed the preparatory work for data digitization beforehand.

- iv. Supplier will submit a report on the quality assurance/control and the process adopted duly ensuring the accuracy in the digitized data (100% accuracy is required). Supplier shall do atleast review at two level for the data digitized and submit the printout of digitized data with sign and stamp of authorized signatory of Supplier for further review and quality assessment by Purchaser. Further, the purchaser will verify the data digitization on random sampling basis within a period of 10 working days from the day of submission of **printouts** (along with online access) of digitized data to Purchaser.
- v. Any corrections identified in the digitized data during Data Quality Assessment and Review shall be addressed by supplier at no additional cost to Purchaser. Supplier shall be required to make corrections as identified as soon as possible and maximum in a week from date of notifying by Purchaser or timeline as agreed with Purchaser.

b) Process to be followed for Data Entry & Digitization

- i. Purchaser/Respective ULB will hand over the physical files (ULB wise) along with all the supporting documents to the Supplier in a batch of 30-50 files or as mutually agreed. Records to be digitized may include physical files and scanned documents as well.
- ii. The supplier would arrange all the papers in an appropriate manner and will put an Identification Number (IN) for each file and papers (as per the categories)
- iii. Supplier will do the data entry of the master data and the transaction data as per the requirements of the Workflow and Document Management System. The data digitized has to be bilingual i.e. **in English and Gurumukhi (Punjabi)**.
- iv. The supplier will also scan all the requisite documents and will link them with the appropriate file in the Document Management System.
- v. All the activities related to the data entry, scanning & digitization will most likely to be carried out at the premises of the Department's district offices.
- vi. Purchaser will arrange for the suitable space, table, chair and electrical connections (including electricity charges) for onsite staffs of Supplier at respective locations, while the Supplier will arrange for other necessary infrastructure, manpower and other consumables. Furthermore, Stationary and toner requirements for digitization related activities (including printed records to be verified by Department) shall be responsibility of Supplier.
- vii. Supplier will submit printouts of digitized data to the Purchaser for further verification. Cost towards printer, paper, cartridge, etc., will be borne by Supplier.
- viii. Purchaser will verify 10% records on random sampling basis viz-a-viz the original documents and will return the whole lot of records to the Supplier if the quality check by the Purchaser fails. In this regard, maximum 2 iterations are allowed.
- ix. The supplier shall update the digitized data based on the input received from Purchaser. The final hardcopy of digitized data, softcopy of the digitized data and softcopy of scanned documents would be returned back to Purchaser on DVDs or other electronic media at the end of the process. Supplier shall be responsible for provision of all types of medias (including DVDs).
- x. The Digitized Data will be the property of Purchaser and should not be copied or used by supplier for any other purposes other than the scope of this project. Any infringement in this regard will be serious and legal action will be taken against the Supplier.

- xi. Proper record of handing over and taking over of the documents shall be maintained by the supplier. Any loss of document shall be reported and treated very seriously and may lead to termination of contract and penal action.
- xii. Indicative Volume of Data is given on the next page. While every effort and care has been taken to ensure the accuracy of the volumes of data reported in the different categories, they are nevertheless based on estimates reported from the field. Supplier is strongly encouraged to adopt measures to ascertain for themselves such volumes.
- xiii. Since at this stage, paper status can't be ascertained, thus paper may be of any state i.e. bind book, loose, torn, multilayered, etc., and of any size i.e. A3, A4, etc. Bidder shall be responsible for digitizing and scanning all types of papers available with the Department. Bidder should accordingly propose cost per record for digitization and cost per page for scanning.
- xiv. An indicative number of records/pages which need to be digitized/scanned are provided in RFP. However there may be difference in actual number of records and pages. Payment to Supplier will be based on actual number of records digitized & actual number of pages scanned as per agreed unit cost for both digitization and scanning in the Contract.
- xv. Supplier will be responsible for printer & consumables, papers, etc. for digitization & scanning related activities (including printed records to be verified by Department).
- xvi. In case of digitization & scanning related activities, Supplier can work from 8AM to 8PM subject to approval from respective office heads.
- xvii. Format of self-assessment form of property tax is provided in Attachment 6 of this Volume of RFP.
- xviii. Sample forms for digitization/scanning are provided in Attachment 10 of this Volume of RFP.

