

**REQUEST FOR QUALIFICATION (RFQ)
CUM
REQUEST FOR PROPOSAL (RFP)
FOR**

**APPOINTMENT OF MASTER SYSTEM INTEGRATOR
FOR
DESIGN, SUPPLY, INSTALL, TEST, INTEGRATE,
COMMISSIONING, OPERATION AND MAINTENANCE
OF ICT COMPONENTS IN CLUSTER A1 OF
ACTIVATION AREA (Retender)**

**AT
DHOLERA SPECIAL INVESTMENT REGION, GUJARAT
ACTIVATION AREA**

**VOLUME-II
SCOPE OF WORK**

**Dholera Industrial City Development Limited (DICDL)
6th Floor, Block No. 1 & 2, Udhog Bhavan,
Sector-11, 'GH-4' Circle, Gandhinagar – 382017
Gujarat, India**

March 2020

Table of Contents

Reference Documents:	1
List of Abbreviations	2
List of Figures	8
1 INTRODUCTION	9
1.1. Project background.....	9
1.2. Information & Communication Technology Overview	10
1.3. Project Phasing	11
1.4. Document overview.....	15
2. General requirements	16
2.1. General business requirements	16
2.2. Architecture principles.....	16
3. Detailed scope of work, business, Functional, Non-functional, Technical requirements, Operation and maintenance	20
3.1. Basic Network Infrastructure Work package	42
3.1.1. Citywide Networks - Ducts & Dark Fiber & Network passive.....	42
3.1.2. City wide networks - Network Active	66
3.1.3. City wide sensors (e.g. sensors network for utilities)	74
3.1.4. City Integrated Operations Platform	78
3.1.5. Basic surveillance solution.....	110
3.1.6. Hosting: On premise and Cloud	128
3.1.6.1. Hosting on GSDC Cloud at Gandhinagar	129
3.1.6.2. Hosting on ABCD Server room	131
3.1.7. Network Operations Center	134
3.1.8. Functional Requirement of Server room Non-IT Infrastructure Setup	135
3.1.9. Information Security	141
3.1.10. Enterprise and Network Management System.....	148
3.2. City Applications Work Package.....	154
3.2.1. ERP suite of Applications	154
3.2.2. Master data governance & Data Migration	183
3.2.3. GIS Integration.....	190
3.2.4. City Applications – eGovernance Integration	190
3.2.5. City Applications - Web Portal	191
3.2.6. City Applications - Multi service kiosk	198
3.2.7. City Applications - Mobile applications	201
3.2.8. Process workflow.....	203
3.2.9. City Applications – Non-Functional requirements	206
3.3. Integrated Operations Work Package.....	210
3.3.1. CIOC – City Integrated Operations Center.....	210
3.3.2. CIOC – Technical Specification for Control Room Interiors	215
3.3.3. CIOC - Surveillance and video analytics	234
3.3.4. CIOC - AV Hardware & Software.....	247
3.3.5. CIOC - Collaboration Solution for Helpdesk	250
3.3.6. CIOC – Dashboards & Reporting	258
3.3.7. Integrated Building Management System	267
3.3.8. Variable message Signboards	273
3.4. Project deliverables / Documentation	283
3.5. Training and capacity building	284
3.6. Standards.....	286
3.7. Bill of Quantity	289
3.8. Technical Specifications:	294
4. Operation & Maintenance Phase	352
4.1. SCOPE OF WORK, DELIVERABLES & TIMELINES	352
4.1.1. Asset Management Services.....	352
4.1.2. Preventive Maintenance Services.....	352

4.1.3.	Corrective Maintenance Services	353
4.1.4.	Configuration and reconfiguration/rollback of equipment's/network/services	353
4.1.5.	Vendor Management Services.....	354
4.1.6.	Network Management Services.....	354
4.1.7.	Server Management Services	354
4.1.8.	Backup & Recovery Management Services.....	355
4.1.9.	Help Desk Support	355
4.1.10.	Database management services	356
4.1.11.	Storage Administration and Management Services	357
4.1.12.	Security Administration and Management Services	357
4.1.13.	ISO 27001 and ISO 20000 certification and sustenance for 5 Years	358
4.2.	Table for O&M (Operation and Maintenance) Reports	359
4.3.	Manpower Resource Table at DSIR.....	360
4.4.	Minimum Qualification, Relevant Experience & Certifications.....	360
5.	Implementation schedule (activities, milestones and deliverables)	362
5.1.	Annexures	363
5.1.1.	Server Room Layout	363
5.1.2.	Server Room Electrical SLD Layout	363
5.1.3.	City DICDL Building 1st Floor ICT Rooms Layout.....	364
5.1.4.	City DICDL Building 2 nd - 8 th Floor ICT Rooms Layout.....	365
5.1.5.	City DICDL Building ICT Shaft Schematic:.....	365
5.1.6.	BEC Building Ground Floor ICT Rooms Layout	366
5.1.7.	BEC Building First Floor ICT Rooms Layout	366

Reference Documents:

The soft copy of the following reference document list is available in DICDL office.

Sr. No	Doc Ref. No	Title
1	WIPRO-TP2E-AA-ICT-PMG-MS-0002	ICT Infrastructure requirements at ABCD Buildings
2	WIPRO-TP2E-AA-ICT-PMG-MS-0002	ICT Infrastructure requirements at Service Areas
3	WIPRO-TP2E-AA-ICT-PMG-MS-0002	CIOC AV / UC Concept Design
4	WIPRO-TP2E-AA-ICT-PMG-MS-0002	Street Light Integration
5	WIPRO-TP2E-AA-ICT-PMG-MS-0002	Baseline Functional Requirements
6	WIPRO-TP2E-AA-ICT-PMG-MS-0002	CONCEPTUAL DESIGN PLANNING FOR DATA CENTRE
7	WIPRO-TP2E-AA-ICT-PMG-MS-0002	Wi-Fi Coverage Mapping
8	WIPRO-TP2E-AA-ICT-PMG-MS-0002	ICT Infrastructure requirements at ESR and MBR
9	WIPRO-TP2E-AA-ICT-PMG-MS-0002	List of City Wide Sensors
10	WIPRO-TP2E-AA-ICT-PMG-MS-0003	Design Document for Wi-Fi Network
11	WIPRO-TP2E-AA-ICT-PMG-MS-0003	Conceptual Design Planning for Surveillance System
12	WIPRO-TP2E-AA-ICT-PMG-MS-0003	ITMS Design Document
13	WIPRO-TP2E-AA-ICT-PMG-MS-0003	OSP Design Document
14	WIPRO-TP2E-AA-ICT-PMG-MS-0003	Network Design Document
15	WIPRO-TP2E-AA-ICT-PMG-MS-0003	Design Document for SCADA Integration
16	WIPRO-TP2E-AA-ICT-PMG-MS-0004	Design Approach for Data Centre
17	WIPRO-TP2E-AA-ICT-PMG-MS-0004	Data Centre Design Final Technical Solution Document
18	WIPRO-TP2E-AA-ICT-PMG-MS-0004	Data Center Network Infrastructure
19	WIPRO-TP2E-AA-ICT-PMG-MS-0004	Design Approach for Disaster Recovery Center
20	WIPRO-TP2E-AA-ICT-PMG-MS-0004	Solution Document on Emergency and Disaster Management System
21	WIPRO-TP2E-AA-ICT-PMG-MS-0004	Functional Requirements Specification
22	WIPRO-TP2E-AA-ICT-PMG-MS-0005	CIOC Design for Audio Visual Systems, Digital Signage, Unified Communications and Dashboards
23	WIPRO-TP2E-AA-ICT-PMG-MS-0005	Cybersecurity Solution Approach
24	WIPRO-TP2E-AA-ICT-PMG-MS-0005	Big Data Solution Design
25	WIPRO-TP2E-AA-ICT-PMG-MS-0005	Overall IOT/ Integration document
27	WIPRO-TP2E-AA-ICT-PMG-MS-006	Submission of Final Draft of RFP (Old scope)

List of Abbreviations

Abbreviation	Definition
3DS	3D Studio
4K	Ultra-High-Definition Resolution
AAA	Authentication, Authorization and Accounting
AC	Audioconferencing
AFD	Automatic Fire Detection
AMI	Advanced metering infrastructure
AML	Advanced Mobile Location
AMS	Asset Management System
AMS	Asset management system
AMWI	Audio Message Waiting Indicator
AMX	Manufacturer Name
API	Application programming interface
ARC	Alarm Receiving Center
ASD	Aspirating Smoke Detection
AV	Audio-Visual
AVLS	Automatic Vehicle/Person Location Subsystem
BAS	Building Automation Systems
BIM	Building information model
BMS	Building Management System
BoM	Bill of Materials
BoQ	Bill of Quantity
BOS	Building Operating System
BYOD	Bring Your Own Device
C&SE	Collaboration & Special Environments
CAD	Computer aided design
CATx	Structured Cabling Type
CCC	Command & Control Centre
CCTV	Closed circuit television
CEPT	Centralized industrial effluent treatment Plant
CH ₄	Methane
CIOC	City Integrated Operating Center
CMMS	Centralized maintenance management system
CMS	Content Management System
CNCF	Cloud Native Computing Foundation
CO ₂	Carbon dioxide
COBie	Construction Operations Building Information Exchange
Codec	Coder - decoder
CRM	Customer Relationship and Management
CSD	Combined Services Drawing
CTI	Computer Telephony Integration
Dante	Audio Protocol Name

DCC	Digital Community Center
DCIM	Data Center Infrastructure Management
DGCA	Director General of Civil Aviation
DISH	Director Industrial Safety & Health
DMS	Document Management System
DPS	Differential Pressure Switch
DSDI	Dholera spatial data infrastructure
DSIR	Dholera Special Investment Region
EAP	Enterprise Application Platform
ECB	Emergency Call Box
eCW	Enhanced Compression Wavelet
EDMS	Emergency & Disaster Management System
EISEC	Enhanced Information Service for Emergency Calls
ERMS	Email Response Management System
ERP	Enterprise resource planning
ERT	Elevated reserve tank
EWS	Early Warning System
FAQ	Frequently Asked Question
FAS	Fire Alarm System
FAT	Factory Acceptance Test
FFE	Furniture, Fixtures, Equipment
FM	Flow Meter
FM	Facility Management
FST	Functional Support Team (room)
GALILIO	Global satellite navigation system by European union
GC	General Contractor / Main Contractor
GCS	ground control station
GDSP	Geoanalytics decision support platform
GeoJSON	Extension of JSON file format
GIS	Geographical information system
GOG	Government of Gujarat
GPRS	General Packet Radio Service
GPS	Global positioning system
GRT	Ground reserve tank
GSDMA	Gujarat State Disaster Management Authority
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
H.323	Protocol Definition
H ₂ S	Hydrogen sulfide
HCL	Hydrochloric acid
HD	High-Definition Resolution
HDMI	High Definition Multimedia Interface
HH	Hand hole
HLD	High Level Design document
HQ	Head Quarters

HSE	Health, Safety, Environment
HTTPS	Hypertext Transfer Protocol (Secure)
HVAC	Heating, Ventilation and Air Conditioning
I/O	Input / Output
IAT	Integrated Application Test
IBMS	Integrated Building Management System
ICC	Incident Command Centre
ICT	Information and Communication Technology
IFC	Issued for Construction
IFC	Industry Foundation Classes
IMD	Indian Meteorology Department
INCOIS	Indian National Centre for Ocean Information Services
IoT	Internet of things
IP	Internet Protocol
IP Rating	Ingress Protection rating
IR	Infra-Red
IR	Invoice Receipt
IRNSS	Indian regional navigation satellite system
ISO	International Organization for Standardization
ISO 19115:2003	Schema for GIS
ISR	Institute of Seismological Research
IT	Information Technology
ITMS	Integrated Traffic Management System
JPG	Joint photographic group (file format for images)
JSON	Java Script object notion
KML	Keyhole markup language (file format used by google earth)
KMZ	Zipped KML file (file format used by google earth)
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Data exchange format
LED	Light Emitting Diode
LiDAR	Light detection and ranging
LLD	Low Level Design
LOD	Level of Development
LULC	Land use Land cover
MAN	Metro Area Network
MCCP	Motor Control Center
MH	Manhole
Mic	Microphone
Micro-DP	DP = Display Port
MQTT	Message Queuing Telemetry Transport
MrSid	Multiresolution seamless image database (file format for images)
MSI	Master system integrator
MTBR	Mean Time Between Repair
MTTR	Mean Time To Repair

NARAR	Need assessment and requirement analysis report
NDMA	National Disaster Management Authority
NH3	Ammonia
NMS	Network Management System
NO	Nitric oxide
NO2	Nitrogen dioxide
NOC	No Objection Certificate (eGovernance)
NOC	Network operations Centre
NSDE	National spatial data exchange
NVMS	Network Video Management Software
NVR	Network Video Recorder with integrated VMS
O&M	Operation & Maintenance
O3	Ozone
OEM	Original Equipment Manufacturer
OGC	Open geospatial consortium
OGC-CSW	Open Geospatial Consortium, Catalog Service for the Web
OIC	Open Interconnect Consortium
OSM	Open street map
OWS	Operator Work Station
PA	Public Address
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PDF	Portable document format (Acrobat reader file format)
PLC	Programmable logic Controller
PM 10	Particulate matter
PM 2.5	Particulate matter
PNG	Portable network graphics (file format for images)
PO	Purchase Order
QoS	Quality of Service
QSC	Manufacturer Name
R&D	Research and Development
RoI	Return on investment
ROV	Remotely Operated Vehicle
RTLS	Real Time Locating System
RTU	Remote terminal unit
RX	Receiver
SACS	Security Access Control System
SAN	Storage Area Network
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SCM	Supply chain management
SCU	Single common unique
SDD	System Design Document
SDI	Spatial data infrastructure
SDLC	Software Development Life Cycle

SDUMM	Spatial data maintenance and management
SEOC	State Emergency Operation Center
SHM	Structural Health Monitoring
SHP	Shape file format (used for GIS file)
SIP	Session initiation Protocol
SLA	Service Level Agreement
SO2	Sulfur dioxide
SQL	Structured query language
SRM	Supplier Relationship Management
SRS	Software Requirements Specification
SSD	Single Services Drawing
STP	Sewer Treatment Plant
T&D	Transmission and distribution
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
TETRA	Terrestrial Trunked Radio
TIFF	Tagged image file format (file format for images)
TIN	Triangulated irregular network
TV	Television
TX	Transmitter
UAT	User Acceptance test
UC	Unified Communications
UI	User Interface
UMM	Update, Maintenance and Management
UNA	User need assessment
UOM	Unit of Measurement
UPAN	Utility Plant Area Network
USB	Universal Serial Bus
USLS	Ultrasound level sensor
UX	User Experience
UX/UI	User Experience/User Interface
VC	Videoconferencing
VCA	Video Content Analytics
VLAN	Virtual Local Area Network
Vlv	Valve with actuator
VM	Visual Management
VMS	Video Management Software
VMS	Variable Message Signboard
VOC	Volatile organic compound
VTMS	Vehicle tracking management system
VTs	Vehicle Tracking System
WAN	Wide Area Network
WBS	Work Breakdown Structure
WCS	Web coverage service
WFS	Web feature service
WLAN	Wireless Local Area Network

WMS	Web map service
WQT	Water quality sensor
WTP	Water Treatment Plant
XLS	Microsoft excel file format
XML	Extended markup language

List of Figures

Sr. No.	Figure No.	Description
1	Figure -1	DMIC and the eight cities
2	Figure - 2	DSIR ICT Cluster A-1(Service Area & ABCD)
3	Figure - 3	ICT requirement domains for Dholera
4	Figure - 4	Overall System architecture for DSIR with Smart City components
5	Figure - 5	Cluster - A1
6	Figure - 6	Proposed ICT duct banks
7	Figure - 7	Manhole dimensions
8	Figure - 8	Fiber optic Schedule for Cluster A-1 Area
9	Figure - 9	Fiber Optic Backbone network
10	Figure - 10	Junctions layout for Cluster-A1
11	Figure - 11	ICT Ducts Reservation proposal
12	Figure - 12	Smart City schematic layout
13	Figure - 13	FOC schedule for Cluster A-1
14	Figure - 14	Server Room (SPV Building) Network Architecture
15	Figure - 15	City Wide Area Network and Integration Points
16	Figure - 16	Logical diagram for early warning sensors
17	Figure - 17	Architectural Overview of City Integrated Operations Platform
18	Figure - 18	Network layer of City Integrated Operations Platform
19	Figure - 19	Enterprise Service Bus for CIOP
20	Figure - 20	Exchange/Message Broker for CIOP
21	Figure - 21	API Service Management
22	Figure - 22	Connectivity Blocks for CIOP
23	Figure - 23	IoT Building Blocks
24	Figure - 24	Logical Diagram Server Room (SPV Building)
25	Figure - 25	Indicative/Conceptual Floor Plan (Server Room)
26	Figure - 26	Electrical Single Line Diagram
27	Figure - 27	Multiservice Kiosk high level architecture
28	Figure - 28	Control Room design overview (illustrative)
29	Figure - 29	CIOC – Entrance view (illustrative)
30	Figure - 30	CIOC - Side view - 1 (illustrative)
31	Figure - 31	CIOC - Side view - 2 (illustrative)
32	Figure - 32	CIOC – Control Desk (illustrative)
33	Figure - 33	CIOC- Lattice paneling (illustrative)
34	Figure - 34	CIOC - False ceiling (illustrative)
35	Figure - 35	Analytics dashboards showcasing various parameters
36	Figure - 36	Screen layout with widgets (indicative)
37	Figure - 37	Video Wall for Surveillance (indicative)
38	Figure - 38	CCTV Display wall

1 INTRODUCTION

This section will provide insight in the background of the project, a document overview and the role of this document in the project and the future.

1.1. Project background

The Government of India has envisaged the development of the Delhi Mumbai Industrial Corridor (DMIC) along the alignment of the proposed Multi-Modal High Axle Load Western Dedicated Freight Corridor (DFC) between Delhi and Mumbai, covering an overall length of 1,483 km.

The Delhi Mumbai Industrial Corridor Development Corporation Limited (DMICDC), a special purpose company, was incorporated to establish, promote and facilitate development of the DMIC Project.

The DMIC is set to provide space for high-tech industrial zones spread over six states, with the goal to expand India's Manufacturing & Services base and have the area become the Global Manufacturing and Trading Hub. The whole project is one of the largest infrastructure projects in the world with a total estimated investment of \$100 billion.

In 1st Leg of the DMIC project, DMICDC is developing eight industrial cities/nodes. Dholera Special Investment Region (DSIR) is the largest of the eight industrial smart cities in Phase1 of the project. One of these cities is Dholera and is located approximately 100 kilometers South-West of Ahmedabad in the state of Gujarat.

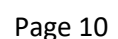
The Dholera Special Investment Region Development Authority (DSIRDA) has the responsibility of planning and development of DSIR and will encompass the function of administering government land within DSIR. An DICDL named Dholera Industrial City Development Limited (DICDL) has been created between the Central Government (DMICDC Trust) and the State Government (DSIRDA) of Gujarat to implement the project.