c) Records to be Digitized

S. No.	Functional Area	Description	Columns / Fields per Record	Indicative Number of Records	Number of Years
i) Municipal Corporations, Municipal Councils and NPs (ULBs)					
1.	Birth/Death Record	Master Data Entry from Register	15	7000000	From 1989 to 2003 And 2013-till date
2.	Water Supply and Sewerage	Water Supply Register (Form W1)	10	758135	Last Year Data
3.		Sewerage Register (Form W1)	10	594762	Last Year Data
4.	License Department	Register of License Application(Form L1)	12	193938	Last Year Data
5.	Library	Library Member's Register	10	12092	All Data Till date
6.		Library Books Register		254992	All Data Till date
7.	Fire Services	Fire Service Register	10	23255	All Data Till date
8.	Legal Matters	Legal Register - Register of Suits(Form G 32)	20	11533	All Data Till date
9.	Rent & Leases	Rent & Lease Register - Rent Demand and Collection Register - (Form R2)	20	94575	Last Year Data
10.	Health & sanitation	Sanitation Register	5	249432	All Data Till date
11.	Education	Teachers Record	5	5667	All Data Till date
12.	Land Department	Land Register	15	2074	All Data Till date
13.	Finance & Accounts	General Cash Book - Form G2 - Accounts Book Entries for Last 5 years	20	2323574	Last 5 Years' Data
14.	Horticulture	Horticulture Register	10	12361	All Data Till date
15.	Establishment Matters	Staff Record - Service Book including PF records		51862	All Data Till date
16.		Number of Pensioners		9455	All Data Till date
17.	Miscellaneous	Advertisement register	14	3340	Last Year Data
18.		Social scheme register	15	145089	All Data Till date
19.		Tahebazari Register - Form R 5	5	97670	All Data Till date
20.	Property Tax	House Tax Assessment Register - (Form TS1)	15	890243	Last Year Data
Total Records to be Digitized for ULBs (X1)				12,734,049	

S. No.	Functional Area	Description	Columns / Fields per Record	Indicative Number of Records	Number of Years
ii) Improvement Trusts					
1.	Land and Property	Land Acquisition Register	14	2214	All Data Till date
2.		Property Register	13	6612	All Data Till date
3.		Property Ledger for Allottees	18	103499	All Data Till date
4.	Enhanced Compensation	Property Register/ in Files/ Enhancement Form	12	808	All Data Till date
5.	Draw of Lots/Auction/ Refund of earnest money	Earnest Money Register	13	136506	All Data Till date
6.	Water Supply and Sewerage	Water Supply Register - Form W1	10	15622	All Data Till date
7.		Sewerage Register - Form W1	10	15622	All Data Till date
8.	Legal Matters	Suit Register - G32	20	3706	All Data Till date
Total Records to be Digitized for Improvement Trusts (Y1)				284589	
Grand Total: Number of Records to be digitized (X1+Y1)				13,018,638	

d) Documents to be Scanned

S. No.	Functional Area	Description	Pages Per Record	Indicative Pages be scanned	No. of years for which data is to be digitized
i) Municipal Corporations, Municipal Councils and NPs (ULBs)					
1	Miscellaneous	Agenda/Proceeding Register	1	29517	All Data Till date
Total number of pages to be scanned for ULBs (X2)				29517	
ii) Improvement Trusts					
1	Land and Property	Sale Agreement	3	96423	All Data Till date
2		Sale Deed	4	109176	All Data Till date
3		Allotment Letters	3	114366	All Data Till date

S. No.	Functional Area	Description	Pages Per Record	Indicative Pages be scanned	No. of years for which data is to be digitized
4		NOC for allotted Plots	1	13185	All Data Till date
5		Permission to Mortgage House/ Plot	1	4048	All Data Till date
Total Number of pages to be scanned for Improvement Trusts (Y2)				337198	
Grand Total: Number of pages to be Scanned (X2+Y2)				366,715	

12. Acceptance Testing, Audit & Certification

The Purchaser will undertake an exercise of Testing and User Acceptance of the e-Governance solution as soon as transactions start taking place via the system and the manual processes are stopped. The testing and user acceptance will happen on component basis for example Hardware, Software, Network, equipment at SDC etc. The supplier needs to identify the testing requirement and must clearly outline & demonstrate the testing methodology.

Purchaser reserves the right to conduct Third Party Audit for functional, performance, security, SLA monitoring, hardware & infrastructure, etc. Cost incurred towards Third Party Audit will be borne by the Purchaser. Third Party Audit of the application would be done by either STQC or by any of the Agencies empaneled with Govt. of India for this purpose and selected at the sole discretion of Purchaser.