DSIR has been planned over an extensive area of 920 square kilometers, with the development being divided into three phases. First, an activation area of 22.5 square kilometers, which is currently under construction, will be developed. This area has an optimum mix of land uses (industrial, residential, mixed use, recreation and tourism). The area is estimated to house 92,600 residents and offer close to 80,000 jobs (including for floating population).

After the activation area is completed and industries and residents have settled in Dholera, phase 1 will be developed in which the city will grow to 153 square kilometers. When phase 1 has finished and there is demand for more city space, phase 2 will be developed. Once all the phases are finished, Dholera will be about 920 square kilometers, which is greater than the size of Singapore, and will have an international airport.

The Development Plan for DSIR is available at: www.dmicdc.com and www.dholerasir.com

The DICDL website can be found at: www.dicdl.in and <https://dicdl.gujarat.gov.in>



In specifying the ICT requirement for a Smart City, an understanding of the dynamics of citizens, systems, technology, infrastructure, environments and future ways of living should be considered. The fundamental

starting point for this is the citizen (of Dholera) and their user journey in the new Smart City, with 'ease-of-use' as the key driver. Understanding global city procedures, processes and ways of working are important in designing and implementing the ICT for Dholera.

The ICT requirements for Smart Dholera have been split into various work packages. Some of the components being covered are shown in the diagram below.

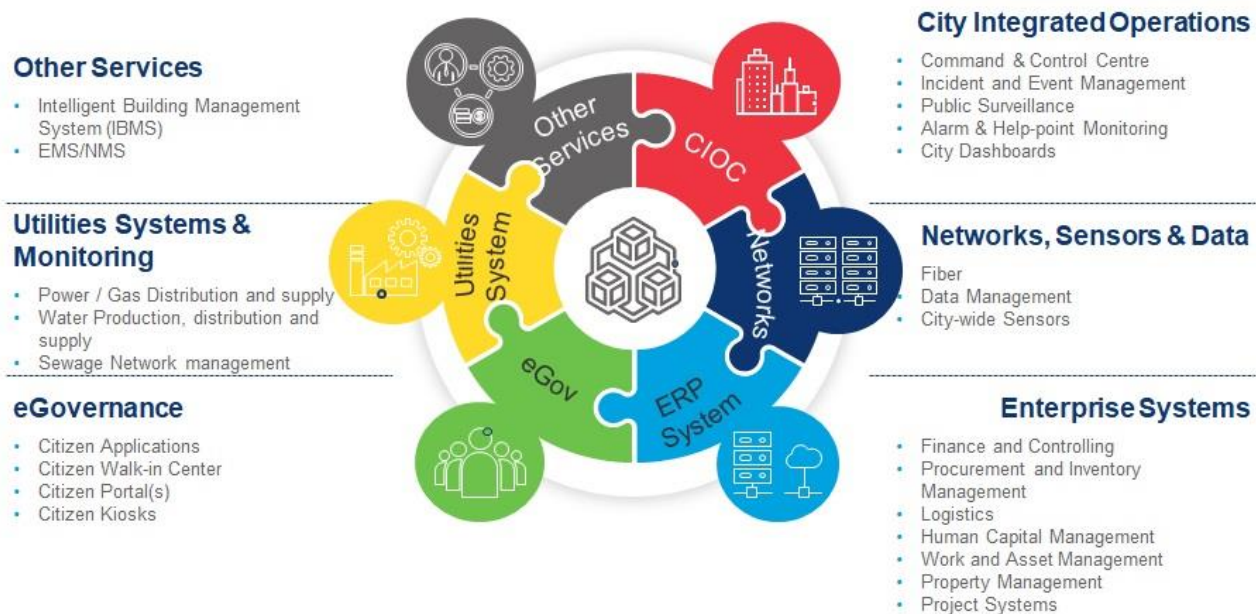


Figure 3 - ICT requirement domains for Dholera

Government of Gujarat through its agency DSIRDA and Delhi Mumbai Industrial Corridor Corporation Ltd., have undertaken development of futuristic smart city Dholera SIR by deploying sustainable and state of the art technologies with the objective of expanding the manufacturing and services base in the state of Gujarat. Dholera SIR (www.dicdl.in and dicdl.gujarat.gov.in) will have smart and sustainable trunk infrastructure in all disciplines of city namely, citizen's safety, transportation, water, power, wastewater, drainage, urban design etc. Dholera SIR is being developed by DICDL - Dholera Industrial City Development Ltd. (DICDL), a JV of GoG and DMICDC. M/s AECOM are the program managers for the new cities (PMNC) and M/S Wipro Ltd are the ICT consultants for Dholera SIR.

1.3. Project Phasing

The Project and its components will be implemented in a phased manner, which will broadly be in-line with both the DICDL requirements and the availability of on-site civil infrastructure. If the respective on-site civil infrastructure is ready before time, the MSI's Project plan shall be flexible to advance the implementation of some work packages before time at no additional cost. Some Project components will be implemented in parallel under different phases. The order of implementation will be subject to revisions from time to time based on Project priorities as decided by the DICDL.

Note that the phasing list is not all inclusive and the MSI shall refer to other sections of the RFQ cum RFP and the Bill of Quantities (BoQ) for exact requirements of components needed.

It is envisaged to implement ICT infrastructure for Dholera.

- Cluster A-1 will be taken up comprising of influence area 7.48 Sq. km covering 7(seven) Service area building and 6 (six) major road junctions, for which the boundaries are as defined by DICDL in figure 2. ICT Cluster A-1 will also include setting up of all the ICT infrastructure for ABCD-1 complex, which

includes DICDL building, BEC, Auditorium, utilities buildings, Service area buildings, etc.

- b. Service Areas house various electrical, mechanical and ICT equipment and are essential for enabling the ICT requirements for the utilities within the Cluster – A1 of Dholera Activation Area. Current Scope of MSI is to implement the ICT infrastructure (Network, Switching, cabling, etc.) and related infrastructure for 7 Service Areas of Cluster A1. MSI need to work closely with the EPC contractor hand in hand and finalize the port requirement in line with discussions with DICDL and provide the necessary inputs to Service Area building contractor for Provisioning of necessary requirements like inside cable path ways, cable trays, conduits, etc. which are required for ICT implementation.

The table shown below showcases the high-level scope of work (but not limited to) for Service area buildings;

Item	Whose scope
HVAC	Service area EPC contractor
UPS (ICT & field equipment's)	Service area EPC Contractor
False ceiling & Flooring	Service area EPC Contractor
Generator & Diesel day Tank	Service area EPC contractor
Rack	ICT MSI
BMS & CCTV	Service area EPC Contractor
Tower	Telecom service provider
Furniture	Service area EPC contractor
LAN & Telephonic cabling	Service area EPC Contractor

The objective of the Service Area Building Layout is to provide the infrastructure requirements necessary to house the city utilities in each of the respective Service Areas. The design and engineering details presented in the RFP document provides a brief about typical Service Area and must be replicated in all identified Service Areas; furthermore, they should also comply with all applicable standards, global practices and the requirements specified by DICDL and other stakeholders of the project.

The proposed Service Area buildings would be having electrical, mechanical and ICT equipment required to provide reliable service throughout DSIR service areas considered for this project scope.

The following list of services and systems will be part of Service Area, however it is not part of MSI Supply under this RFP

Sr. No.	Equipment
1	Cellular towers (desirably monopole for use by 7-8 telecoms)
2	RF boxes for towers (to be provided by telecom service providers)
3	Compact distribution transformers for power supply
4	Electric distribution cabinets (for the vicinity)
5	FO to RF convertors for antennas
6	Street light control and metering equipment
7	Control/monitoring equipment for water, gas etc.
8	Radio transmitter/repeater
9	Cable TV equipment
10	Microwave towers
11	Uninterruptable Power Supply (UPS) and small diesel generator (DG)
12	Other smart city equipment etc.

Site Selection, Building Design and Area Statement

This section mentions the information regarding site selection, building design and space requirement of equipment for a typical Service Area to be constructed by EPC contractor.

- **Site Selection**

The key parameters considered for site selection include the following:

- The minimum site size is 21.5m X 18.5m (397.75 sq. m).
- Each site is having direct access from the city road.
- In addition to the building, each site has adequate space for the erection, commissioning and installation of two monopole shared cellular towers which will host the cellular/RF antennas of approximately 7-8 Gujarat circle telecom operators.

- **Building Design**

The key parameters considered for building design:

- The Service Area building has emergency vehicle access on three sides. The minimum allowable access from the perimeter wall is 4.5 meters.
- Each proposed Service Area building has the following duct bank provisions:
 - One dedicated electrical duct bank
 - One dedicated street light duct bank
 - Two (including one redundant) duct banks for ICT services entering the building.

- **Area Statement**

The following is a list of equipment and the space considered for each in the Service Area buildings:

Sr.	Equipment	Location	Size
1	Cellular towers	Open Ground	4 X 4 meters
2	Telecom equipment/ RF boxes for towers	Second Floor	50 square meters
3	Compact distribution transformers for power supply	Ground Floor	3.5 X 2 meters
4	42u FO cabinets for city fiber and FTTx	First floor	1 X 1 meter
5	42u FO to RF convertors for antennas	Second floor	1 X 1 meter
6	Street light control and energy metering equipment	Ground Floor	1.5 X 1 meter
7	Control/monitoring equipment for water, gas etc.	Ground Floor	1 X 1 meters each
8	Tubular tripod type towers for radio taxi (and police)	Rooftop	1.5 X 1.5 meters
9	42u rack for cable TV (CATV) equipment	First Floor	1 X 1 meter
10	Microwave towers	Cellular tower	
11	Uninterrupted power supply (UPS)	First Floor	4.6 X 3.9 meters
12	42u rack for smart city ICT equipment etc.	First floor	1 X 1 meter
13	Maintenance-free earthing pit	Open Ground	300mm X 300mm
14	Diesel generator	Open Ground	3 X 2 meters

DSIR High Level Implementation Overview:

Implementation Plan	Tasks
Mobilization / Inception	MSI Contract Sign-off
	Inception Report
	Project Management Plan
	Fully developed Project Plan/ Schedule for all the resources (including procurements)
	Manpower Mobilization, setup of project/site offices (one each at Dholera and Gandhinagar)
Basic network and other Infrastructure	Design, Engineering and Procurement
	Backbone Fiber connectivity along with Duct bank laying between ABCD 1 to Service area building inside activation area.
	Active + Passive implementation for cameras, sensors, VMS, etc.
	Laying of Dark Fiber for provisioning FTTx services to users across Cluster A1.
	City wide sensors (environmental, meteorological, gas, etc.), Citywide VMS, Smart network for all ICT enabled city provided services
	EMS/NMS, Network Access Control & Authorization, End Point security, Set up server room and connectivity between Server room in ABCD building and POP – I in Service Area No. 25
City Applications	Design, Development, Integration and Implementation of City apps as briefly stated below and detailed later
	City apps + Portal Go-live
	e-Gov, City Portal, ERP (HR, Payroll, Asset management, CRM, Finance management, scheduling, workflow, projects & works management, contract management, utility management and billing, etc.)
	Industry Specific Solutions for Utilities, Set-up of BI/Analytics solution, etc.
	Mobile Application Platform
	Integration with State and Central government systems as well as other third-party applications/systems as needed by the DICDL
Integrated Operations	City Integrated Operation Centre
	Integrated Operations, IBMS integration
	Monitoring and control by integrating SCADA systems, surveillance, etc.
Smart City	Variable Message Sign boards, Analytics
Supporting Work Packages	Scaling of Dashboards / Reporting / City's cockpit Centralized processing, City optimization, etc.
Misc.	Miscellaneous and remaining works

1.4. Document overview

The document presents the full project overview to develop the ICT for the Smart City of Dholera and covers all areas as described in Figure 3. Not all areas are required from the start as the city will only have limited numbers of citizens and industries at the start. While the number of residents and industries grows the need and demand for more services will grow too. To highlight this, the sections have been divided into subsections that describe the requirements and scope of services of work packages. Following work packages have been defined:

- Basic Network Infrastructure
- City applications
- Integrated Operations

2. GENERAL REQUIREMENTS

2.1. General business requirements

Below general principles are applicable to every area of the design, implementation and support. Every design needs to be validated against below principles.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
GBR-GBR-01	General Business Requirements	GBR	Business Centric	A business first approach to innovative deployment of technology that will align and drive business value with realistic costs for our Information Services, Strategy and Technology and the underlying architecture and Industry Standard Solutions
GBR-GBR-02	General Business Requirements	GBR	Agile	Entire Framework will be modular and agile to allow componentized solutions which can be delivered iteratively and orchestrated together to fulfill end-to-end business processes and best practices.
GBR-GBR-03	General Business Requirements	GBR	'As a Service' approach	Approach to the adoption of services rather than assets will be considered within all aspects of our business and technology deployments and operation.
GBR-GBR-04	General Business Requirements	GBR	Information consumable anywhere	All information is made available and consumable that is protected but accessible to any user. With the only limitation being the authorization of the user itself
GBR-GBR-05	General Business Requirements	GBR	Technology Lock-in	The right choice of technology that addresses the immediate need but is interoperable with other technologies as they all evolve. Avoiding lock-in to a specific Technology, vendor and or proprietary services.
GBR-GBR-06	General Business Requirements	GBR	Right Level of Security	Adopt the right level of security to protect and manage our Infrastructure and information assets that is pragmatic and practical
GBR-GBR-07	General Business Requirements	GBR	Applications	Consideration for rationalization against the full application portfolio for simplification not expansion, Replacement should consider reuse and a "many for one" approach versus "one for one" - like for like and avoiding the development of bespoke applications

2.2. Architecture principles

Below Architectural principles needs to be applied to every design. Every design option needs to be evaluated in consideration of the below applicable guidelines. Any exceptions to the below principles needs to be documented and approved by the design authority.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ARP-ARP-01	Architecture Principles	ARP	Information is accessible	Information is accessible in a timely manner for users to perform their business functions. Information is presented and provided to the users in a structured, timely and consistent manner such that the information is readily available and accessible.
ARP-ARP-02	Architecture Principles	ARP	Information is defined	Defining the Enterprise Information models - Information is defined consistently throughout the enterprise and the definitions are understandable and available to all users.
ARP-ARP-03	Architecture Principles	ARP	Re-use before buy before build	Using applications and infrastructure that is already in use and proven is preferred. Where this isn't appropriate, buying standard components is preferred over developing custom development.
ARP-ARP-04	Architecture Principles	ARP	Information systems are implemented cost effectively	The implementation of information systems should take the total cost of ownership into account. All application servers will be built on single OS with a rationalized non-production environment.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ARP-ARP-05	Architecture Principles	ARP	Changes in the IT architecture do not compromise business continuity	The IT architecture supports the business and changes should be implemented in a way that does not put the business at risk. The solution and implementation are being designed to support the future business requirements to ensure efficiency and continuity of DICDL operations.
ARP-ARP-06	Architecture Principles	ARP	Processes are standardized	Critical business processes are defined and standardized. All business processes are standardized and agreed with DICDL during the high-level design phase.
ARP-ARP-07	Architecture Principles	ARP	Decisions are based on a cost/benefit analysis	Decisions are based on an analysis of the requirements and the matching of the solution to the delivered benefits. Possible options for addressing business requirements are thoroughly evaluated in view of cost and benefit and the recommendations and decisions are discussed and agreed with DICDL.
ARP-ARP-08	Architecture Principles	ARP	Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.	IT components should be based on defined and agreed standards that promote interoperability and technical interoperability. All recommended software and hardware components adhere to DICDL standards; the selected components need to be discussed, options evaluated and agreed with DICDL.
ARP-ARP-09	Architecture Principles	ARP	Documents are stored in the Document Management System	All documents are stored in DICDL DMS solution- Documents are a critical asset and should be stored in the system that is designed for their storage and management.
ARP-ARP-10	Architecture Principles	ARP	Reporting and Analytical applications don't use the operational environment	A detailed reporting strategy should be defined- Reporting from a separate non-operational environment prevents unpredictable performance from operational systems.
ARP-ARP-11	Architecture Principles	ARP	Access to IT systems is authenticated and authorized	People should not have access to information which they are not authorized for. Where possible by the underlying technology like LDAP authentication or SSO has been proposed to be used. Profiles are strictly defined according to the agreed organization structure and the access is strictly limited based on the user profile.
ARP-ARP-12	Architecture Principles	ARP	Information is organized	The use of information is critical to the operation of the business and it should be organized. The information is organized and contained in the respective systems with well-defined data standards.
ARP-ARP-13	Architecture Principles	ARP	Conformance	All projects and solutions built should confirm to Architecture Standards and Framework.
ARP-ARP-14	Architecture Principles	ARP	Coverage	All solution/ technical components must be assessed against the architecture. All the components adhere to architectural recommendations
ARP-ARP-15	Architecture Principles	ARP	Design	Solution components should be assessed to fit against the reference architecture models and fit with other components. All key decisions have an options paper which need to be approved by the ICT Consultant/DICDL. Designs are reviewed and base lined before starting on development.
ARP-ARP-16	Architecture Principles	ARP	Simplicity	The IT architecture should be kept as simple as possible while still meeting business and enterprise requirements. Follow well defined patterns. Minimize duplication and reduce complexity and build things easy to use and understand. The solution is designed following best practices, to keep the end-to-end solution simple.
ARP-ARP-17	Architecture Principles	ARP	Service Levels	Technology Components to be compliant with DICDL service levels. Technology components should be available for the agreed uptimes and ensure business continuity. All technical components are designed to be available for the agreed SLA's.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ARP-ARP-18	Architecture Principles	ARP	Scalability	Solution should be capable of scaling to meet any increase business needs. Solutions should be sized considering the agreed growth rate and can be scaled further, if required, to address increase in business demands & needs.
ARP-MDM	MDM	ARP	Planning and Strategy	Open data principles to govern the interaction between government and partners: - Establish the scope of city data and its use. - Small and medium sized enterprises to partake in the development of city solutions with open data. - Bring together various 'data innovators' around specific challenges using the data sets to develop solutions that can then be rolled out - Collating, managing and processing city data - City to have a one-stop portal offering publicly-available datasets from government agencies using which citizen centric apps can be developed.
ARP2.0	MDM	ARP	Planning and Strategy	Open Data: - Enable data sharing to conveniently and securely share data through application programming interfaces (APIs).