- a) Supplier must build up an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by Purchaser. The acceptance test plan will be defined by the Supplier, agreed and approved by Purchaser and will include all the necessary steps to ensure complete functionality, operation and performance of the system.
- b) All levels of testing will be conducted at the installation sites
- c) Testing must demonstrate that the new systems satisfy the operational and technical performance criteria
- d) It is Supplier's responsibility during the tests to evaluate and recommend any further changes to the infrastructure & application, at no extra cost to Purchaser. Any recommendations for change will be discussed with Purchaser.
- e) The Supplier must outline the methodology that will be used for testing.
- f) The Supplier must define the various levels or types of testing that will be performed.
- g) Supplier shall use automated tools for functional & regression test for application including mobile application and load testing.
- h) The Supplier must provide necessary checklist/documentation that will be required for testing.
- i) The Supplier must describe how the testing methodologies will conform to requirements.
- j) The Supplier must indicate how one will demonstrate to Purchaser that all functions in the new system installed have been tested.
- k) The Supplier will be responsible for correcting all faults found during the acceptance process at no extra cost to Purchaser.

12.1 Acceptance Criteria

a) General Acceptance

- i. System would be accepted in a phased manner. The supplier has to ensure the delivery of the system as per Implementation Plan. The purchaser will accept the system only when the system is up as per implementation plan (along with data digitization & migration requirement for the respective sub system/module) and the shortlisted Services are getting delivered via the same.
- ii. Primary goal of Testing & Acceptance would be to ensure that the project meets requirements, standards, specifications and performance prescribed by the RFP by ensuring that following are associated with clear, quantifiable metrics for accountability:
 - Functional Requirements
 - Availability
 - Performance
 - Security
 - Manageability
 - Project Documentation
 - Data Quality
- iii. The project is to be designed to meet all functional, non-functional and management requirements as mentioned in the RFP.

b) Functional Requirements: The detailed functional requirements of each component of e-Governance solution have been provided in Attachment-2 to this Volume of the RFP. The system developed/customized by supplier shall be reviewed and verified by the third party agency against the Functional Requirements signed-off between Purchaser and Supplier. Any gaps, identified as a severe or critical in nature, shall be addressed by Supplier immediately prior to Go-live of the system. One of the key inputs for this testing shall be the traceability matrix to be developed by the supplier for Punjab Local Government system. Apart from Traceability Matrix, the third party may develop its own testing plans for validation of compliance of system against the defined requirements. The acceptance testing w.r.t. the functional requirements shall be performed by both independent third party agency (External Audit) as well as the select internal department users (i.e. User Acceptance Testing).

c) Performance

- i. Performance is that aspect of service, which is measured in terms of throughput and latency. Higher throughput and lower latency values represent good performance of a service. Throughput represents the number of service requests served. Latency is the round-trip time between sending a request and receiving the response. This test process will include the following activities:
 - Determination of performance metrics
 - Designing performance tests
 - Development of workload
 - Performance testing

- Identification of bottlenecks and providing solutions
 - Determining final performance figures.
 - Communication of final results to all stakeholders
- ii. Final output of this process would be a sizing guide for the solution tested. The sizing guide will document the details of the performance tests, test data, bottlenecks identified, alternate solutions provided, and the final performance data.

d) Availability

- i. High Availability is a key requirement. The project must provide employees /Citizens/Sewa Kendras Operators with timely, continuous access to information. The project must also be able to rebound or recover from any planned or unplanned system downtime, ensuring a minimal impact on the operations.
- ii. Availability is the quality aspect of whether the service is present or ready for immediate use. Availability represents the probability that a service is available. Larger values represent that the service is always ready to use while smaller values indicate unpredictability of whether the service will be available at a particular time.
- iii. Also associated with availability is time-to-repair (TTR). TTR represents the time it takes to repair a service that has failed. Ideally smaller values of TTR are desirable.
- iv. The availability test would include the following activities:
- Designing test for high availability testing
 - Execution of high-availability tests
 - Assessment of transaction/data losses in relation to Disaster
 - Recovery system
 - Communication of final results to all stakeholders
- v. High Available clustering at all Web, App and DB server levels will be targeted. It is expected that supplier would maintain average availability / uptime of all components included but not restricted to hardware items, servers, database servers, system software, enterprise wide application software, etc. as per the SLA.

e) Security

- i. Security is the aspect of the service of providing confidentiality and non-repudiation by authenticating the parties involved, encrypting messages, and providing access control. The applications can have different approaches and levels of providing security, depending on the service requester.
- ii. Security Process will include:
- Audit of Network, Server and Application security mechanisms
 - Assessment of authentication mechanism in application / components / module
 - Assessment of data encryption mechanism
 - Assessment of data access privileges, retention period and archival mechanism