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Overall system architecture as envisaged for DSIR is shared below;

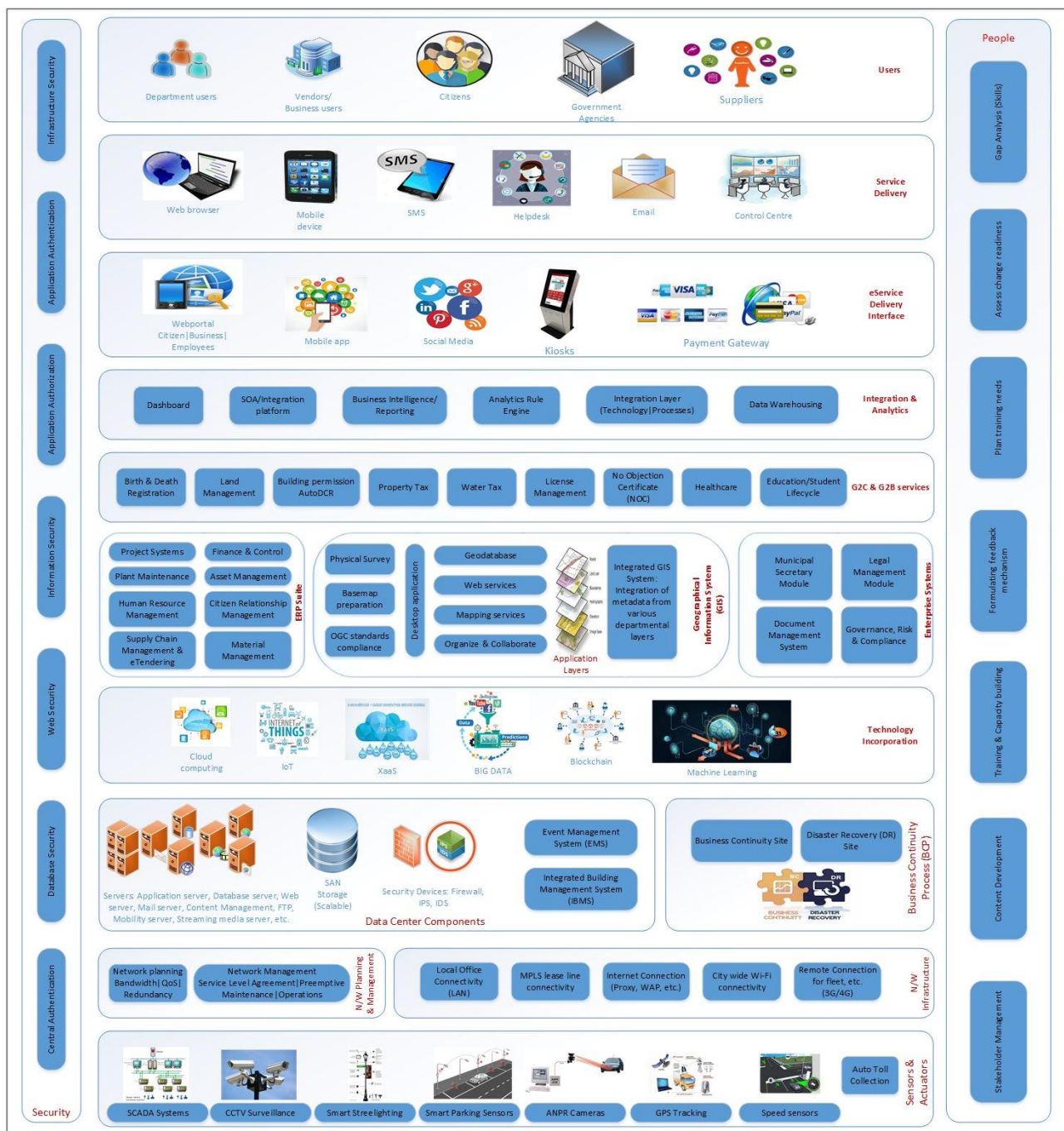


Figure 4 – Overall System architecture for DSIR with Smart City components

3. DETAILED SCOPE OF WORK, BUSINESS, FUNCTIONAL, NON-FUNCTIONAL, TECHNICAL REQUIREMENTS, OPERATION AND MAINTENANCE

The Project requires turnkey services wherein the MSI shall broadly cover the following main scope of services:

- Design
- Supply
- Install
- Test
- Integrate
- Commission
- Operations and maintenance
- And other related works for the job in reference

The subsequent sections detail out the broad scope with respect to execution of this Project. The MSI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. MSI is expected to perform independent analysis of all the additional works that may be required to be carried out to fulfil the requirements of ICT infrastructure as mentioned in this document and factor the same in its scope.

Project Management

MSI shall be responsible for project management for the implementation and maintenance of the smart city ICT components. MSI shall deploy a competent team of experts for project management.

The Project Manager shall be the single point of contact that shall assume overall responsibility of the Project and ensure end-to-end working of the Project. He shall function as the primary channel of communication for all DICDL requirements to the implementation team. In case of any absence of the project manager (sickness or vacation), the MSI shall ensure that an alternate project manager (as approved by the DICDL or its representative) shall be provided during the absence period.

All key personnel associated with the project shall be available for meetings whenever asked by the DICDL or its representative.

MSI shall prepare minutes of every meeting which takes place and submit to DICDL/ICT Consultant or its representative for tracking of the Project.

All the tools required by MSI for project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by MSI.

All design and engineering deliverables shall be submitted in at least two (2) formats i.e. draft and final. The DICDL/ICT Consultant representative will have maximum 45 days to review and comment on every deliverable. The practice of submissions for all deliverables will be Four (4) hard copies in color and soft copy of every deliverable shall be submitted. If required further copies of the deliverable may be asked to be shared with any other stakeholders for review and approval which shall be provided by MSI on request by DICDL/ICT consultant. The submissions will include both hard and soft copies. Upon providing review comments by ICT Consultant and DICDL or any other stake holders, the same will be incorporated by MSI and

once again 4 sets of documents in color will be submitted.

Survey and Detailed Design Validation of all Smart City ICT Components

MSI shall conduct survey of the site area, additional requirement gathering and based on the observations, assess and validate the present conditions, implementation approach and methodology, project challenges and mitigations and other project critical information. During the survey stage itself, MSI shall mobilize its entire staff and fully acquaint them with the site conditions. It is MSI's responsibility to periodically survey the site and be updated on the conditions during the course of the contract. During the design validation stage, MSI is also expected to:

- Conduct workshops with different stakeholders for capturing business requirements, creating awareness of best practices, communicating the changes, building consensus on process design etc. This needs to be organized at different intervals and in different places throughout the duration of the projects as needed.
- Carry out stake holder consultations other than workshops, with those stake holders who will be identified by DICDL, for critical inputs, review, suggestions, process description, etc.
- Have review sessions with different stake holders for signing off the design deliverables, walking through the deliverables for facilitating quick understanding etc.
- Do the needful in terms of what is needed for acceptance of respective ICT infrastructure by stakeholders and training the required no. of users
- All the Installations must be regulator, GoG compliant and all the necessary approvals in this regard to be obtained by MSI.
- All civil, electrical, mechanical, etc. works as needed will be in the scope of MSI for completeness of ICT infrastructure.
- A fully blown fiber connectivity will be provided by MSI from ABCD-1 building to the nearest Police Station. In this regard, all the ROWs will be provided by DICDL, MSI needs to facilitate and any further equipment needed are to be procured/provisioned by MSI. Any charges for ROW permission and approval will be borne by DICDL. MSI will provide all the equipment needed on both ends to make it functional. This connectivity will be joined by appropriate means (to be decided by police dept.) with surveillance network.
- The MSI will not proceed with any kind of build without the approval of DICDL/ICT consultant. DICDL/ICT consultant will not pay for any builds that has not been approved.
- MSI shall recommend/submit system architecture for all the applications/systems/platforms in scope for both cloud and on-premises;
- All telecom rooms of each floor of DICDL building needs to be connected through fiber with server room in a secured manner.
- All LANs of the service areas must be connected and routed over fiber through absolutely secured means to POP for connecting to citywide networks.
- MSI will provide all the assistance needed by various contractors and stakeholders as part of the scope of work.
- MSI at its own initiative co-ordinates with all the stakeholders for all the overlapping areas and the help needed by stakeholders.
- To the extent possible, ESB should be used for all integrations within the city ICT. Appropriate means should be deployed for integrations happening over the cloud.
- MSI will be responsible for upkeep of all ICT infrastructure in its scope during its entire engagement and any pilferage, theft, damage, etc. of any ICT equipment/component needs to be rectified/replaced by MSI himself.

- MSI shall provide Disaster recovery, back-up solution, specify RTO (Recovery time objective), RPO (Recovery point objective), Clustering, Single sign on, proposed application uptime, proposed Application response time for various applications in scope, storage requirements over the implementation and O & M period;

The MSI shall also be responsible for the detailed design validation of the project. MSI shall discuss in detail and validate with the DICDL/ICT Consultant or its representatives the detailed design of the smart city ICT components and fine-tune any requirements. It is the MSI's responsibility to satisfy the operational requirements of the DICDL and adopt industry best practices for implementation during the design stage itself. Based on the survey observation, analysis and discussion with the DICDL/ICT Consultant, the MSI shall submit Detailed Design Documents for review and approval by DICDL/ICT Consultant. The detailed design document shall include end-to-end design validation for the project including any project understanding, analysis, detailed design, integration plan, and as build drawings for implementation.

Complete set of design and construction drawing including method of installation as applicable shall also be included in the Detailed Project Design Document. Construction details shall accurately reflect actual job conditions. All technical data sheets of the products should be submitted by the MSI along with design documents. It is MSI's responsibility to get all technical data sheets approved by the DICDL/ICT Consultant or its representative to meet the overall project schedule. Design and construction drawings shall include the following at a minimum:

- Configuration and customization details as needed
- All system device locations as required for installation, operation and maintenance;
- Cable requirements, routing and location (as applicable);
- Typical mounting details;
- Single Line Diagrams (SLDs);
- Splicing diagrams;
- Wiring diagrams;
- Any other documents as requested from time to time by DICDL/ICT Consultants including layouts;
- Any other requirement to meet the requirements of the RFP.

All drawings shall be updated/revised to "as-built" conditions when installation is complete. Design submissions shall be based on project requirements and shall include as applicable, but not limited to, the following:

- Complete listing of specifications to be used along with detailed technical data sheet;
- Detailed engineering drawings;
- Shop drawings including product data sheets;
- Revisions to original design submissions.

For the software components like ERP, Webportal, Mobile app, CIOP as well as other ICT components/applications, MSI shall create requirement analysis documents for various components of the solution. This includes System Requirements Specification (SRS) and updated Functional Requirements Specification (FRS) documentation as well as other system design documents. The MSI shall be responsible for documenting any existing/planned 'processes' of the DICDL as part of these deliverables. MSI shall document all kinds of input and output forms for ERP, Webportal, Mobile app, CIOP, Industry specific services, etc.

As part of the Project, the ICT Consultant shall provide drawings to the MSI in raw format. These drawings include typical details, proposed equipment location, routing and typical splicing. It will be MSI's responsibility to work on these drawings as a base, update them as per the latest site conditions, and convert these drawings to 'for construction' drawings. The detailed design report shall be submitted to DICDL/ICT Consultant or any other representative for their review and approval.

Prototype Acceptance and Factory Acceptance Testing

After the approvals of the technical data sheets by the DICDL/ICT Consultant or its representative, MSI shall submit the prototype of all the material presented in the Detailed Design Report to the DICDL/ICT Consultant or its representative for its review and approval. Note that it shall be MSI's responsibility to get the prototypes approved in due course of time without affecting the overall schedule of completion of works.

Material provided as part of the Project shall undergo Prototype Acceptance Test (PAT) and Factory Acceptance Test (FAT). Details regarding the PAT and FAT are presented in Testing Section of the Scope of Work. MSI shall also present to the DICDL/ICT Consultant and its representatives the test results for PAT and FAT in the form of Test Result Documentation presented in the Testing section. The DICDL/ICT Consultant and its representative at their own discretion shall visit any FAT site. MSI shall be responsible for organizing all logistics required for any such site visit and the related expenses shall be borne by DICDL.

For all the software components like ERP, Webportal, Mobile app, CIOP and other solutions MSI shall also prepare and submit prototype of solution components in this design phase and get the required approvals from DICDL/ICT Consultants or its representatives.

Hardware Supply and Installation Stage

MSI shall be responsible for the supply and installation of all components as part of the DSIR ICT components to meet the technical, functional, business and performance requirements of the RFQ cum RFP. No deviations from these requirements shall be acceptable by the DICDL. Any additional hardware or software component required to meet the technical and performance requirement of the project and not specified as part of this document but required to meet the overall requirements of the project shall be factored in as part of the Bid, and to be provided by the MSI. MSI shall deliver the project and install and handle the equipment in accordance with DICDL requirements. Installation process of the MSI shall be flexible and shall accommodate DICDL's requirements without affecting the schedule as specified in the RFQ cum RFP.

MSI shall be responsible for all supply, storage and handling of the material provided as part of the project. If there is removal/change of any existing material during installation process and belongs to the DICDL, the material shall be handed-over to the DICDL. MSI shall also be responsible for reinstating any site in the project limits at no additional cost to the DICDL. It shall be the MSI's responsibility to supply and install all hardware and software in compliance with the requirements of the RFQ cum RFP. Since this is a turnkey contract, MSI shall be responsible for all implementation works on the project including any civil, structural, electrical, etc. works required to meet the requirements of the project. All power conversions necessary to operate the equipment shall be under the scope of MSI. The DICDL shall only provide raw power for all the equipment.

Software Development

MSI shall be responsible for customization, development and deployment of all software required to meet the requirements of the project. Some of the software may be COTS or open source with enterprise support development, however bespoke development is not allowed MSI shall be fully responsible for design, customization, development, integration and implementation for the scope defined for the project. All software applications/modules designed and developed needs to be demonstrated/presented to DICDL/ICT consultants or its representative for approval and further processing/deployment on periodic basis as per project requirements. The technology platform chosen for all software shall be based on industry standards based and shall be secure. Migration of existing data to newly configured database shall be the responsibility of the MSI. MSI is required to take the source data in the format which is available. Subsequently, MSI is required to take complete ownership of data migration and also develop a detailed plan for data migration.

The MSI shall ensure that full support from the OEM's is provided during the course of the contract. MSI shall

be responsible to provide any upgrades, patches, fixes to the software during the course of the contract as part of scope to the DICDL.

System Integration

MSI shall be responsible for the integration of all hardware and software supplied as part of this Project as per the technical and performance requirements. The system integration scope also includes integration of the Project components with the components provided by others as per the details of the RFQ cum RFP.

It shall be the responsibility of MSI to take approval of the DICDL for the Integration of the overall system as per the RFQ cum RFP. Post systems integration, the DICDL shall review and approve the overall performance of the integrated system as per the requirements of the RFQ cum RFP. MSI shall be responsible for fixing any requirements that are not found in compliance with the original RFQ cum RFP and approved detailed design as part of scope to the DICDL.

Testing

All materials, equipment, systems, manufacturing or configuration processes, or other items to be provided under the Contract shall be inspected and tested in accordance with the requirements specified in this document and will be subject to DICDL/ICT Consultant or its representative's approval. The testing shall include any existing civil infrastructure equipment or materials to be taken over by the MSI. Approvals or passing of any inspection by the DICDL shall not, however, prejudice the right of the DICDL/ICT Consultant or its representative to reject the material if it does not comply with the specification or requirements of the RFQ cum RFP.

MSI shall be responsible for design, development, successful system tests and implementation of the same in compliance to the requirements furnished in the RFQ cum RFP.

All tests shall be subject to inspection/witnessing by the DICDL/ICT Consultant or its representative. Inspection or witnessing of tests may be waived at the sole discretion of the DICDL or their representative, subject to the MSI furnishing the DICDL or their representative with properly completed test certificates in accordance with the requirements of the RFQ cum RFP. Failure of the DICDL or their representative to witness any test shall not relieve the MSI of the obligation to meet the requirements of the Contract. MSI shall submit an Acceptance Test Procedures document (ATP), for DICDL's/ICT Consultants approval prior to undertaking any testing. The ATP shall clearly address:

- Type of testing and device to be tested
- How each specification requirement will be demonstrated, including the test environment and set-up, specific functionality to be tested, method for performing the test and quality assurance procedures
- The results that will constitute success for each test
- Timing of test within the overall Contract schedule
- The location for testing
- Personnel required to conduct the test
- Approximate time required to execute the test or set up tests
- Responsibilities of both the MSI and DICDL's representatives during each test
- A cross-reference to which Contract requirements from the Compliance Matrix (to be developed by the MSI) are being addressed by each test procedure.

For all applications hosted on government owned public/ private cloud at GSDC Gandhinagar or hosted on premises at DSIR Gujarat, the security testing shall be a mandatory requirement.

The ATP shall include an updated Compliance Matrix to include the test relevant stage at which each contract requirement will be demonstrated; and a cross-reference to the test procedure(s) that serve to address each contract requirement. The Compliance Matrix shall be used as a “punch list” to track which requirements have not yet been demonstrated at each stage of testing. A requirement classified as having been “demonstrated” during a certain ATP stage can be subsequently redefined as having been “not demonstrated” if compliance issues emerge prior to System Acceptance. ATP shall be submitted to DICDL/ICT Consultant at least three (3) weeks in advance of any intended testing.

All measuring instruments required to measure test parameters shall be calibrated by an approved testing authority. The equipment shall be inspected for standards of construction and electrical and mechanical safety.

Test results shall be recorded for all tests conducted under this Contract. The MSI shall make test results available to DICDL/ICT Consultant or their designated representatives for review immediately after completion of the tests.

ATP for each test shall be collated, bound and delivered as part of the close-out documentation requirements specified herein.

ATP shall incorporate the following distinct stages for each deployed stage:

Prototype Acceptance Tests (PAT): Prototype Approval Test shall be conducted only on the customized application/solution except hardware for their design and compliance to functional specifications. PAT shall be completed before conducting FAT and only after approval of PAT by DICDL’s/ICT consultant's representative, the equipment shall go in production. PAT shall be witnessed by DICDL’s/ICT Consultant’s representatives.

Factory Acceptance Tests (FAT): FAT shall be conducted before the equipment and software is shipped to DICDL for installation, and deficiencies shall be rectified before shipping to DICDL for installation. All devices furnished by the MSI shall be tested and subjected to a nominal 72-hours burn-in period at the factory. FAT shall be witnessed by DICDL’s representatives at their discretion. In case of software components like ERP, Webportal, Mobile app, CIOP applications, etc. unit testing will be carried out by the MSI team and test results will be submitted for verification.

Pre-Installation Testing (PIT): All equipment supplied under this Contract shall undergo pre-installation testing in accordance with the ATP. This shall include existing equipment, any spare parts, any new equipment provided by DICDL or their designate and new equipment provided by the MSI.

If the equipment is considered a standard production item, the MSI may, with the prior consent of the DICDL or their representative, supply a copy of the equipment manufacturer’s quality control test results in place of a MSI performed test.

All PIT testing shall be carried out prior to installation of the equipment. After satisfactory completion of the MSI’s PIT tests, the MSI shall supply all test measurements and results to the DICDL or their representative, together with a Test Certificate.

Installation Acceptance Tests (IAT): IAT shall be conducted after each installation of each equipment type, and deficiencies shall be rectified before the initiation of SAT. IAT may be witnessed by DICDL’s representatives.

Proof of Performance Testing (POP): The MSI shall implement a structured proof of performance testing, which will progressively place all components in service. Site tests shall be performed on individual

components, subsystem sites, and the complete subsystems, as necessary to confirm that each element of the system functions satisfactorily and fulfils the requirements of this specification.

Completion, submission, and approval of all relevant PIT and IAT tests and results must be completed prior to carrying out any POP tests.

All subsystem equipment and components shall be tested by the MSI regardless of whether or not it is a standard item.

After satisfactory completion of the MSI's POP tests, the MSI shall supply all test measurements and results to the DICDL or their representative, together with a Test Certificate.

System Integration Testing (SIT): The MSI is responsible for the proper and harmonious operation of all subsystems installed under this Contract. Where connections of the new systems to existing subsystems or equipment supplied by others are required, the MSI is responsible for connection of equipment specified in the Contract and for initial system integration tests. Such a test will verify the full functionality of each subsystem as they are interconnected. This will require testing to be coordinated by the MSI with the DICDL or their designate. This work will be carried out under the direction of the DICDL or their designate.

Completion, submission and approval of all relevant PAT, FAT, PIT IAT and POP tests and results must be complete prior to carrying out any SIT tests.

The MSI shall:

- Complete all equipment and subsystem tests required in the Contract;
- Test each subsystem independently;
- Add subsystems one at a time and monitor the overall performance;
- Fail safe testing of all subsystems one at the time while monitoring overall systems performance.

A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system, together with final copies of all Operating and Maintenance Documentation for the System.

Stress and Load Testing: Comprehensive stress and load testing of the modules shall be conducted to demonstrate robustness and reliability of the system.

Security Testing (including penetration and vulnerability test): Security test shall be conducted to demonstrate security requirements at network layer and software applications. Components shall pass vulnerability and penetration testing for rollout of each phase. Components shall also pass web application security testing for portal, mobile app, and other systems. Security testing shall be carried out for exact same environment/ architecture that shall be set up for go-live. Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase. For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory requirement.

Pilot Test: Requirements for Pilot Test is explained in the Pilot Deployment Section of the Scope of Work.

System Acceptance Tests (SAT): SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of Burn-in Test. SAT shall be conducted on full system completion only to determine if the system business, functional and technical requirements as specified in the bidding documents are meet. SAT shall be witnessed by DICDL's representatives. Data migration, if any will be carried out by MST prior to commencement of this stage. SAT shall also include any performance and load testing for the software applications.

Burn-in Tests (BT): Following successful completion of the SIT and SAT, the approved System will be put into service and its performance monitored for a period of thirty (30) consecutive calendar days for the purpose of verifying system reliability in an operating environment. Any failures and defects occurring in this time will be documented. Any serious defects which affect the availability of the system will be a basis for restarting the test. Upon the satisfactory completion of this performance testing a Completion Certificate will be issued.

The MSI shall not commence BT until SIT and SAT have been performed and successfully completed/approved and all documentation of the successful completion of PAT, FAT, PIT, IAT, POP, SIT and SAT, along with notification of the schedule date of the BT is provided to the DICDL or their representative in accordance with the Requirements. Commencement of BT will be conditional on the DICDL or their designate providing written notification of DICDL's readiness to proceed to BT.

The MSI shall be suitably prepared for the BT prior to the start date. Repeated failure of the BT may result in the MSI having to reimburse the DICDL or their representative for costs incurred. No compensation to the MSI will be made for repeat testing.

Where equipment supplied by the MSI fails during the burn-in period, the MSI shall restart the test at day zero (0) following appropriate corrective measures. If a utility failure is proved to be the cause of testing failure, then the MSI shall restart the fourteen (14) day burn-in test at the day the failure occurred. If a subsystem failure is proved to be the cause of testing failure, then the MSI shall start the test over at day 0 (zero).

Where tests or burn-in indicate that an existing subsystem or component, not provided by the MSI, is defective, the MSI shall immediately report the deficiency to the DICDL or their representative. The DICDL or their representative may assign corrective repairs, retesting and repeat of BT to the MSI, in accordance with change provisions of the Agreement.

The MSI shall provide the DICDL or their representative with a contact name and phone number(s) for a designated emergency contact person during BT. The emergency contact person shall be accessible twenty-four (24) hour a day, for each day of testing.

Operational Acceptance Test: Shall be conducted after successful SAT and Burn-in tests. Continuous fault free running of the System shall be tested. Post the completion of Operational Acceptance Test, System shall be considered for Operational System Acceptance and Defect Liability Period (DLP) shall commence. Operational Acceptance Test shall include the following as a minimum:

- Completion of all activities and fulfilment of all business, functional and technical requirements listed in RFQ cum RFP;
 - Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc.;
 - Satisfactory completion of closing of accounts and generation of complete balance sheet for one financial quarter, with the ERP solution and approved by the head of finance and accounts.

DICDL may authorize the MSI to proceed to the next testing stage with certain deficiencies not yet resolved.

The MSI shall provide written notice to DICDL at least five days in advance of any testing, indicating the specific tests to be completed as well as the date, time and location. The MSI shall be required to reschedule testing if DICDL witnessing representatives cannot be present or if other circumstances prevent testing from taking place.

MSI shall provide written Test Results Documentation (TRD) within one week of completing each stage of testing. The TRD shall document the results of each ATP procedure and provide an updated Compliance Matrix that indicates which contract requirements have been demonstrated. The TRD must be approved before DICDL will grant System Acceptance. A sample format for the TRD is provided:

Item #:		Tester:	
Item Description:		Date:	
Test:			
Test Set-up:			
Clause	Test Procedure	Expected Results	Actual Results
Witnessed: (This Does Not Constitute Approval) Reviewed and Approved:			

MSI shall be responsible to carry out all the testing as per the satisfaction of the DICDL and its representatives. It is the responsibility of the MSI for all documentation required for establishing approval and acceptance of installation and operation of the system components.

All the costs those are associated with any testing are to be borne by the MSI excluding the costs of travel and accommodation of the DICDL/ICT Consultants or its representatives from their home locations in their cost bid. In the interest of the MSI maximum of three (3) people shall be nominated by the DICDL to attend any such testing wherever it is carried out. All expenses related to travel and accommodation for such testing shall be borne by DICDL.

In case of failure of any testing, the failure component shall be repaired and the test shall be rerun. If a component has been modified as a result of failure, that component shall be replaced in all like units and the test shall be rerun for each unit.

MSI shall provide the DICDL with a copy of the manufacturer's quality assurance procedures for information. Documentation certifying and showing that each item supplied has passed factory inspection shall also be submitted by the MSI.

Pilot Deployment

The MSI shall conduct Pilot deployment and testing for meeting DICDL's business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on DICDL's feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.

The Pilot shall be demonstrated to the DICDL's representatives. If for any reason the pilot is found to be incomplete, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making good on the lapses pointed out before offering the system to DICDL for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to DICDL.

Training

Post the system integration, MSI shall train DICDL team and their representatives to operate the implemented systems and to conduct any routine diagnostics and routine maintenance work. Training shall be done during Pilot Deployment and before Final Deployment. The period of training shall be mutually agreed upon by DICDL and MSI.

The MSI shall provide training courses for at least:

- Decision Makers/ Management;
- DICDL's/ICT Consultant operations personnel;
- Users of Various Systems/Applications developed as part of the project.

The actual number of each of above categories of trainees will be provided during the course of the Contract. MSI shall provide all training materials in both Microsoft Office and Adobe PDF formats, consisting of graphics, video and animations on Flash drive with a permission to reproduce copies later on.

The Training Plan (TP), including the training schedule and course outlines, must be provided to DICDL for review at least three weeks in advance of the start of training. The TP must be approved by DICDL before the start of training.

MSI shall furnish all special tools, training videos, self-learning tools, equipment, training aids, and any other materials required to train course participants, for use during training courses. Training shall include various session on system maintenance and configuration along with multiple sessions on system operation, which can further be required to be extended by DICDL/ICT Consultant as per the requirements.

The instructors shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the DICDL feels that on-field sessions are required, the same shall be conducted by the MSI. The language of training shall be in English/Hindi/Gujarati.

If any instructor is considered unsuitable by DICDL, either before or during the training, the MSI shall provide a suitable replacement within one week of receiving such notice from DICDL.

The MSI shall provide brief refresher versions of each training course to the original trainees and new inductees between three to six months after System Acceptance for each deployment stage at no additional cost.

Training shall be provided to DICDL staff along with other representatives in periodic manner as and when requested by DICDL.

MSI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive online feedback mechanism.

Final Deployment and Documentation

After addressing the DICDL/ICT Consultant feedback and any deficiency observed during the Pilot deployment and upon completion of System Acceptance Tests (SAT) and data migration, final deployment of the project components shall be considered by the MSI. For achievement of final deployment, MSI shall also be responsible for development of a cutover strategy, which shall include initial data take on, sequence of data takes on, set up of support mechanisms to minimize business impact due to any cutover activities.

Post the final deployment, MSI shall handover detailed documentation that describes the site conditions, system design, configuration, training, as-built conditions, operation and maintenance. All documentation shall be in English, shall utilize metric measurements, and shall be submitted directly to DICDL as well as ICT Consultant in paper hardcopy and electronically in Word/AutoCAD/Excel/Project and Adobe Acrobat.

All installation drawings shall be prepared in AutoCAD, GIS exchange format and Adobe Acrobat, provided on CD-ROM/Flash drive as well as hard copies. The drawings shall contain sufficient detail including but not

limited to equipment dimensions, interfaces, cable details, equipment mounting and fire protection.

Electrical and electronic drawings shall be supplied to show engineering changes made to any component or module any time during the contract period.

‘As-built’ Documents delivered by the MSI shall include:

- An inventory of all components supplied including model name, model number, serial number and installation location
- An inventory of all spare parts supplied including make, model number, and serial number and storage location
- All reference and user manuals for system components, including those components supplied by third parties
- All warranties documentation, including that for components supplied by third parties
- As-builts in CAD and GIS
- A diagram indicating the as-built inter-connections between components
- Software documentation which also includes the version number of all software, including that supplied by third parties
- Cable run lists and schedules
- All network and equipment details such as IP addresses, user names, and passwords
- Manufacturer’s test procedures and quality assurance procedures for information
- Data communication protocols
- ‘As-Built’ drawings for all components installed.

MSI shall submit to DICDL copies of comprehensive operating and maintenance manuals, and log sheets for all systems and hardware supplied as part of this bid document. These shall be supported with the manufacturer’s operating and maintenance manuals. The manuals shall be complete, accurate, up-to-date, and shall contain only that information that pertains to the system installed. Maintenance documents shall include:

- Equipment installation and operating documentation, manuals, and software for all installed equipment
- System Installation and setup guides, with data forms to plan and record options and configuration information
- The schedule/procedures for preventative maintenance, inspection, fault diagnosis, component replacement and on-site warranty support administration on each system component
- Hard copies of manufacturer's product specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM or non-volatile memory stick of the hard-copy submittal
- Complete list of replaceable parts including names of vendors for parts not identified by universal part numbers (such as EIA codes)
- Manufacturer's product specification sheets, operating specifications, design guides, user's guides
- Permits and Contractor names and telephone number lists for all project trades.

MSI shall provide Systems Manuals (SM), documentation including:

- The configuration and topology of central systems hardware and software
- Central systems software functions and operations
- Scheduled maintenance required for the central systems and
- Database structure and data dictionary.

MSI shall also provide following documents for any bespoke software development:

- Business process guides
- Process flow descriptions

- Data model descriptions
- Sample reports
- Screen formats
- Frequently Asked Questions (FAQ) guides
- User Manuals and technical manuals
- Any other documentation required for usage of implemented solution.

Documentation of processes shall be done using standard flow charting software. An intuitive online learning tool depicting standard operating procedures of system usage are required to be deployed. There shall be a provision of training system in the deployment architecture so as new employees can be inducted easily.

All pages of the documentation shall carry a title, version number, page number and issue date, and shall contain a complete subject index. MSI shall be responsible for fully coordinating and cross referencing all interfaces and areas associated with interconnecting equipment and systems.

Documentation shall require re-issues if any change or modification is made to the equipment proposed to be supplied. MSI may re-issue individual sheets or portions of the documentation that are affected by the change or modification. Each re-issue or revision shall carry the same title as the original, with a change in version number and issue date.

Each volume shall have a binder (stiff cover and spine), and drawings shall be protected by clear plastic to withstand frequent handling. The binding arrangement shall permit the manual to be laid flat when opened. The paper used shall be of good quality and adequate thickness for frequent handling.

Operational System Acceptance

At the completion of operational acceptance test, the system shall be considered for operational system acceptance. At the close of the work and before issue of final certificate of completion by the DICDL, the MSI shall furnish a written guarantee indemnifying DICDL against defective materials and workmanship for a period of one (1) year after completion which is referred to as Defect Liability Period. The MSI shall hold himself fully responsible for reinstallation or replace free of cost to DICDL during the Defect Liability period as well as Operation and Maintenance period. MSI shall provide approved temporary replacement equipment and material such that the system remains fully functional as designed and commissioned during repair or replacement activities at no cost to the DICDL.

Comprehensive Maintenance for System and Services

MSI shall be responsible for comprehensive maintenance of both hardware and software, up-gradations in the system, expansion of the system, technical manpower, spares management and replenishment, performance monitoring and enhancements, preventive and corrective maintenance of the DSIR ICT components deployed as part of this project and shall maintain service levels as defined in the RFQ cum RFP. All equipment and material supplied by the MSI shall be provided with standard warranty against defects of design and manufacturing and against faults and failures associated with workmanship of MSI and its sub-contractors commencing from operation acceptance of the system. All equipment found to be defective during comprehensive maintenance shall be repaired or replaced by the MSI at no cost to the DICDL.

MSI shall provide all the technical, managerial, and other staffing required to manage day-to-day maintenance of the DSIR ICT components during the Contract period.

All spares required for the smooth operation of the DSIR ICT components shall be maintained by the MSI for the entire duration of the contract to meet SLA requirements.

The cost of the all kinds of spares, repairs, and replacement shall all be deemed to have been included in the price quoted by the MSI. MSI shall also institutionalize structures, processes and reports for management of SLA. Root cause analysis and long-term problem solutions shall also be part of MSI scope.

MSI shall maintain all data regarding entitlement for any upgrade, enhancement, refreshes, replacement, bug fixing and maintenance for all project components during Warranty. MSI shall be responsible for updates/upgrades and implementation of new versions for software and operating systems when released by the respective OEM at no extra cost to the DICDL during entire duration of contract. Requisite adjustments / changes in the configuration for implementing different versions of system solution and/or its components shall also be done by MSI. The MSI shall also ensure application of patches to the licensed software covering the appropriate system component software, operating system, databases and other applications. Software License management and control services shall also be conducted by the MSI during this phase. Any changes/upgrades to the software during comprehensive maintenance shall be subjected to comprehensive and integrated testing by MSI to ensure that changes implemented in system meets the specified requirements and doesn't impact any other function of the system. Issue log for errors and bugs identified in the solution and any change done in solution (vis-à-vis the FRS, BRS and SRS signed off) shall be periodically submitted to the DICDL/ICT Consultant. MSI shall also be responsible for operating the website, city portal, city application, mobile applications, etc. including all support, content updates and upgrades throughout the duration of contract.

MSI shall ensure OEM support during Comprehensive Maintenance stage for system performance, performance tuning, upgrades, etc. MSI shall provide all support for formulation of all policies and procedures related to System Administration, Data Base Management, applications, archives, network management & security, back up and data recovery and archive, data synchronization after crash.

Assistance to DICDL shall be provided as needed in Management of legacy data interfaced, print spools, batch jobs, printer configuration etc.

MSI shall prepare a detailed System administration manual, Data administration manual, operational manual, User manual which shall be used by DICDL's employees to operate DSIR ICT components. This shall also include how the various parameters shall be monitored/ tuned in a live system. Preparation of requisite system configuration for disaster recovery management and fail over system plan shall also be under the supervision of MSI.

All the Installations must be regulator, GoG compliant and all the necessary approvals in this regard to be obtained by MSI.

The MSI shall also maintain the following minimum documents with respect to ICT components:

- High level design of system
- Module level design of system
- System Requirement Specifications (SRS)
- Any other explanatory notes about system
- Traceability matrix
- Compilation environment.

MSI shall also ensure updating of following documentation of software system: Documentation of source code;

- Documentation of functional specifications
- Application documentation is updated to reflect on-going maintenance an enhancement including FRS and SRS, in accordance with the defined standards

- User manuals and training manuals are updated to reflect on-going changes/enhancements
- Adoption of standard practices in regards to version control and management.

The communication costs (Internet charges, telephone charges, 4G/GPRS connectivity charges) and any other incidental charges related to maintenance period shall be in the scope of the MSI and considered to be included in the proposal submitted by the MSI for the entire contract duration.

Any planned and emergency changes to any component during maintenance period shall be through a change management process. For any change, MSI shall ensure:

- Detailed impact analysis
- Change plan with roll back plan
- Appropriate communication on change required has taken place
- Approvals on change
- Schedules have been adjusted to minimum impact on production environment.
- All associated documentation are updated post stabilization of the change Version control maintained for software.

Any software changes required due to problems/bugs in the developed software/ application will not be considered under change control. The MSI will have to modify the software/application as part of original scope. This may lead to enhancements/customizations and the same needs to be implemented by the MSI at no extra cost.

If the Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed, the same should be done as part of the post implementation support.

Support Personnel Required

Well trained, efficient and effective support personnel (Engineers) shall be provided by the MSI during the maintenance phase of the project. Any fault originating for the DSIR ICT components shall be addressed by the MSI support staff in the least time possible. The support staff shall work in a shift based system and provide full support coverage and maintain the system as per the SLA's defined.

The support Personnel shall be well qualified and trained to support the DICDL's operational and technical staff in day-to-day operations of the DSIR ICT components provided by the MSI. The staff assigned shall be well qualified to attend to the emergency situations and shall be able to communicate in an effective and efficient manner. Support staff shall be well trained on the smart city ICT components to understand and take necessary action in any kind of situation.

In addition to the training to the operations staff during acceptance stage, the MSI shall conduct half-yearly training refreshment sessions to train the new staff inducted by DICDL and to enhance the knowledge of the DICDL's staff operating the DSIR ICT components by adopting "train the trainer" approach.

Application Management Services. AMS shall consists of various service components listed and described below.

- **Incident Management:** accepting Tickets from Users according to defined SLA's, analysis and resolution of Incidents for all the applications according to defined SLA's, recommendations on application- and system optimization, ticket-based documentation and request involvement of Product/OEM Support when necessary.
- **Problem Management:** accepting Tickets from Users according to defined SLA's, root cause analysis and resolution of Problems according to defined SLA's, recommendations on application- and system

optimization, ticket-based documentation and request involvement of Product/OEM Support when necessary.