- Assessment for tools provided by bidder for Vulnerability assessment and automated policy compliance tools, Log Correlation, end to end data encryption and various other security tools.
- iii. Final outcome of this process would be a comprehensive audit report including all Network, Server and Application security features incorporated in this e-Gov project.
- f) Manageability: This needs to be a crucial aspect of an Enterprise Solution. Implementation Vendor has to ensure that the solution deployed has adequate monitoring and tracking features for measuring the utilization and availability of resources. This includes:
- i. Remote monitoring of Status and Statistics of all high-level components
 - ii. Management capability to start/stop/restart services and systems
 - iii. Auto discovery of all components manageable
 - iv. Auto discovery of all other system components
 - v. Ability to track changes in configuration of the system components to help track service
 - vi. System disruptions
- g) Project Documentation: 3rd Party Agency/Purchaser shall review the project documents developed by Supplier including requirements, design, source code, installation, training and administration manuals, version control, Layout Plan, etc. Any issues/gaps identified by the Third Party Agency/ Purchaser, in any of the above areas, shall be addressed to the complete satisfaction of Purchaser. Documentation requirement (but not limited to) are as follows:
- i. Centralized Infrastructure
 - Technical, Operational and User Manuals for operation of deployed solution
 - All policy documents such as Security Policy, Backup and Recovery Policy, Business Continuity Plan (BCP), etc.
 - Source Code and solution design documents.
 - Maintenance manuals for equipment at SDC, Networks, server and other hardware.
 - Network Diagrams
 - Documentation of IP and Subnet Scheme, Routing Tables and ACL etc. deployed for Intranet.
 - Documentation of device configurations such as firewall, routers, servers etc.
 - Details of IT infrastructure required
 - ii. Back Office System
 - Details of IT infrastructure required
 - All the relevant documents related to Implementation and any other document which may be necessary.
- h) Data Quality: 3rd Party Agency/ Purchaser shall perform the Data Quality Assessment for the data digitized/ migrated by Supplier. The errors/gaps identified during the Data Quality Assessment shall be addressed by Supplier before moving the data into production environment, which is a key mile stone for Go-live of the solution.

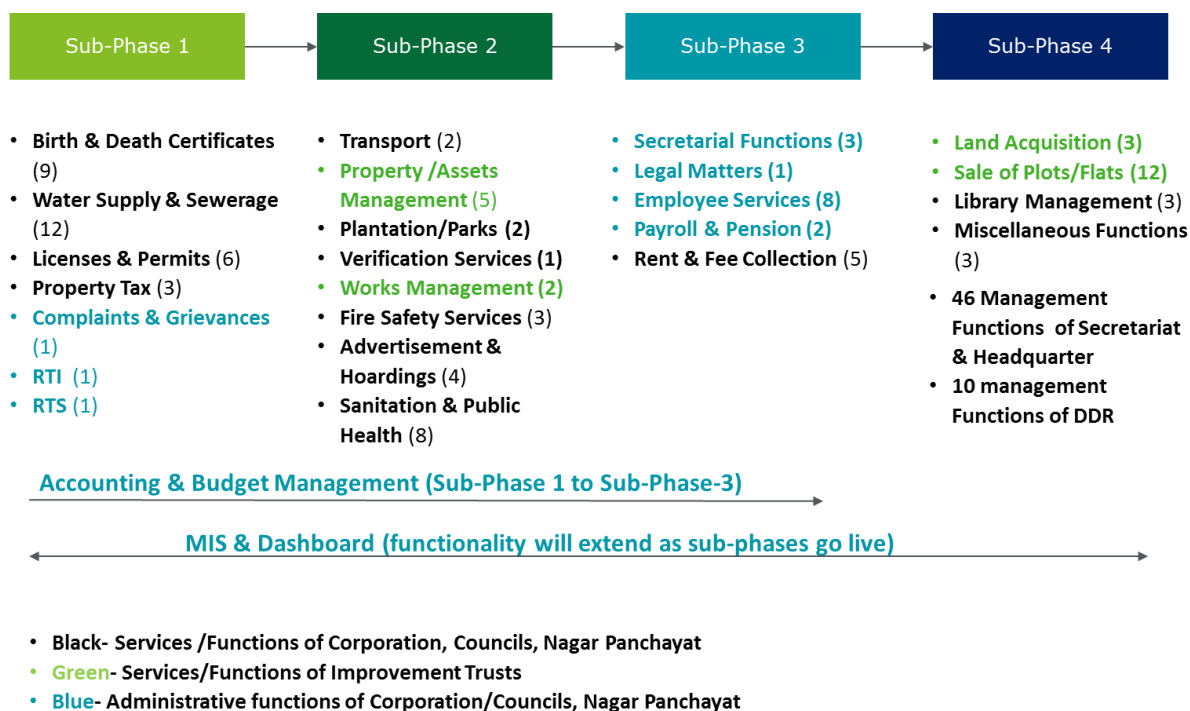
13. Phasing, Timeframe and Deliverables

a) Project Phases:

- i. The Project will be implemented in two phases- Phase-I and Phase-II. The classification of phases is based on Purchaser's priority for ULBs. Phase-I is further classified into four sub-phases based on Purchaser's priority in terms of implementation of modules and its readiness.
- ii. On successful completion of the phase-I, the solution needs to be rolled out in the entire state in the Phase-II. However, the PMIDC reserves the right to decide on continuing with the same implementation Vendor for rolling out the solution across the state in phase II.
- iii. Location wise coverage of phases is illustrated in table below:

Phases	Locations
Phase-I Pilot	(subject to applicability of module in pilot locations) <ul style="list-style-type: none"> • 1 Municipal Corporation (Amritsar) • 1 Class-I Municipal Council • 1 Class-II Municipal Council • 1 Class-III Municipal Council • 1 Nagar Panchayat • 1 Improvement Trust (Amritsar) • Secretariat • Head office
Phase-I Rollout	(other than pilot locations) <ul style="list-style-type: none"> • 4 Municipal Corporations (Jalandhar, Ludhiana , SAS Nagar, Patiala) • 1 Class-1 Municipal Council • 1 Class-2 Municipal Council • 1 Class-3 MC • 1 Nagar Panchayat • 3 Improvement Trusts (Jalandhar, Ludhiana , Patiala) • 2 DDR offices
Phase-II Rollout	All other ULBs/offices in the state of Punjab

b) Modular coverage under sub-phases of Phase-I:



c) Timelines and deliverables:

Supplier has to ensure the timely delivery of all deliverables and completion of all activities of the project in line with Project Plan submitted by Supplier and approved by Purchaser. Indicative timeframe of key deliverables/activities are provided below:

S. No.	Milestones	Timelines
Project Initiation		T*+0.5 months
1.	Detailed Project Plan	
2.	Resource Deployment Plan	
3.	Implementation, Rollout & Integration Plan	
4.	Capacity Building and Change Management Plan	
Assessment & Design (For all modules)		T+6 Months
5.	Draft Functional Requirement Specification (FRS)	T+3 Months
6.	Software Design Document (SDD) including Overall Solution Architecture, Networking Architecture, Security Architecture, Deployment Architecture, Integration Architecture and others	
7.	Business Continuity Plan	
8.	All Policies (such as Security policy, Backup and Recovery policy) and other design documents as required	
9.	Final FRS after incorporation of Client feedback	T+6 Months
10.	System Requirement Specifications (SRS)/Blueprint Design	

S. No.	Milestones	Timelines
11.	Data Migration Strategy	
12.	Finalization of Master data templates	
13.	Finalization of MIS and dashboard requirements	
Development/ Customization and Implementation		
Pilot		T+24 Months
14.	Sub-Phase 1	T+12 Months
15.	Sub-Phase 2	T+16 Months
16.	Sub-Phase 3	T+20 Months
17.	Sub-Phase 4	T+24 Months
Phase-I		T+28 Months
18.	Sub-Phase 1	T+16 Months
19.	Sub-Phase 2	T+20 Months
20.	Sub-Phase 3	T+24 Months
21.	Sub-Phase 4	T+28 Months
Phase-II		T+36 Months
22.	Module/ULB wise roll out in entire state	T+36 Months
Readiness of Data Centre (DC), DR and Near DR (NDR) Sites		T1+2 months
23.	Delivery of Hardware, Software & Networking Infrastructure including OEM Certificate	T1 is date of UAT completion of sub-phase 1
24.	Report on Installation & Commissioning of ICT components at DC and Near DR	
25.	Report on Compliance of BS 27001, ISO 9002 standards for DC and NDR	
26.	Readiness of DR on Cloud	
27.	Infrastructure and Security Audit by Purchaser	
Operation & Maintenance		
28.	Operation & Maintenance- Phase I	5 Years from Operational Acceptance-Pilot of Sub-Phase 1
29.	Operation & Maintenance- Phase II	From start of rolling out application in Phase-II locations till end of 5 Years from Operational Acceptance-Pilot of Sub-Phase 1
30.	Quarterly Report on Data Digitization	
31.	SLA Compliance Report (Monthly)	
32.	Security Audit and its compliance reports	
33.	Monthly Progress Report	
34.	Updated documents (e.g. User Manuals, FRS, SRS, SDD and training materials) quarterly	
35.	Other Project Related Documents (such as release documents) as and when required	
36.	MIS Reports (as and when required)	

d) Detailed Timelines for Stage 'Development/ Customization and Implementation':

S. No.	Activity	Timeframe
Sub-Phase 1		T+12 Months
1.	Development/Customization	T+8 months
2.	Readiness of master data and its migration to new database	T+9 months
3.	Requirement Traceability Matrix (RTM) and Test Cases for UAT	
4.	UAT and application security audit from CERT-In empaneled Agency (T1)	
5.	Training Material (i.e. handout, presentation, feedback form and e-content)	
6.	Training to pilot location users and submission of training feedback form	T+9.5 Months
7.	Pilot implementation (implementation in one city) and incorporation of feedback during pilot implementation	T+9 – T+11 months
8.	Operational Acceptance/G-Live of sub-phase 1 in pilot locations and STQC security audit certificate	T+12 months
9.	Rollout in Phase-I locations including data readiness, migration and training	T+12 – T+16 months
Sub-Phase 2		T+16 Months
10.	Development/Customization	
11.	Readiness of master data and its migration to new database	
12.	Requirement Traceability Matrix (RTM) and Test Cases for UAT	
13.	UAT and application security audit from CERT-In empaneled Agency	
14.	Training Material (i.e. handout, presentation, feedback form and e-content)	
15.	Training to pilot location users and submission of training feedback form	
16.	Pilot implementation (implementation in one city) and incorporation of feedback during pilot implementation	
17.	Operational Acceptance/G-Live of sub-phase 1 for one city and STQC security audit certificate	
18.	Rollout for Phase-I locations including data readiness, migration and training	T+16 – T+20 months
Sub-Phase 3		T+20 Months
19.	Development/Customization	
20.	Readiness of master data and its migration to new database	
21.	Requirement Traceability Matrix (RTM) and Test Cases for UAT	
22.	UAT and application security audit from CERT-In empaneled Agency	
23.	Training Material (i.e. handout, presentation, feedback form and e-content)	
24.	Training to pilot location users and submission of training feedback form	
25.	Pilot implementation and incorporation of feedback during pilot implementation	

S. No.	Activity	Timeframe
26.	Operational Acceptance/G-Live of sub-phase 1 in pilot location and STQC security audit certificate	
27.	Rollout in Phase-I locations including data readiness, migration and training	T+21 – T+24 months
Sub-Phase 4		T+ 24 Months
28.	Development/Customization	
29.	Readiness of master data and its migration to new database	
30.	Requirement Traceability Matrix (RTM) and Test Cases for UAT	
31.	UAT and application security audit from CERT-In empaneled Agency	
32.	Training Material (i.e. handout, presentation, feedback form and e-content)	
33.	Training to pilot location users and submission of training feedback form	
34.	Pilot implementation and incorporation of feedback during pilot implementation	
35.	Operational Acceptance/G-Live of sub-phase 1 locations and STQC security audit certificate	
36.	Rollout in Phase-I locations including data readiness, migration and training	T+24 – T+28 months

** Note: T is the date of either the 'award of work' notification issued by the Purchaser to the selected System Integrator OR signing of contract between Purchaser and selected System Integrator OR the meeting conducted by the Purchaser to kick-off the project; whichever happens the earliest.*

e) The schedule of activities listed below has been devised based on following assumptions:

- Separate Teams shall be deployed by the Supplier to undertake data digitization/migration, implementation of proposed solution and Training & Capacity Building.
- These Teams shall be available to work in parallel to each other. For instance, when the team designated for implementation of proposed solution is undertaking rollout of a particular sub-phase, the team for data digitization/migration can continue their tasks for the next sub-phase.
- Historical data should be digitized/migrated in reverse order i.e. first complete most recent year data, before undertaking digitization work of previous years. Digitization/Migration of the data will be tightly linked with the roll-out of services as the unavailability of digitized data will hamper the service roll-out.
- Tables given above highlight the broad timelines for implementation of this project. Please note that names of the ULBs, which would be covered in Phase-I (pilot and roll out) and Phase-II, would be finalized subsequent to signing of the Contract between the Purchaser and the Supplier. However, the phasing would be finalized based on priority of services at the time of submission of detailed Project Plan by the Supplier and at the sole discretion of Purchaser.

f) Operation Acceptance:

Supplier shall obtain the Operation Acceptance Certificates from the Purchaser for each sub-phase, Phase-I rollout and Phase-II rollout.