- **Change Management:** accepting Tickets from Key Users according to defined SLA's, analysis of Requests for Change, scope definition and creation of Requests for Change in collaboration between MSI's Engagement Manager and Employer's Engagement Manager, planning and deployment of Requests for Change according to agreed SLA's after Employers approval either as part of services described during the Operations Phase or as a Change Request; Ticket-based documentation and request involvement of Product/OEM Support when necessary.

- **Request Fulfillment:** accepting Tickets from Key Users according to defined SLA's, implementation of Service Request, request for Continuous Operations and agreed Standard. Change according agreed SLA's, Ticket-based documentation.

- **Event Management:** monitoring activities and creation of Incident Tickets for identified issues; monitoring alerts, categorization of alerts according to criticality, and creation of Incident Tickets for critical alerts, taking corrective actions by processing the Incident Tickets, proactive adjustment to relevant parameter to avoid further issues, Ticket-based documentation and request involvement of Product/OEM Support when necessary,

- **Proactive Services for MSI Applications:** MSI to proactively perform recurring services. MSI will execute the agreed Employer specific service plan without further triggering by Employer via a Service Request or otherwise. Proactive services shall be documented in a Ticket and be made transparent via the service reporting.

Proactive Solution Maintenance: management of service plan for Employer solution maintenance. Which is including: management and execution as Application Software Support Packages, implementation of support packages, application related validation and testing, proactive evaluation of available Product/OEM Security Notes and Legal Change Notes, proposal of relevant scope for Employer specific application and implementation in alignment with Employer specific requirements

Test Management & Execution: management of testing service plan in operations and performing readjustments on a regular basis. Which is including: Build of test case library for agreed test scenarios, enabling of test automation by scripting test cases, execution of regression test scripts and manual test scenarios, proactive maintenance of test scenarios and scripts for Employer applications, including taking corrective actions for test case defects and documenting change logs in Incident Tickets, defect logging and triggering of corrective actions for test findings by creating Incident Tickets for applicable functional area, reporting on test progress during execution

Release & Deployment Management: management of the release & deployment service plan in operations and performing readjustments on a regular basis. Which is including: definition of release categories, change categories and priorities, provision of Employer major and minor release calendar, planning of retrofit activities for dual track landscapes (maintenance and development landscapes), management of release cycles, support the engagement management and coordination of release activities, support of Project Portfolio Management (major releases) and support of Change Request Management (minor releases)

Managed Operations Control Center: establish critical incident procedures in collaboration with Employer business and IT processes, proactive monitoring of pre-defined monitoring metrics, monitoring alerts and exceptions, executing analysis for thresholds that are breached (events), executing remediation activities to help mitigate business or operations impact, on demand trigger resolution process for critical incidents on behalf of Employer and maintenance of monitoring environment and dashboard capabilities

Security Operations: management of security in operations which includes: Security Strategy & Planning (Security Advisory Service, Security Strategy and Planning (Management of effectiveness of security service plan in operations and readjustment on regular basis), Security Reporting (Segregation on Duty Check, Pre and Post Audit Guidance), Security Operation (Security Risk Assessment, Security Monitoring), Security for Application Operation and Maintenance (External

Support Authorization, API Security, Secure Network Communication, Authorization Upgrade, User and Role Management)

IT Operations Improvement: management of effectiveness of operations, improvement service plan in operations and readjustment on regularly basis. Which is including analysis of Employer's current and targeted maturity state in terms of operations, Application Lifecycle Management and IT Service Management.

Business Improvement: regular pro-active analysis of Employer business requirements for the MSI application environment, providing MSI solution architecture guidance, identification of potential technological and business process related improvement and innovation potentials, development and maintenance of a improvements backlog, propose high-level implementation design, effort estimation and mapping to release & deployment plan and handover release backlog items into further processing within Change Management as well as Release and Deployment Management

- **Continuous Improvement:** MSI shall provide continuous improvement services, Employer and MSI will agree on a pre-defined service plan defining tasks, efforts and frequency of execution. MSI will execute the agreed Employer specific service plan without further triggering by Employer via a Service Request or otherwise. Continuous improvements services shall be documented in a Ticket and be made transparent via the service reporting.

MSI shall provide some services in either a proactive or a reactive mode. When providing services in a reactive mode, Employer shall identify issues, problems or work tasks. Each Request shall be addressed to MSI by opening and sending a Ticket to MSI via MSI Support Application with the full documentation of the inquiry. Tickets shall be classified as Event-, Incident-, Problem-, Change Management or Request Fulfilment. When providing services in a proactive mode, MSI will take the initiative to identify issues, problems or work tasks.

Engagement Approach for Application Management Services

a. Engagement Management

All Application Management Services performed by the assigned MSI resources shall be coordinated with Employer's Engagement Manager.

b. Engagement Methodology

An AMS engagement shall consists of four phases with varying duration: Transition, Stabilization, Operations and Closure.

b1. Transition

The Transition phase precedes the Stabilization and Operations phases and shall have the objective to cooperatively establish all roles, processes and tools required for a successful delivery of the Application Management Services in the next phases. MSI shall provide a support structure to ensure that the resources required to provide the Application Management Services are available and that they have the necessary Employer-specific knowledge of the supported applications that will be used.

A mutually agreed project plan shall be drafted in detailed discussions with the Employer during the initial stages of the implementation and will be used to track all services throughout this phase.

One key activity of Transition phase is the knowledge transfer to make the MSI AMS team familiar with the specifics of the Employer's solution. The MSI Engagement Manager will coordinate the knowledge transfer phase. The knowledge transfer shall provide the MSI AMS team with the necessary knowledge required for the provision of the services, which may, as appropriate include information, records, documents, test scripts and data and live demo-sessions pertaining to MSI's delivering its in-scope services to the Employer. The Transition phase shall consist of 2 primary steps: Transition Planning and Transition Execution (including final service validation and test).

The main steps in the Transition phase shall be as follows:

Transition Planning	Planning and Preparation	Detailed workshops between Employer and MSI (including skills requirements gathering for staffing, knowledge transfer planning, etc.), team on-boarding (Employer related, cultural, etc.), defining responsibility matrix and governance models.
	Setup	Request and provisioning of infrastructure and application accesses and other resources necessary to support Employer. Setting up and testing of ticketing tool.
Transition Execution	Knowledge Acquisition	MSI AMS team to attend expertise transfer sessions led by MSI Implementation team, gather, update and/or prepare documentation. Review of documentation provided by MSI Implementation team.
	Shadow Support	MSI AMS team to observe and shadow support MSI Implementation team.
	Reverse Shadowing	MSI AMS team to perform services while MSI Implementation team to support, as escalation contacts.
	Finalize Transition Phase	Service Test on SLA Management, Reporting and Monitoring. MSI to perform final Operations Readiness checks and move on to coordinate cutover activities Sign off of the Transition phase by Implementation team and AMS team.

In addition to MSI Implementation Team Responsibilities and Obligations regarding Application Management Services listed in this, MSI Implementation team is required to provide the following during the Transition phase:

- Detailed system documentation for all the systems
- Ensure that MSI AMS Personnel receive all necessary usage rights for all the systems. During the planning phase, it should be determined which authorizations have to be assigned to these users.
- MSI Implementation team will support the MSI AMS team in acquiring the necessary knowledge for supporting the business processes in scope. In addition, MSI Implementation team will provide the relevant documentation required for Application Management Services, and other documents if required.

b2. Stabilization

The Stabilization phase precedes the Operations phase and has the objective to mature all aspects of solution operations to a steady state when productive SLA measurement starts in the Operations phase. Tickets shall be processed in compliance with the Event, Incident, Problem, Change Management or Request Fulfilment Process. During this phase application landscapes shall be stabilized.

The main steps in the Stabilization phase are as follows:

Stabilization	Kick-off Operations	Conduct a kick-off meeting with the Employer organization and ICT Consultants.
	Finalize documentation and ITSM procedures	Business processes and technical documentation, Procedural Manual shall be updated.

b3. Operations

The Operations Phase is the main phase of the AMS engagement.

The services shall be documented in a Ticket that has to be processed in compliance with the Event-, Incident-, Problem-, Change Management or Request Fulfillment Process. All Tickets will be processed in accordance with the agreed SLA's and solution scope.

The main steps in the Operations phase are as follows:

	Service delivery	Perform day-to-day monitoring and support

Operations	SLA monitoring	Perform SLA monitoring to prevent SLA violations
	Governance meetings	Perform regular internal meetings and meetings with the Employer / ICT Consultant to ensure quality of service delivery and to discuss and agree on proactive tasks as well as continuous improvements
	Reporting and Invoicing	Provide regular reporting
	Update documentation about ITSM procedures	Regularly review and update of business processes and technical documentation by Employer / ICT Consultant.

b4. Closure

The Closure Phase shall be the last phase of the AMS engagement. The start and end of this phase shall be agreed on once either Employer or MSI provide termination notice or in the last year of Operate and Maintain. The objective of the Closure Phase is to jointly ramp down the AMS service by handing back responsibilities to the Employer / Employer nominated entity. MSI will return all Employer documents received and provide support to the knowledge transition during this engagement Closure Phase.

During the Closure phase service delivery shall continue as described in Operations Phase, i.e. this particularly includes Ticket processing in compliance with the Event-, Incident-, Problem-, Change Management or Request Fulfillment Process. A joint project plan (Exit Plan) will be drafted in detailed discussions with Employer during the initial stages of the Closure Phase and will be used to track all services throughout this phase.

The main steps in the Closure Phase are as follows:

Knowledge Transfer	Knowledge Transfer sessions	Employer / Employer nominated entity will attend knowledge transfer sessions led by MSI.
	Handover meeting and sign-off	Employer and MSI verify that if all closure action items have been executed and Employer signs off the official end of the engagement.
Engagement Closure	Ticket handling	Ticket processing and confirmation by the Employer before Services end
	Deactivation	Termination of processes, meetings, final reporting and invoicing
	Setup	Deactivation of users, infrastructure and tool environment

c. Service Levels

Service Levels for Application Management Services are defined as following

- Initial Reaction Time
- Solution Time
- Service Time

Solution Time SLA is met if within the Service Level, MSI provides a solution proposal for resolving the issue or a workaround. If the solution proposal is based on a workaround, MSI and Employer shall agree on an action plan for creating and implementing a permanent resolution. This action plan shall include a timeline, action items and persons responsible. Solution Time SLA should be measured in the MSI AMS Ticket tool.

The Solution Time shall start when the Ticket status is set to "In Process". Solution time shall stop when the Ticket is on status "Employer Action" and continues to count when it is on status "In Process" at MSI. Solution Time also stops if MSI sets the status "On Hold" and only continues to count when the status is set to "In Process" by MSI. The status "On Hold" may be set in the following situations:

- Returning Ticket to Employer to request additional information
- Returning Ticket to Employer to request a solution approval
- Delays caused by 3rd Parties (i.e. not by MSI AMS team). In this context other MSI units than MSI AMS are also considered "3rd Parties".

d. Ticket Priorities

The following priority levels (Ticket priorities) shall apply to all Tickets:

Very High: An Incident shall be categorized with the priority "Very High" if the incident reported has very serious consequences for normal business processes or IT processes related to core business processes, and urgent work cannot be performed. This is generally caused by the following circumstances:

- A production system is completely down.
- The imminent go-live or upgrade is jeopardized.
- The core business processes of Employer are seriously affected.
- A workaround is not available.

The incident requires immediate processing as the malfunction may cause serious losses.

High: An Incident shall be categorized with the priority "High" if normal business processes are seriously affected. Necessary tasks cannot be performed. This is caused by incorrect or inoperable functions in the AMS Environment that are required immediately. The Incident should be processed as quickly as possible because a continuing malfunction will seriously disrupt the entire productive business flow.

Medium: An Incident shall be categorized with the priority "Medium" if normal business processes are affected. The problem is caused by incorrect or inoperable functions in the AMS Environment. The Employer orders a change to or a service for an existing critical business process.

Low: An incident shall be categorized with the priority "Low" if the problem has little or no effect on normal business processes. The problem is caused by incorrect or inoperable functions in the AMS Environment that are not required daily, or are rarely used. This priority will also be used for any other service request.

e. Service Reporting for AMS

MSI shall create a monthly AMS report providing Employer / ICT Consultant with information about the services provided in the previous month. The AMS report will be made available online via the AMS Reporting Dashboard for the last reporting month and as downloadable PDF document for last twelve (12) reporting months and will include the following information in the respective reporting period:

- Overview of the all supported applications
- Management summary / recommendations for continuous improvement
- Total number of Tickets received including break down per service category, per priority, per location, per application
- Total number of completed / not completed Tickets including break down per application
- Total efforts for Tickets processed per month and accumulated over last 12 months (including break down per application and service category)

In addition, real time Ticket reporting shall be made available online via the AMS Reporting Dashboard providing detailed information (including ticket ID, priority, application, service category, status) on tickets for AMS.

f. Engagement Governance

To support effective communication between MSI and the Employer, MSI and Employer will regularly conduct a status meeting, to clarify open issues and answer questions, according to the frequency defined in the table below:

Event	Attendees	Time & Date	Purpose	Frequency	Typical Method
Employer / ICT Consultant and MSI weekly meeting	Employer / ICT Consultant SME, Employer Engagement Manager & MSI Engagement Manager	1 hour date and time TBD	- Weekly status update - Review open items - Discuss risks & issues and agree resolutions - Review open or breached incidents/problems or configuration requests	Weekly	Face to Face and/or Tele conference or Video Conference
MSI provides monthly Service Reporting	N/A	Monthly event	Provide transparency on actual service delivery and SLA performance of the last month	Monthly	Monthly Service Report
Employer / ICT Consultant and MSI Steering Committee Meeting	Steering Committee, Management, Employer Engagement Manager, ICT Consultant & MSI Engagement Manager	2 hours date and time TBD	- Review Transition progress - Review financials, timelines & outputs - Review risks and issues - Resolve action items - Gather feedback	Quarterly	Face to Face
Employer and MSI Contract Review session	Employer Engagement Manager & MSI Engagement Manager	1 day Date and time TBD	- Review Scope Document timeline, scope, service hours, number of resources - Review SLA - Review performance review deliverables	Yearly	Face to Face
When the AM Service scope items “Business Improvement” and/or “IT Operations Improvement” have been chosen, the following additional governance events will be typically conducted by AMC and Employer.					
Business Improvement - Planning meeting	Employer management and SME (business owner, architects, Employer’s	2 days Date and time TBD	- Set business priorities and focus areas for improvements and innovations - Validate provide business requirements and maintain backlog	yearly	Service Planning Workshop (Face to Face and/or Tele conference or Video Conference)

Event	Attendees	Time & Date	Purpose	Frequency	Typical Method
	engagement manager) MSI Engagement Manager, MSI Solution Architect		- Define action items and link to solution release calendar - Creation of yearly business improvement service plan and initiate sign-off by Employer		
Business Improvement - Operational Review & planning session	Employer SME, ICT Consultant, MSI Engagement Manager, MSI Solution Architect	2 hours Date and time TBD	- Review of business improvement activities and delivered value - Review of on-going activities and open action items - Update of business improvement service plan and initiate sign-off by Employer	TBD (quarterly /monthly)	Review & planning session (Tele conference or Video Conference and/or Face to Face)
IT Operations Improvement - Assessment & planning meeting	Employer management and SME (IT process owner, architects, engagement manager), ICT Consultant, MSI Engagement Manager, MSI Solution Architect	2 days Date and time TBD	- Baseline assessment of current operations efficiency - Determination of operations improvement KPIs - Review of previous period improvement KPIs - Creation/update of rolling operations improvement service plan	yearly	Service planning workshop (Face to Face and/or Tele conference or Video Conference)

Event	Attendees	Time & Date	Purpose	Frequency	Typical Method
IT Operations Improvement - Operational Review & planning session	Employer SME, ICT Consultant, MSI Engagement Manager, MSI Solution Architect	2 hours Date and time TBD	- Review of continuous operations improvement activities and delivered value - Review of current operations improvement KPIs - Open action items and ongoing activities - Adjustment of rolling operations improvement service plan	TBD (quarterly/monthly)	Review & planning session (Tele conference or Video Conference and/or Face to Face)

Eligible Good & Services and OEM Criteria:

- For purposes of this Clause, the term “goods” includes commodities, raw material, machinery, equipment, and industrial plants; and “related services” includes services such as Insurance, Transportation, Supply, Installation, Integration, Testing, Commissioning, training and initial maintenance.
- MSI shall quote only one specific make and model from only one specific OEM, for each of the products/services. Providing more than one option shall not be allowed. All products/services quoted by the MSI should be associated with item code and names and with printed literature/brochure describing configuration and functionality. There should not be any deviation for the solution proposed by MSI in reference to the requirements and scope defined in this RFP document.
- The proposed OEM for Connectivity Bandwidth must possess necessary Telecom licensing required for providing leased network infrastructure or leased circuits as per TRAI/DOT regulations. The Bandwidth OEM must possess necessary ISP & NLD licenses (valid at the time of bidding) required for providing leased network infrastructure.
- MSI should give a declaration that the OEM for all active components/products or technology quoted are neither end-of-sale nor end-of-life as on the date of installation and commissioning and are not end-of-support till the successful completion of O&M period of the project.
- MSI has to ensure that the hardware/ ICT Infrastructure component proposed by the bidder should be latest version of the product at the date of submission of the Bid. Also the bidder has to ensure that the support for the proposed equipment's is available during the entire duration of the project and after that if required
- Each of the proposed OEMs should either have existing capability and infrastructure to provide 24x7x365 technical support in India, or should provide an undertaking that they would establish the requisite infrastructure and capability to provide 24x7x365 technical support, within 45 days post emerging a winner in this bidding process.
- All proposed equipment/items should be necessarily quoted with back-to-back OEM warranty.
- MSI other than sole agents in India of the quoted software solutions, IT Equipment's, etc. must submit a letter of authority from the OEM on their letterhead duly signed and stamped by authorized signatory that they have authorized the MSI to quote for the said system/application/equipment/platform/solution.

3.1. Basic Network Infrastructure Work package

3.1.1. Citywide Networks - Ducts & Dark Fiber & Network passive

Fiber optic has become a unanimous choice for higher bandwidth, longer distances, speed and more importantly convergence. In fact, this period is an era of “Fiber-to-the-everything”, where fiber connectivity is indispensable to support all the services/applications of a smart city.

Therefore, the objective is to build a citywide fiber optic Network for CLUSTER A-1 of Cluster-A, Dholera Activation area. The network should be robust, redundant, and scalable and provide enhanced citizen experience through improved connectivity across the city.

The fiber optic network must be built to provide connectivity to all citywide services like surveillance, Utilities, Wi-Fi etc. and to all its tenants (FFTX), ISPs, TSPs, and LCO etc. The network should have a high availability and to be built on “Open-Access Fiber network” principle, which can easily accept passive and active upgrades and the type of upgrade required shall depend on Day-1 and future services/applications to be served. The proposed design for the citywide fiber network should be scalable and flexible to support new technologies as the city evolves to make use of emerging services/applications. In addition, it should enable an efficient use of capital where onetime investment is made and it caters to all the above-mentioned requirements, and avoid any digging in future for laying of additional cables.