Operational Acceptance – Pilot (Sub-phase)

After successful pilot completion, Supplier shall submit a report to obtain the **Operational Acceptance-Pilot** (separately for each-sub phase). In order to get Operational Acceptance-Pilot Certificate, following activities relating to the Pilot implementation must be completed:

- FRS/SRS sign-off by Purchaser
- Purchaser's Approval of all related deliverables of Supplier as specified in this Section of RFP
- Testing by Supplier including Functionality Test, Database Test, Integration Testing, Unit Test, System Test, Stress test and Load/ Performance test.
- UAT completion by Purchaser
- Application Security Audit (Agency for this audit will be engaged by Department) and compliance to audit observation by Supplier
- Readiness of Data Centre, Near DR and DR sites with all proposed ICT infrastructure including SLA monitoring tool
- Completion of Training and Change Management Workshops in pilot locations
- Completion of data migration, digitization and master data related activities for pilot locations
- Delivery of all transactions of services/management functions relating to concerned sub-phase for a period of atleast one month through the on-line system from the date of Government Order* in pilot locations
- Completion of pilot for atleast 80% of modules of concerned sub-phase

**Department of Local Government will issue a Government Order regarding effective date of delivery of services through on-line mode only. All manual processing of services will cease with effect from issue of Government Order. In case Department of Local Government chooses to opt for manual operation of select services at select ULB offices, Department will issue the Government order accordingly."*

Based on the above and only after being completely satisfied that all the concerned users of pilot locations have access to the System and are using the System for the respective functional areas, the Purchaser shall issue **Operational Acceptance – Pilot** for particular sub-phase.

Operational Acceptance – Go-Live (ULB and module wise)

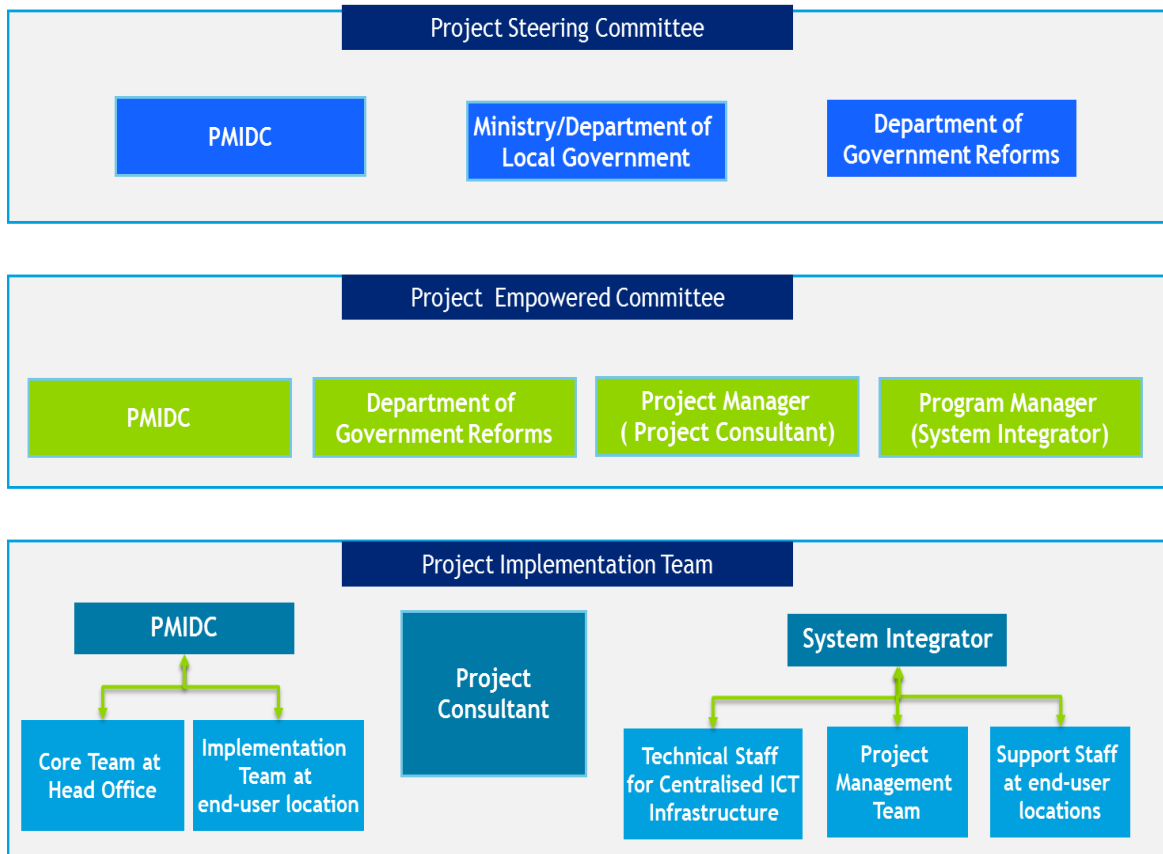
After successful Operation Acceptance – Pilot, system shall be Go-Live at all the remaining locations of Phase-I and Phase-II. Supplier may submit a report to obtain the **Operational Acceptance- Go-Live** (Phase wise OR ULB and module wise) as and when required. To obtain Operational Acceptance – Go-Live Certificate, following activities relating to the Go-Live must be completed:

- Submission of updated FRS/SRS
- Submission of all updated documents (such as User Manuals, design documents and training material)
- Readiness of Data Centre, DR and Near DR site with all proposed ICT infrastructure/Services including SLA monitoring tool
- Completion of Training and Change Management Workshops
- Completion of data migration, digitization and master data related activities
- Delivery of all transactions of services/management functions relating to concerned sub-phase for a period of atleast one month through the on-line system from the date of Government Order* in pilot locations

Based on the above and only after being completely satisfied that all the concerned users of related locations have access to the System and are using the System for the respective functional areas, the Purchaser shall issue **OPERATIONAL ACCEPTANCE – GO-LIVE** (Phase wise OR ULB and module wise).

14. Project Governance Structure

- a) For the success of the project, it is imperative to put an appropriate Governance Structure in place. The roles and responsibilities of all the stakeholders should be clearly identified to ensure clarity of strategic control through the project implementation and beyond. This would ensure adequate buy in for the project across all levels/ stakeholders of Department of Local Government.
- b) The below 3-tier project governance structure has been proposed to monitor and control the project implementation.



c) Roles & Responsibilities

The key roles and responsibilities of each tier of above project governance structure are described as below:

- i. Project Steering Committee:
 - a. Decision on the changes in regulation & policies
 - b. Issuance of project related guidelines as appropriate

- c. Decision on major changes to Project components
 - d. Holding project progress meeting atleast once in a quarter period
 - e. Decision related to fund allotment and its disbursement
 - f. Decision on various concerns raised by Empowered Committee
- ii. Project Empowered Committee:
 - a. Responsible for taking all middle level decisions related to implementation of the project such as decision on change management issues, approval of deliverables and operational acceptance of System
 - b. Hold meetings at least once every month to review the progress made in relation to the project during the implementation period and once every three months during the operation period.
 - c. Moderate interactions with external stakeholders
 - d. Resolve issues that might occur during implementation, which are relevant to EC
- iii. Project Implementation Team:
 - a. PMIDC
 - a) Ensure time bound implementation of the project and adherence to its objectives
 - b) Oversee and monitor the work performed in the project
 - c) Provide inputs to EC members on Project status
 - d) Day to day monitoring of the project
 - e) Coordination between stakeholders
 - f) Manage first level of escalation
 - b. Project Management Consultant
 - a) Key interface between PMIDC and System Integrator
 - b) Assist in meetings with PMIDC and System Integrator to discuss about the project progress, issues to be addressed, way forward, review the project milestones, etc.
 - c) Assist in preparing progress reports, review of the deliverables submitted by System Integrator, monitor project progress, etc.
 - d) Assist PMIDC in work plan management
 - e) Assist PMIDC in scope management
 - f) Assist PMIDC in project governance and issue management
 - g) Assist in addressing the issues affecting the project progress
 - c. System Integrator
 - a) Responsible for entire scope of work and SLAs as mentioned in the RFP
 - b) Resource mobilization, planning and deployment
 - c) Participation in the regular meetings including steering committee meeting, meetings with the project management team, etc.
 - d) Keep the project on track
 - e) Ensuring timely and quality deliverables
 - f) Making client presentations on these deliverables
 - g) Co-ordinate with PMIDC for delivery, testing and acceptance schedules for solution
 - h) Planning and responding to contingencies

- i) Monitoring/ review project progress and its team members work
- j) Managing the entire project end to end.
- k) Analyze the technical and functional requirements
- l) Design & Customize the solution in line with requirements
- m) Prepare/Develop the project deliverables
- n) Impart training and conduct change management workshop
- o) Implement the project
- p) Provide operation & Maintenance support
- q) Escalate to 'Project Empowered Committee, if any issue, in project execution & delivery