More importantly, the network should be so built that it should be scalable to adjacent areas as and when the city grows and in turn should have no effect/re-work in existing live network of Cluster A-1 area.

In addition, the city-wide fiber optic Network should ensure optimal use of proposed ICT duct banks/Manholes with sufficient spare ducts and space within the ducts/Manholes which will provide a relatively inexpensive method of addressing subscriber growth, additional service providers and emerging technologies which in turn shall increase the life expectancy of OSP system for over 30 years.

Below are the proposed infrastructure and considerations.

The entire Area in Cluster A-1 covers influence area of 7.48 Sq. Km and ICT concrete encased duct banks is being constructed on both sides of the road. Trench length from ABCD to Activation Area both sides is of Length 6.83Km and Length 6.24Km

- . Refer below drawing.

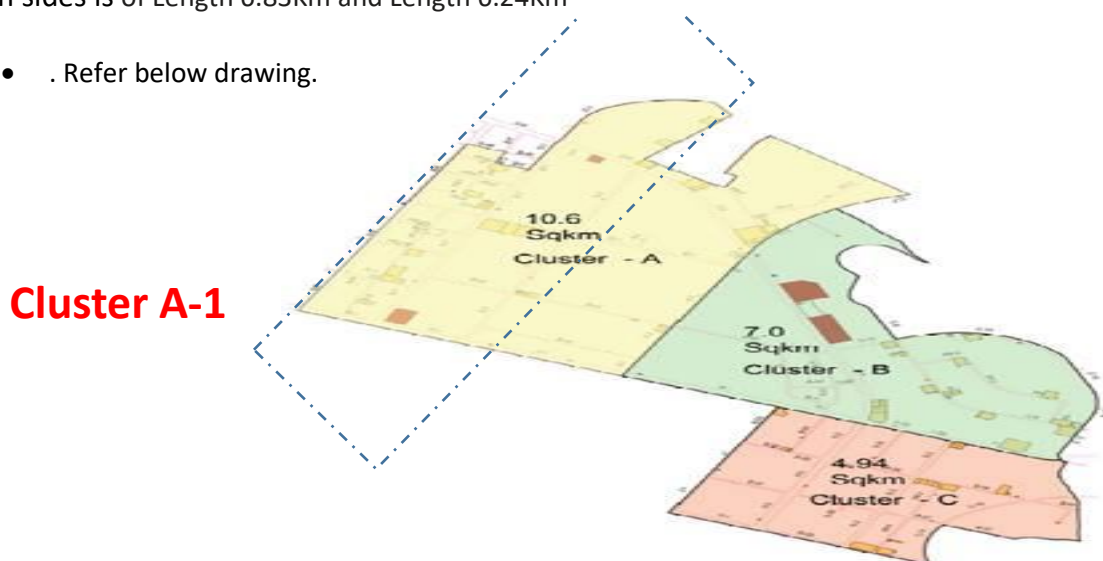


Figure -5, Cluster A-1

- Proposed dedicated concrete encased ICT duct banks consisting of 30 HDPE Conduits of 50 mm OD on both sides of the road shall be used for installation of fiber optic cables for citywide services and FTTx services. Refer below Drawing-1.

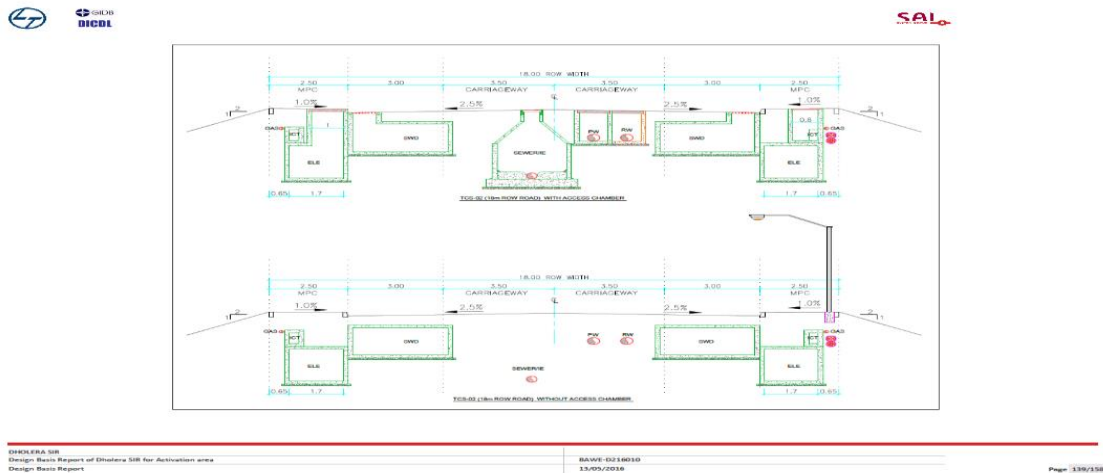


Figure -6, Proposed ICT duct banks

- Manholes are proposed at every 60-meter distance, which facilitates the Installation of fiber optic cables and placement of splice closures for splicing/branching of cables to properties and other utilities. Refer below Drawing for manhole dimensions.

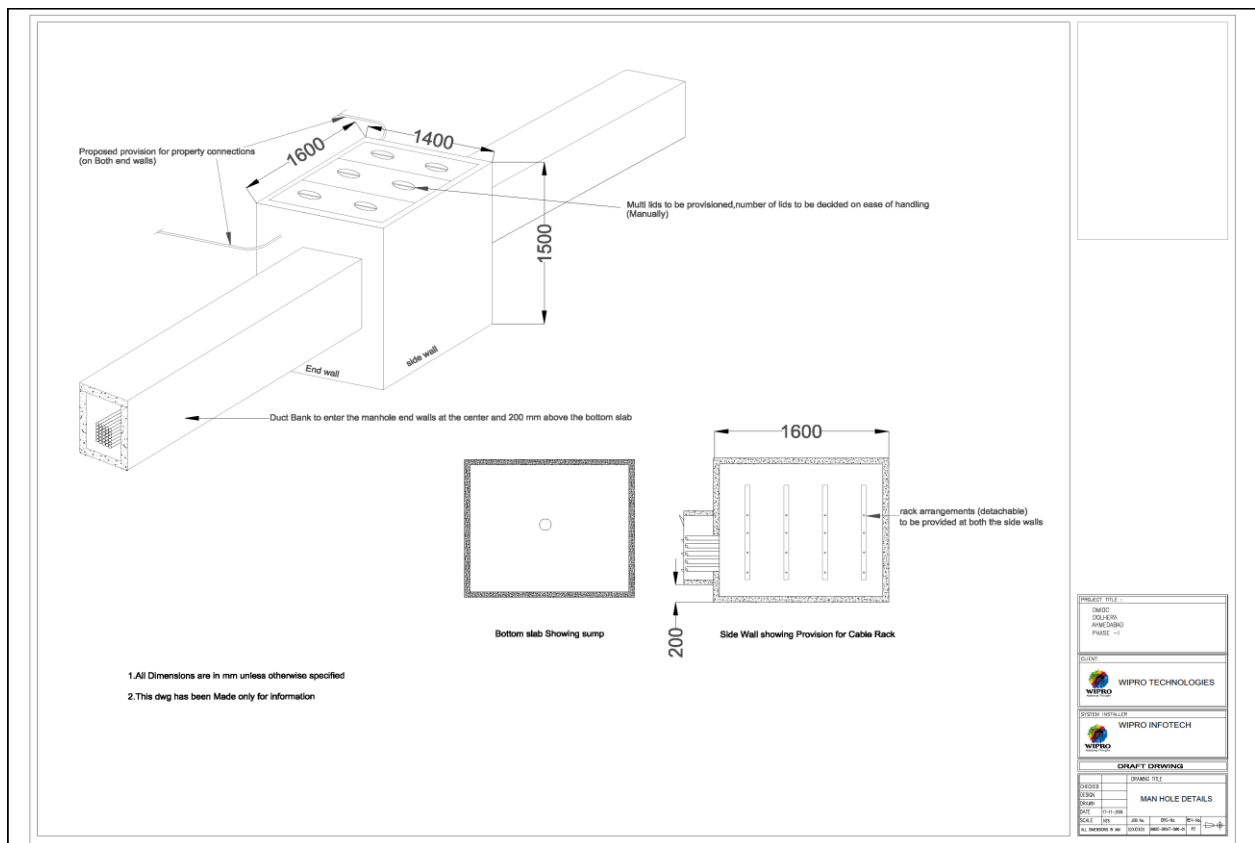


Figure-7 Manhole dimensions

- The whole Cluster A-1 area has seven numbers of service area buildings spread across as per the RF Mapping and these individual service area buildings shall be used for rolling out the Access/Distribution fibers to end devices and buildings.
- Dedicated 5-way HDPE ducts are proposed along with street light power cable ducts for installing FO cables(Roads and services vendor scope) for connecting CCTV, which are in turn proposed to be mounted on street light poles. Each street light pole will be provided with Hand hole and Accesses panel (integral part of Street light pole) for installation and splicing/termination of fiber optical cables.
- For establishing connectivity (Back bone) from Server room (located In City, DICDL building) to Phase -1 area, direct buried HDPE ducts bank (trenching/HDD) to be constructed by MSI. Two geographically redundant paths must be constructed depending on the path and ROW availability, each path having 12 HDPE ducts of 40 mm OD.
- Duct should be Corrugated from outside and inside layer should be smooth with Silicone Coating. Size 40mm OD /32mm ID, 750N (Newtons) DWC Pipe with Silicone Coating,
- Requirement and testing for 40mm OD / 32mm ID Double Walled Corrugated (DWC) HDPE Ducts with Silicone Coating as per IS-14930 Part II, 750N, buried underground including ducts & Duct Fittings for protection. BIS License is must
- MSI shall implement complete Backbone (including trenching) and Distribution and FTTX fiber optic cable (including supply) network and the remaining (installation of FO cable in accesses area) is in the scope of Roads and services vendor.

In Accesses Network, Roads and services vendor will install optical fiber cable to street light poles, RTUs, Bus stations and utility buildings. However, termination, splicing, supply and installation of Patch panels, and patch chords including installation and testing for CCTV system are in the scope of MSI and remaining is in the scope of Roads and services vendor.

Scope of Work

The scope of the RFP is to build an END-TO-END citywide fiber optic and FTTX network for the entire Cluster A-1 area with an uptime of 99.74%, which shall include supply, installation, testing & commissioning of this networks and its operations and maintenance.

- The solution shall comprise of supply, installation, testing, commissioning, training and handing over of the complete passive network to operations team. All materials, equipment, hardware, software, appliances and necessary toolkits, complete with all the required components & documentation strictly as per the enclosed tender specifications is in the scope of MSI.
- The scope includes the supply, installation & commissioning of any material or equipment including civil works and works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project
- The MSI shall provide documentation including system and operation manuals as well as the necessary as- build diagrams and design drawings.
- The complete network must be handover to DSIR/city DICDL and shall be responsible for providing support and maintenance (five years) for all equipment and systems installed on site on 24 x 7 x 365 basis, reporting to City DICDL/DSIR and adhere to an uptime of 99.74 %.
- The network so built must cater to all the services envisaged in this RFP and take care of the future needs of the city and integration of Cluster A-1 area with other part of Dholera smart city, which shall be developed in a phased manner.

The MSI shall provide qualified and experienced implementation team on site for execution of the Project including complete maintenance of the network for a period of 5 years.

MSI shall be responsible to carry out the detailed survey for each of the solution component required to finalize infrastructure requirement, network bandwidth requirement, operational & administrative

challenges etc. and shall submit detailed Site Survey Report and Project Execution Plan to the customer or its designated agency/department before implementation of this network.

The subsequent sections detail out the high-level solution and functional requirements with respect to each of the solution components. The MSI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. MSI must perform an independent analysis of any additional work that may be required to fulfil the requirements as mentioned in this RFP.

Solution Architecture

The following two Fiber networks solution is envisaged for Cluster A-1 area in Cluster-A, Dholera Activation area,

- Fiber Optic Network connecting 7 service areas
- FTTx Network

Fiber Optic Network (For 7 Service areas):

Fiber Optic Cable Schedule for Cluster A1

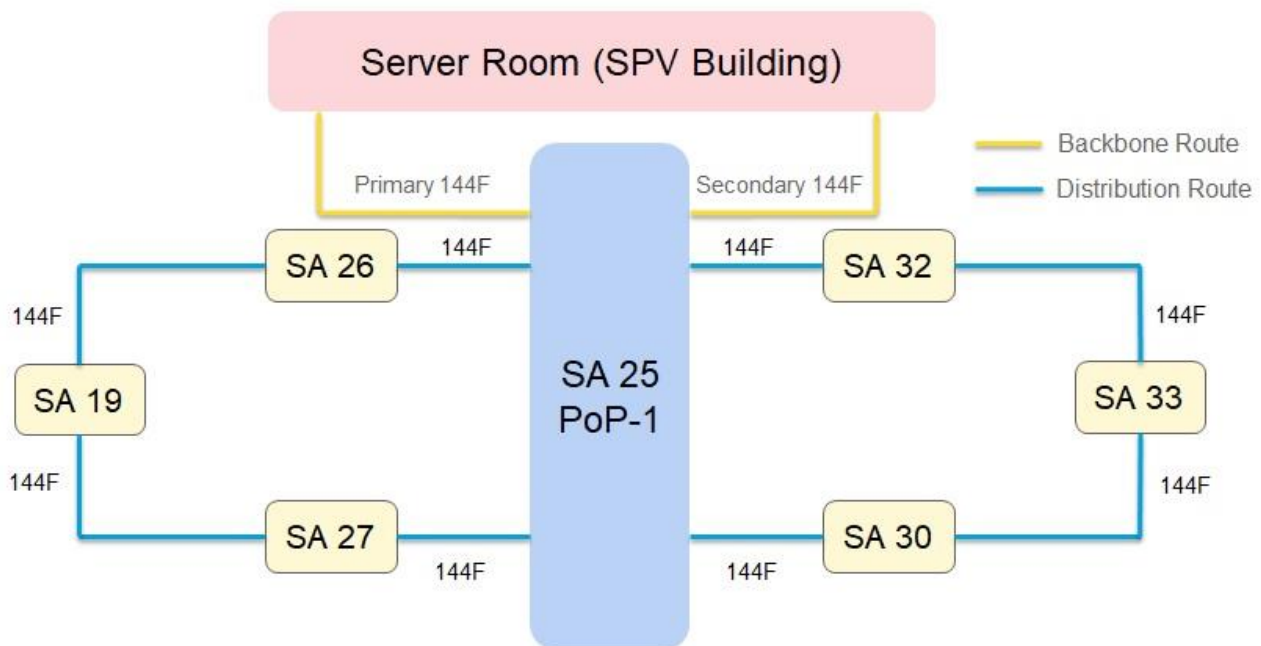


Figure-8, Fiber optic Schedule for Cluster A-1 Area.

The above Citywide fiber optic network architecture for Cluster A-1 area consists of following elements.

- Backbone fiber network (Blue Line, MSI scope).
- Distribution fiber network (Green line , MSI scope)
- Access fiber network
- FTTx Network

Back Bone Network.

Back bone network between DICDL building and primary POP to be built using 144 F single mode , G652 D , Armored fiber optic cable and shall have two completely redundant paths , Primary and secondary . Nowhere

these two paths to cross each other. For the portion in Back bone path, wherever the Ducts/Duct Banks are not available, direct buried Duct bank construction must be done for installation of Backbone cables. Below is the proposed routes for Backbone cable installation.

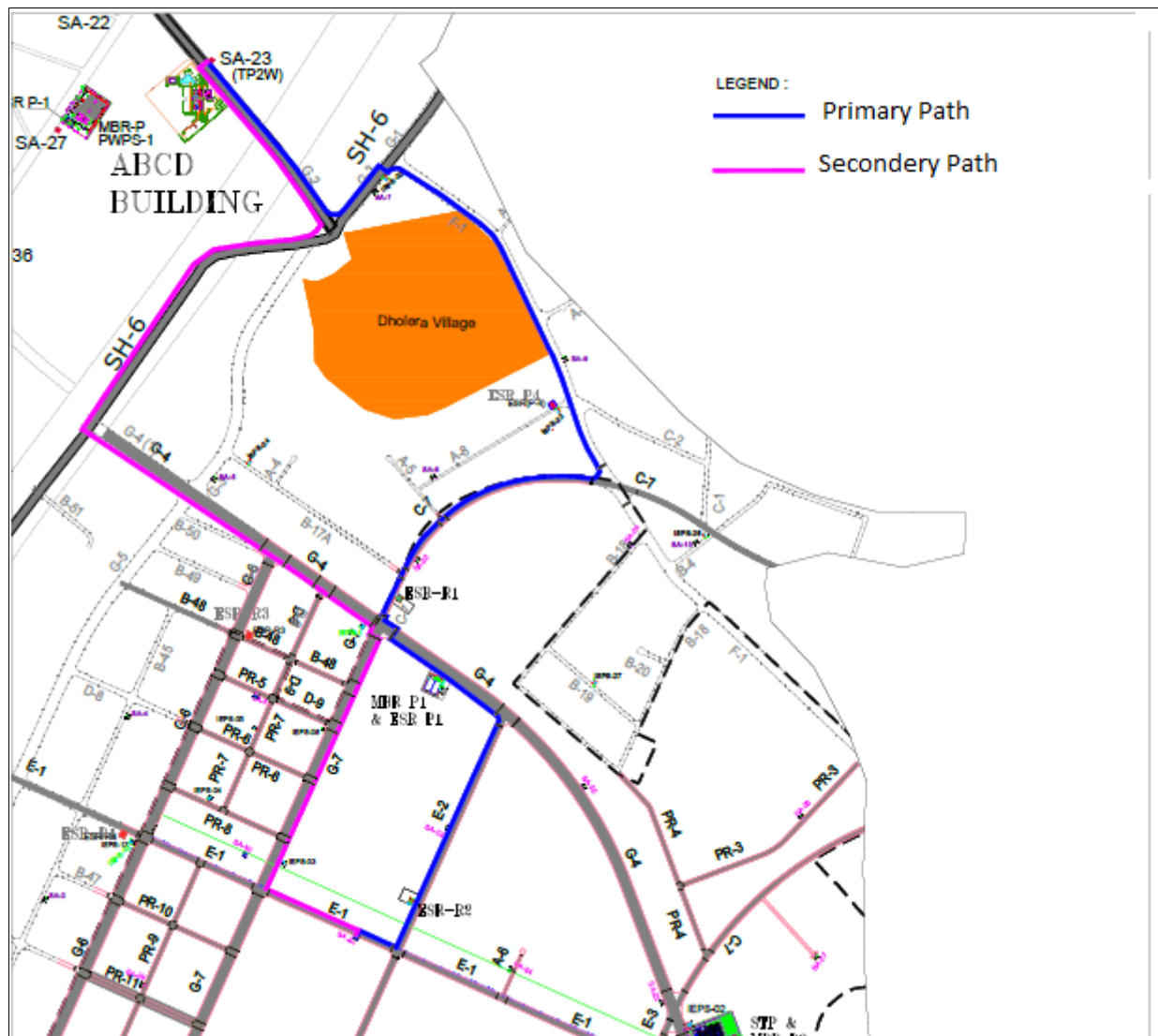


Figure-9, Fiber Optic Backbone network.

Distribution Network.

Distribution Network in Cluster A-1 area of Cluster-A must be built using 144 F single mode, G652 D, unarmored fiber optic cables and for the same existing Concrete encased duct bank on both sides of the roads has to be used.

Out of 7 service area buildings one strategically placed service area building to be designated as primary POP and all the distribution cables coming from the remaining service area building's has to converge into Primary POP and they should be in a ring configuration. Each distribution ring to have 3 service area Buildings in a ring topology and a mesh network has to be created for these distribution rings for optimizing the availability of the Network.

Accesses Network.

MSI to terminate and test all the fiber cables related to CCTV surveillance in service area buildings with in the Cluster A-1 area. Supply of all the Patch panels, Racks and all other required Splice accessories is in the scope of MSI.

Apart from termination of fiber cables in all the service area buildings, MSI must splice /terminate fiber at six traffic junctions mentioned in drawing -4, two fiber drops of 12 core at each location (street light poles) for Surveillance, Variable Message Signboard systems as well as other system from 144F CCTV fiber cable.

Also, design (fiber and copper), Copper cable installation (from switch to end equipment's), termination, testing activities for Surveillance, VMS and other systems is in the scope of MSI. Supply includes Copper cables, din rail Patch panels/ Pre-terminated industrial grade pigtails, splice closures, racks and rack mount patch panels, copper patch panels and other accessories required for the complete solution.

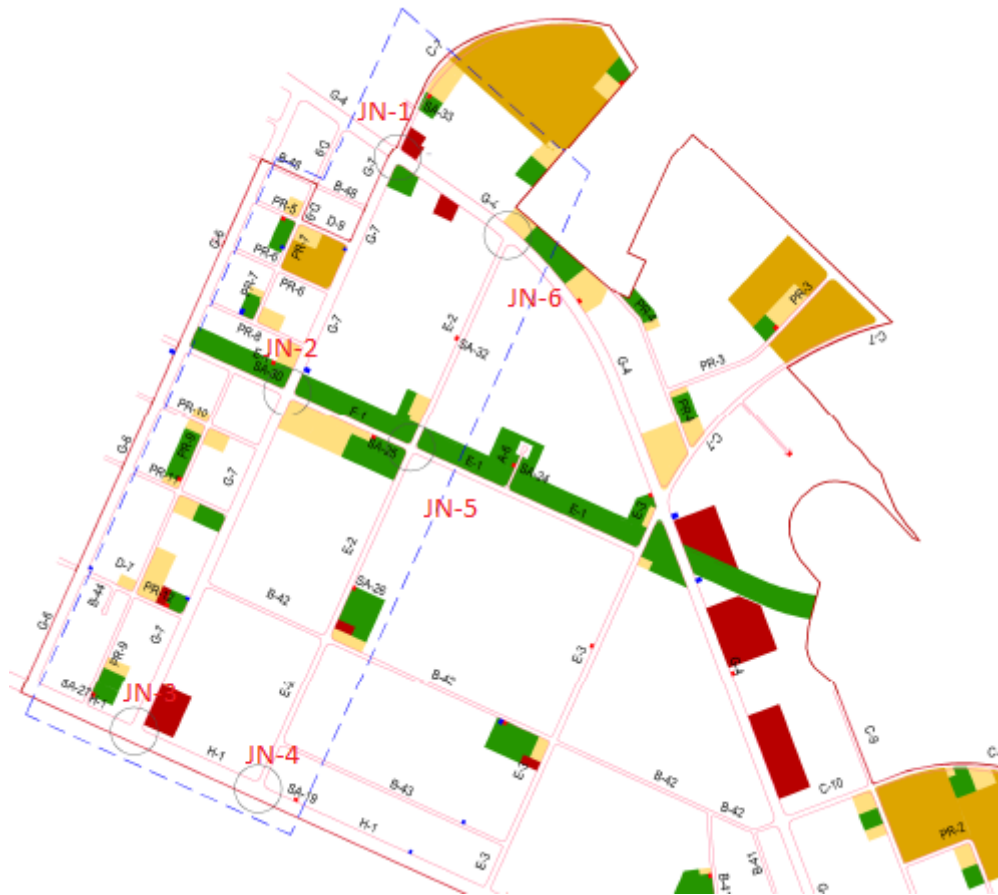


Figure -10, Junctions layout for Cluster-A1

POP Room:

- MSI shall be required to undertake the complete site preparation and design-build exercise for one (1) POP facility as per the requirement in consultation with Client and their representatives.
- The detailed design in all aspects for the design-build (including but not limited to civil, mechanical, structural, electrical, communications, fire, fit-outs, etc.) of the POP facility and the plot shall be the responsibility of the MSI and be approved by the Client or its representative. MSI shall have the required personnel on the team including architect, structural engineer, MEP, etc. as needed for this design-build. At least two (2) options for the design-build shall be proposed for the POP facility.

- MSI's scope includes finalization of locations of the POP in cognizance with DICDL as well as its ICT Consultants, development of the building, development of the plot in compliance with the regulations including necessary infrastructure within the plot, fencing, coordination with the tenants, coordination for installation of cellular towers and any other infrastructure of the tenants, partitioning for dedicated space for every tenant, and construction of the POP facility as a telecommunications rated facility;
- All tenants will get dedicated partitioned space for their equipment along with access to power and other basic infrastructure. MSI shall ensure that the passive infrastructure in terms of ducts, termination points, etc. for routing within the POP is provided for all tenants. MSI shall coordinate with all tenants to ensure end-to-end installation of all the tenant provided equipment. All tenant space shall have dedicated access, be secure and should be modular in construction so that the number of tenants can be increased or decreased in the future;
- MSI shall furnish the POP room as part of the civil work in all aspects. All material to be used shall be of fine quality ISI marked or equivalent. The furnishing includes but not limited to:
 - False ceilings;
 - False floorings;
 - Paint work;
 - Storage;
 - Layouts and partitioning;
 - Doors and Locks;
 - Fire proofing of all surfaces;
 - Insulation, etc.
- MSI shall install electrical distribution system in the buildings. MSI shall be responsible for proper and uninterrupted equipment working and shall ensure this by having the telecom equipment and server room power distribution with redundancy:
 - Incoming electrical feeder supply;
 - UPS system with battery bank for all DICDL loads;
 - Connection between UPS system and the DICDL equipment shall be redundant. No single point of failure shall exist in the power connectivity between the DICDL equipment and UPS.
- Since POP room is a critical area, precise air conditioning/Air conditioning system as per the directions from DICDL and ICT consultant MSI shall exclusively install and maintain the required temperature for the said room/area. MSI should design and deploy the air conditioning units such that there should not be any impact on the operating temperature required to be maintained in the POP room;
- MSI shall install UPS system to provide redundant power supply to following needs:
 - All ICT equipment's procured and installed as well as deployed for DICDL;
 - Access control;
 - Fire detection and suppression system of POP facility;
- MSI shall do complete electrical cabling work for telecommunication equipment which shall include but not limited to:
 - Main electrical panel in room;
 - Power cabling;
 - UPS distribution board;
 - UPS point wiring;
 - Power cabling for utility points and utility components etc.;

- Online UPS;
 - Required earth pits for the components;
 - Fire retardant cables of rated capacity exceeding the power requirements of equipment to be used at maximum capacity;
 - All material shall conform to ISI standards as per industry practice.
- The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards;
 - MSI shall install Building Management System (BMS) at POP room for integrated monitoring, control and automation of multiple building components;
 - MSI shall also be responsible for installing a rodent repellent provision inside the POP facilities.

FTTx Network:

In Cluster – A1 area, a significant investment is made in establishing the ICT duct banks/manholes for citywide services/FTTx and sufficient duct containment is envisaged for future use. So the MSI is expected to build a robust “open- access fiber network” which can be leased to TSPs, ISPs and others which will in turn earn significant revenue and avoid repeated digging by other operators. TSPs and ISPs can access this fiber optic network, install their own active components and provide required services within Cluster – A1.

For FTTx services, 12-core fibers has to be reserved in all the Manholes for whole of Cluster – A1 area Manholes from the nearby service area buildings. Necessary cable loop to be kept at alternative ICT manholes for branching and operation and maintenance purpose. In each of the 144F fiber cable, the last tube shall be kept as spare for O&M and future use.

MSI has to conduct detailed site survey to confirm redundant path availability for backbone, distribution Accesses and FTTx networks. MSI shall have to take all required ROW approvals from the respective authorities.

MSI shall submit detailed architecture of the citywide and FTTx network. All the equipment shall comply with the specifications given in RFP. MSI shall prepare High level network architecture and Low level Network architecture for both networks and produce IFC drawings before implementation of any works. The same has been captured in the RFP.

Functional, Technical and Non-Functional Requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Description
NET-CWN-1.1	OSP	City wide FO network	Back bone network	A detailed field survey to be conducted for freezing two redundant paths (trenching/HDD) for connecting Server room (DICDL building) to Primary POP. These two paths to be completely redundant which forms the Backbone Network for Cluster A-1 area. Nowhere these two paths to cross each other. Wherever ITC existing duct bank is not available, new trench to be built with legitimate ROW permissions for installation of Backbone cables. Duct number 1-3 (on either side of road) in the existing ICT duct bank to be used, with in Cluster A-1 area for Back bone cable installation .Lainson for ROW to be done By MSI and the trenching permission charges if any will be borne by DICDL.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Description
NET-CWN-1.2	OSP	City wide FO network	Back bone network	Detailed RFI drawings (schedules, schematics, spicing diagrams, cable routing diagrams, implementation plan, and method statement) to be approved by Customer before start of any work. If any change in design is suggested, which will enhance the network availability has to be discussed with customer for his approval.
NET-CWN-1.3	OSP	City wide FO network	Back bone network	Direct buried pre-Lubricated HDPE ducts of 40 mm OD shall be laid at a depth of 1.5 MT's from top of the HDPE ducts for installing Back Bone FO cables .12 number of 40 MM HDPE ducts shall be installed in each path of 6 different colors.
NET-CWN-1.4	OSP	City wide FO network	Back bone network	Open cut / HDD method to be adopted for laying the ducts from DICDL building (ABCD complex Battery limits) to Cluster A-1 area battery limits. This trench has to be properly connected at both ends to existing MH i.e. At Cluster A-1 area Battery limit MH and MH at ABCD complex battery limits.
NET-CWN-1.5	OSP	City wide FO network	Back bone network	Splice/Pull thru chambers has to be provided along the path also warning tape, route markers, electronic route indicators, protection if required, to be installed throughout the trench length. These trenches shall be constructed as per ITU-T Telecom standards or any other International Telecom standards. Wherever the specified depth is not achieved proper protection to be provided (like DWC duct with concrete cover, GI pipe etc.). For culvert/road/bridge crossing GI pipes to be installed, for the same method statement has to be approved by Customer.
NET-CWN-1.6	OSP	City wide FO network	Back bone network	G652 Single mode 144 F Armored cable is to be installed (including supply) for this purpose and proper earth for laid cable to be provide as per standards. Cable installation, splicing, termination and testing has to be done as per ITU-T standards. Each primary cables and secondary cables to be terminated on different patch panels mounted on two different racks at both ends (Server room and Primary POP). Fiber cable to be installed inside the HDPE duct by blowing methodology. Duct integrity test for all the cable carrying ducts and spare ducts to be done before blowing of FO cable and the report has to be submitted to customer. 4 Km drum lengths are suggested for backbone network and cable drum lengths to be so procured that minimum or no fiber cable joints should be achieved in any particular link.
NET-CWN-1.7	OSP	City wide FO network	Back bone network	In each Backbone path, one 144 F FO cable to be installed as per Approved standards. Also, shall propose any leased line provisioning for the third path to customer.
NET-CWN-1.8	OSP	City wide FO network	Back bone network	MSI to Supply and install all the required FO cables, HDPE ducts, racks, patch panels, fiber patch chords (LC-LC), Duct accessories like end plugs/simple plugs, clamps, splice/pull thru chambers (at every 500 MT), warning tape, route indicators, electronic route locators for chambers etc. and all these materials to be approved by Customer before installation and meet all the required standards (as per ITU-T outside plant telecom standards)
NET-CWN-1.9	OSP	City wide FO network	Back bone network	Pre installation (drum test) and post installation test to be done for all the FO cables as per standards .Also should adhere to manufacturer's instructions/installation manuals. Customer approval should be obtained before carrying out any Implementation works.
NET-CWN-1.10	OSP	City wide FO network	Back bone network	Any damage to public or Private property during implementation work (trenching and cable installation works) to be borne by MSI. All the safety measures like installing barricades, taking cross pits, tracing of existing utilities etc. to be taken care of to avoid any damage to existing properties and accidents at the time of execution. In case of any damage/ faults to cables/Accessories and other items during execution must be Replaced / Rectified by MSI on his own cost.
NET-CWN-1.11	OSP	City wide FO network	Back bone network	All the required documents like fiber test reports (pre installation and post installation), As build drawings (cable routing drawing, cable schematic, splicing drawings, schedules etc.) to be submitted for each link for acceptance test. In addition, NOC copies to be obtained by relevant Government and private agencies before carrying out the final Acceptance test. Proper housekeeping has to be maintained at all places during any implementation activity.
NET-CWN-1.12	OSP	City wide FO network	Back bone network	Tagging of cables (tagging material to be approved by customer), ducts, splice chambers, patch panels, racks etc. to be done before handing over of each link and should be as per any international Labelling standards. The labelling materials to be as per customer approved standards.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Description
NET-CWN-1.13	OSP	City wide FO network	Distribution network	Distribution fiber optic network to be built across Cluster A-1 area connecting all the Service area buildings and this fiber network will provide the backbone on which all the other layers (Access) can reside for connectivity requirements for all proposed smart city solutions /applications. This citywide fiber shall enable city DICDL to provide connectivity across Cluster A-1 area to provide bandwidth to all sections of society, public offices and city utilities.
NET-CWN-1.14	OSP	City wide FO network	Distribution network	Distribution Fiber Optic Network to be redundant and for the same Proposed ICT duct bank (30 ducts on either side of the road) shall be used with in Cluster A-1 area and a mesh network to be created between all the Service areas in Cluster A-1 area.
NET-CWN-1.15	OSP	City wide FO network	Distribution network	In Cluster A-1 area, there are 7 service area buildings identified as per RF mapping. Out of these 7 buildings one strategically placed Service area building shall be designated as Primary POP, which will act as aggregation node for all the remaining service areas buildings (6 Buildings). This primary POP, apart from acting as the aggregation node for reaming 6 service areas will also serve as service area building for the adjacent area .
NET-CWN-1.16	OSP	City wide FO network	Distribution network	The ICT duct banks on each side of the road shall be used for Building the Distribution network with in the Cluster A-1 area. Duct number 6-10 on each side of the road is reserved for the laying of Distribution FO cables.
NET-CWN-1.17	OSP	City wide FO network	Distribution network	The cables running between any two-service area buildings should have slack cable of 25 meters in every 5th existing ICT manhole for operation purpose. These cable slacks to be stacked on the Racks provided inside of the ICT manholes, tagging of the same to done as per standards approved by Customer.
NET-CWN-1.18	OSP	City wide FO network	Distribution network	Before installation of this FO cable Mandrill test must be done for all HDPE ducts (50 mm) and submit the Mandrill test report to Customer. Once mandrill test for a section is done (MH to MH), the ducts must be sealed with standard end plugs.
NET-CWN-1.19	OSP	City wide FO network	Distribution network	Once the FO cable is installed for any link between 2 service area buildings the cable carrying HDPE ducts to be plugged with proper Split plugs and both ends of the cable to be terminated on to a dedicated 144 F patch panel of approved make on dedicated Network racks inside each service area building. Each link to be tested with power meter and OTDR traces to be obtained from both ends for all the cores (for both 1310 and 1550 Nm) .All the fiber cores in each cable has to be terminated/ tested and test reports to be submitted in a standard format to customer.
NET-CWN-1.20	OSP	City wide FO network	Distribution network	All the distribution cables to be terminated in first floor of each service area building on to dedicated patch panel/racks. These cables inside the service area building must be routed properly on the dedicated cable trays provisioned inside of the service area Building.
NET-CWN-1.21	OSP	City wide FO network	Distribution network	After the detail design, drum lengths (2.KM / 4 KM) to be so procured that splice between any two-service area buildings must be avoided.
NET-CWN-1.22	OSP	City wide FO network	Distribution network	All the materials like FO cables, patch panels, network racks, duct accessories, cable accessories, tags, ties etc. must be procured by MSI. Also, all the tools and equipment's like, duct rods, mandrills, cable un-coilers, lubricants, jacks, cable blowers, safety equipment, communication equipment, cranes, man lift, cable blowing m/c's etc. to be arranged by the MSI. Patch panel and splice closure should support mid-span splicing.
NET-CWN-1.23	OSP	City wide FO network	Distribution network	Before starting of any implementation activities all the documents like detail design documents, RFI drawings, implementation plan, pre- installation test reports, manufacturer's installation manuals etc. must be approved by customer.
NET-CWN-1.24	OSP	City wide FO network	Distribution network	After completion of any link As build drawings, redline drawings, post installation test reports, NOC documents etc.to be submitted to customer for Final Acceptance test. All the cables, patch panels, racks, fiber ports, ducts, cables, splice closures must be tagged as per approved standards.
NET-CWN-1.25	OSP	City wide FO network	Distribution network	Safety measures and proper housekeeping must be taken care throughout the entire Implementation phase of the project.
NET-CWN-1.26	OSP	City wide FO network	Distribution network	All the cores in a link to be tested with power meter and traces to be obtained with OTDR, from both sides. The splicing and testing to be carried out as per ITU-T telecom standards. MSI to procure and install patch chords for patching between Fibers patch panels and switches in all the buildings in Cluster A-1 area and server room (DICDL building).

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Description
NET-CWN-1.27	OSP	City wide FO network	Distribution network	At the time of Acceptance test, if any faults and defects are observed the same must be rectified /replaced with no extra cost to customer.
NET-CWN-1.28	OSP	City wide FO network	Operations	After handing over of the network to city DICDL with all the relevant documentation the MSI has to take care(operation and maintenance) of this network for the number of years specified in the RFP by engaging sufficient manpower for daily patrolling , FRT teams , team for regular health checkup and documentation etc. in discussion with customer /Customer representative
NET-CWN-1.29	OSP	City wide FO network	Operations	An uptime of 99.74 % must be maintained for the entire citywide fiber optic network. The MTTR (mean time to restore) for any fiber faults is to be less than 3 hours. Penalty will be applicable for any non-adherence to the above-mentioned SLA's.
NET-CWN-1.30	OSP	City wide FO network	Operations	The operation / maintenance has to be carried out for entire fiber optic network which is going to be built under this project i.e. Back bone fiber, Distribution fiber Access fiber (to be laid by Utility vendor), FTTX fiber and copper cables etc.
NET-CWN-1.31	OSP	City wide FO network	Operations	Apart from Operations of citywide fiber Network the operations team has to take care of all the provisioning and establishing of fiber (splicing testing, documentation) connectivity to the end equipment's and Buildings with in Cluster A-1 area(as and when required) like fibers for /ISP's /TSP's /government Buildings including any civil works related to this activity.
NET-CWN-1.32	OSP	city wide FO network	Operations	One FRT team to be provided for maintenance of the entire citywide network (once handed over). Team having dedicated splicing team and Civil team (in two shifts) with all the necessary tools and equipment's. The same team will be used for extending the fiber connectivity to end user's as and when required. MSI should adhere to the SLA's fixed by DICDL for all connectives with in the Cluster A-1 area.
NET-CWN-1.33	OSP	NET-FTTX	FTH	FTTx FO cables to be installed in the existing ICT duct banks on either side of the road.
NET-CWN-1.34	OSP	NET-FTTX	FTH	In 144 FTTx network a slack cable as per requirements to be kept at every alternative MH starting from the service area building for carrying out splicing activity for property connectivity and operation purpose . This slack cable to be properly stacked and secured on to the cable racks provide inside of each MH.
NET-CWN-1.35	OSP	NET-FTTX	FTH	After installation of all the cables all the ducts inside each MH has to be plugged properly so as to avoid any water ingress and rodent entry. DIT /Mandrill test has to be carried out before installation of any cable.
UTI-STL-1.1	OSP	UTI-CCTV	CCTV	Supply and Installation of dedicated 144 F FO cable to all the street light poles on which CCTV are proposed to be mounted, is in the scope of roads and services vendor. supply and installation of smart street light poles with access panel with mounting arrangement for switches , Patch panels ,PDU'S, camera etc. Is in the scope of roads and services vendor .Also each pole will have a dedicated HH to facilitate Installation of cable and space for placing Joint closure and the same will be provided by roads and services vendor.
UTI-STL-1.2	OSP	UTI-CCTV	CCTV	Terminating 144F, CCTV FO cables at both ends inside of service area building testing, and submitting the test repots is in the scope of MSI. For the same all the required dedicated patch panels, racks and fiber patch chords must be provided by MSI.
UTI-STL-1.3	OSP	UTI-CCTV	CCTV	The MSI has to provision fiber (12 core) to two street light pole in each traffic junction (six junctions) for connecting CCTV's proposed to be mounted in these Street light poles . MSI needs to carry out the detail designing and get customers approval before proceeding with the above said Splicing, termination, and testing activities.
UTI-STL-1.4	OSP	UTI-CCTV	CCTV	Supply and installation din rail mount patch panels, and required Patch chords inside the accesses panels(for 6 Junctions ,12 street light poles) and dedicated racks and rack mount patch panels at Service area building is in the scope of MSI . The din rail patch panel to be of industrial grade and must have a rugged constructing as it is going to be placed in the field.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Description
UTI-STL-1.5	OSP	UTI-CCTV	CCTV	Supply and installation of required copper cable(CAT6 A) from the Industrial grade switch inside of the accesses panel to the CCTV mounted on the pole is in the scope of MSI .All these installation should be well protected and tamper proof. In addition, supply and installation of Required Patch panels and patch chords (LC) inside each service area building is in the scope of MSI.
UTI-STL-1.6	OSP	UTI-CCTV	CCTV	The branch splicing at the six traffic junctions must be done using mid-span technic to minimize the Losses in other dark fibers.

Technical specifications

Fiber optic Cable

Fiber optic cables will comprise of single-mode cores with a graded index of 9/125µm meeting the minimum requirements of ITU-T G.652

Each fiber cable shall have 144-core minimum count of loose-buffer tubing type with 12-cores per buffer tube. Cables with core counts less than 48-cores may be used for cable routes to field or end-user equipment and drop connections. Internal fiber optic cables that run within a building will be of loose-tube construction and have a central strength member, will be fire retardant, and shall have LSZH sheath.

All fiber optic cables will be terminated on fiber optic patch panels mounted in rack /cabinets except for field equipment such as CCTV cameras/RTUs etc. that may be terminated in the Accesses panels with suitable patch panels like industrial type Din rail patch panels as per the space availability. Cores will be fusion spliced to pigtails. Duplex patch cords shall be used to complete the circuit to the end equipment. Patch cords in field shall be of ruggedized type. Patch cords may be color-coded to identify the associated system and/or application.

Cable Specification:

Unarmored FO cable (inside ICT Duct banks)

The FO cable shall operate over the entire wavelength range from 1310 nm to 1550 nm, removing the water peak (high attenuation) in the E-band. All dielectric, Loose Buffered, Filled, for underground and direct buried environment. The structure of the cable core shall permit high cable flexibility with minimum stress to the individual fibers. One or more strength members shall be an integral part of the cable construction. The strength members shall be sufficient to support the stress of installation and to protect the cable in service.

- The core shall be filled with a compound to inhibit water migration and shall be wrapped with a barrier tape. The filling compound shall be homogenous and uniformly mixed. The compound will at least be sufficiently translucent for fiber identification. The filling compound shall not affect the color of the individual fibers, is non-toxic and present no thermal hazards. The drop point of the filling compound shall be not less than 80° C. The filling compound shall remain stable and remain unaffected by long-term exposure to weather. It shall have chemical and mechanical compatibility with other cable components and splicing hardware. If Gel free cables are used each buffer tube shall contain water blocking material embedded in the inside wall of the buffer tube for water-blocking protection. The water blocking material shall be non-nutritive to fungus, electrically non-conductive, and homogeneous. It shall also be free from dirt or foreign matter. This element will preclude the need for any other water blocking material.
- Neither the inner nor the outer surfaces of the jacket will exhibit visible cracks, splits, tears, or other openings. The jacket shall have constant uniform thickness as well as be smooth and continuous.
- Buffer tubes shall be stranded around the dielectric central member using the reverse oscillation stranding process. Water swell able yarns should be applied longitudinally along the central member

while standing. This arrangement of tubes will allow to takeout any individual tube at any length for splicing.

- Optical fibers shall be placed inside a loose buffer tube. The nominal outer diameter of the buffer tube shall be approx. 2.5 mm. The buffer tube shall be polypropylene and each buffer tube shall contain fibers as required to meet requirement.
- The fibers shall not adhere to the inside of the buffer tube.
- Each buffer tubes containing fibers shall be color coded with distinct and recognizable colors in accordance with TIA/EIA-598-B, "Optical Fiber Cable Color Coding."
- The cable shall meet the requirements of ANSI/ICEA or AS/ACIF Standard for Fiber Optic outside plant communications cable, ANSI/ICEA S-87-640-2006 or AS/ACIF S008; AS/NZS 3080.
- Buffer tube colored stripes shall be inlaid in the tube by means of co-extrusion. The nominal stripe width shall be approx. 1 mm.
- If buffer tubes containing multiple fibers, the colors shall be, stable across the specified storage and operating temperature range and shall not be subject to fading or smearing onto each other. Colors shall not cause fibers to stick together.
- The buffer tubes shall be resistant to external forces and shall meet the buffer tube cold bend and shrink back requirements.
- Fiber cable circular cross section to be symmetric.
- The central member shall consist of a dielectric, glass reinforced plastic (GRP) rod. The central member shall be over-coated with a thermoplastic when required to achieve dimensional sizing to accommodate buffer tubes/fillers.
- Two polyester yarn binders shall be applied contra-helically with sufficient tension to secure each buffer tube layer to the dielectric central member without crushing the buffer tubes. The binders shall be non-hygroscopic, non-wicking, and dielectric with low shrinkage.
- For single layer cables, a water swell able tape shall be applied longitudinally around the outside of the stranded tubes/fillers. The water swell able tape shall be non-nutritive to fungus, electrically non-conductive, and homogenous. It shall also be free from dirt and foreign matter.
- The MDPE jacket material shall be as defined by ASTM D1248, Type II, Class C, Category 4 and Grades J4, E7 and E8.
- The shipping, storage, and operating temperature range of the cable shall be -40 deg C to +80 deg C. The installation temperature range of the cable shall be 0 deg C to +55 deg C.
- In accordance with FOTP-3, "Procedure to Measure Temperature Cycling Effects on Optical Fibers, Optical Cable" the change in attenuation at extreme operational temperatures (-40 deg C and +80 deg C) shall not exceed 0.15 dB/km at 1550 nm for single-mode fiber.
- In accordance with FOTP-82, "Fluid Penetration Test for Fluid-Blocked Fiber Optic Cable," a one-meter length of unaged cable shall withstand a one-meter static head or equivalent continuous pressure of water for one hour without leakage through the open cable end.
- In accordance with FOTP-81, "Compound Flow (Drip) Test for Filled Fiber Optic Cable," the cable shall exhibit no flow (drip or leak) of filling and/or flooding material at 80 deg C.
- In accordance with FOTP-41, "Compressive Loading Resistance of Fiber Optic Cables," the cable shall withstand a minimum compressive load of 220 N/cm applied uniformly over the length of the sample. The change in attenuation shall not exceed 0.15 dB at 1550 nm for single-mode fibers.
- In accordance with FOTP-104, "Fiber Optic Cable Cyclic Flexing Test," the cable shall withstand 25 mechanical flexing cycles around a sheave diameter not greater than 20 times the cable diameter. The change in attenuation shall not exceed 0.15 dB at 1550 nm for single-mode fiber.
- In accordance with FOTP-33, "Fiber Optic Cable Tensile Loading and Bending Test," using a maximum mandrel and sheave diameter of 560 mm, the cable shall withstand a rated tensile load of 2670N and residual load of 30% of the rated installation load. The change in attenuation at residual load and after load removal shall not exceed 0.15 dB at 1550 nm for single mode fiber.
- In accordance with FOTP-37, "Low or High Temperature Bend Test for Fiber Optic Cable," the cable shall withstand four full turns around a mandrel of less than or equal to 20 times the cable diameter

after conditioning for four hours at test temperatures of -30 deg C and +60 deg C. Neither the inner or outer surfaces of the jacket shall exhibit visible cracks, splits, tears, or other openings. The change in attenuation shall not exceed 0.30 dB at 1550 nm for single mode fiber.

- Certificate of conformance to be produced for similar FO cables manufactured by OEM earlier with technical bid to support above listed FOTP. In addition, on supply of the FO cables, OEMs certificate of conformance is required with the product.

Armored fiber cable (for Backbone).

- The core shall be filled with a compound to inhibit water migration and shall be wrapped with a barrier tape. The filling compound shall be homogenous and uniformly mixed. The compound will at least be sufficiently translucent for fiber identification. The filling compound shall not affect the color of the individual fibers, is non-toxic and present no thermal hazards. The drop point of the filling compound shall be not less than 80° C. The filling compound shall remain stable and remain unaffected by long-term exposure to weather. It shall have chemical and mechanical compatibility with other cable components and splicing hardware. If Gel free cables are used, each buffer tube shall contain water blocking material embedded in the inside wall of the buffer tube for water-blocking protection. The water blocking material shall be non-nutritive to fungus, electrically non-conductive, and homogeneous. It shall also be free from dirt or foreign matter. This element will preclude the need for any other water blocking material. Neither the inner or outer surfaces of the jacket will exhibit visible cracks, splits, tears, or other openings. The jacket shall have constant uniform thickness as well as be smooth and continuous.
- Buffer tubes shall be stranded around the dielectric central member using the reverse oscillation stranding process. Water swell able yarns should be applied longitudinally along the central member while standing. This arrangement of tubes will allow to takeout any individual tube at any length for splicing.
- Optical fibers shall be placed inside a loose buffer tube. The nominal outer diameter of the buffer tube shall be approx. 2.5 mm. The buffer tube shall be polypropylene and each buffer tube shall contain fibers as required to meet requirement.
- The fibers shall not adhere to the inside of the buffer tube.
- Each buffer tubes containing fibers shall be color coded with distinct and recognizable colors in accordance with TIA/EIA-598-B, "Optical Fiber Cable Color Coding."
- The cable shall meet the requirements of ANSI/ICEA Standard for Fiber Optic outside plant communications cable, ANSI/ICEA S-87-640-2006.
- Buffer tube colored stripes shall be inlaid in the tube by means of co-extrusion. The nominal stripe width shall be approx. 1 mm.
- If buffer tubes containing multiple fibers, the colors shall be, stable across the specified storage and operating temperature range and shall not be subject to fading or smearing onto each other. Colors shall not cause fibers to stick together.
- The buffer tubes shall be resistant to external forces and shall meet the buffer tube cold bend and shrink back requirements.
- Fiber Cable circular cross section to be symmetric.
- The central member shall consist of a dielectric, glass reinforced plastic (GRP) rod. The central member shall be over-coated with a thermoplastic when required to achieve dimensional sizing to accommodate buffer tubes/fillers.
- Two polyester yarn binders shall be applied contra-helically with sufficient tension to secure each buffer tube layer to the dielectric central member without crushing the buffer tubes. The binders shall be non-hygroscopic, non-wicking, and dielectric with low shrinkage.
- For single layer cables, a water swell able tape shall be applied longitudinally around the outside of the stranded tubes/fillers. The water swell able tape shall be non-nutritive to fungus, electrically non-conductive, and homogenous. It shall also be free from dirt and foreign matter.
- Armored cables without an inner jacket shall have an armor layer applied directly over the water

swell able tape. The armor shall be a corrugated steel tape, plastic-coated on both sides for corrosion resistance and shall be applied around the outside of the water swell able tape and cable core with an overlapping seam with the corrugations in register. The outer jacket shall be applied over the corrugated steel tape armor. The outer jacket shall be a LLDPE (Linear Low density polyethylene) with a minimum nominal jacket thickness of approx. 1.25 mm. The polyethylene shall contain carbon black to provide ultraviolet light protection and shall not promote the growth of fungus.

- The MDPE jacket material shall be as defined by ASTM D1248, Type II, Class C, Category 4 and Grades J4, E7 and E8.
- The shipping, storage, and operating temperature range of the cable shall be -40 deg C to +80 deg C. The installation temperature range of the cable shall be 0 deg C to +55 deg C.
- In accordance with FOTP-3, "Procedure to Measure Temperature Cycling Effects on Optical Fibers, Optical Cable" the change in attenuation at extreme operational temperatures (-40 deg C and +80 deg C) shall not exceed 0.15 dB/km at 1550 nm for single-mode fiber.
- In accordance with FOTP-82, "Fluid Penetration Test for Fluid-Blocked Fiber Optic Cable," a one-meter length of unaged cable shall withstand a one-meter static head or equivalent continuous pressure of water for one hour without leakage through the open cable end.
- In accordance with FOTP-81, "Compound Flow (Drip) Test for Filled Fiber Optic Cable," the cable shall exhibit no flow (drip or leak) of filling and/or flooding material at 80 deg C.
- In accordance with FOTP-41, "Compressive Loading Resistance of Fiber Optic Cables," the cable shall withstand a minimum compressive load of 220 N/cm applied uniformly over the length of the sample. The change in attenuation shall not exceed 0.15 dB at 1550 nm for single-mode fibers.
- In accordance with FOTP-104, "Fiber Optic Cable Cyclic Flexing Test," the cable shall withstand 25 mechanical flexing cycles around a sheave diameter not greater than 20 times the cable diameter. The change in attenuation shall not exceed 0.15 dB at 1550 nm for single-mode fiber.
- In accordance with FOTP-33, "Fiber Optic Cable Tensile Loading and Bending Test," using a maximum mandrel and sheave diameter of 560 mm, the cable shall withstand a rated tensile load of 2670N and residual load of 30% of the rated installation load. The change in attenuation at residual load and after load removal shall not exceed 0.15 dB at 1550 nm for single mode fiber.
- In accordance with FOTP-181, "Lightning Damage Susceptibility Test for Optic Cables with Metallic Components," the cable shall withstand a simulated lightning strike with a peak value of the current pulse equal to 55 kA without loss of fiber continuity.
- In accordance with FOTP-37, "Low or High Temperature Bend Test for Fiber Optic Cable," the cable shall withstand four full turns around a mandrel of less than or equal to 20 times the cable diameter after conditioning for four hours at test temperatures of -30 deg C and +60 deg C. Neither the inner nor the outer surfaces of the jacket shall exhibit visible cracks, splits, tears, or other openings. The change in attenuation shall not exceed 0.30 dB at 1550 nm for single mode fiber.

Certificate of conformance to be produced for similar FO cables manufactured by OEM earlier with technical bid to support above listed FOTP. In addition, on supply of the FO cables, OEMs certificate of conformance is required with the product.

In addition, the cable jacket shall have permanent surface printed (embossed) sequentially numbered length markers at one-meter (1m) intervals along with Year of manufacture, project name, number of fibers, and Drum ID.

The following tests on FO cable to be observed for,

- Outer jacket test;
- Cable bend test;
- Cable impact test;
- Cable compression test;
- Cable twist test;
- Cable flex test;

- Water penetration test.

1. Cable drum lengths

Maximum lengths of cable shall be used to minimize the number of splices. The amount of cable in any drum shall be identified in accordance with routing requirements while minimizing wastage. Four Km drum length for Backbone applications and two Km drum length for access is recommended.

2. Packing and shipping

The reels shall be constructed to prevent damage to the cable during shipping and handling. The cable ends to be sealed. The cable reels shall be plainly marked (embossed) with the length, the cable code and such other information as may be agreed upon (i.e. job number, reel number, etc.). In addition, individual reels shall be identified with their own serial number. Certified summaries of fiber cable factory test measurements to be provided for each cable reel.

Note: For Distribution Network Unarmored fiber optic cables shall be installed whereas for Back bone network Armored cable to be installed (Single mode 9/125 ITU G.652D Bend Insensitive, Multi-Loose Tube, full rodent protection, Outdoor – Corrugated Steel Tape Armor (CST) PE Jacket.)

FO Patch panels

All patch panels offered shall be capable of supporting high and medium capacity splicing as well as multi-fiber Push on (MPO) Connectors for next generation fiber optic applications. Empty space to be provisioned in each OSP fiber termination rack for future growth within or external to the city. The fiber patch panels shall be suitable for cross connect installations for connection to other parts of the city. They shall also be suitable for inter-connect applications for connection directly to equipment. The cable plant should be interconnected to the applications equipment with patch cords to minimize accidental damage to the backbone/other cables.

Connector housing patch panels requirements

1. Housings shall be mountable in an EIA-310 compatible 465mm (19”) rack and should be 4U in size.
2. The unit shall be mounted with a frontal projection.
3. The unit shall not exceed a depth requirement of 19”.
4. The unit shall meet the design requirements of ANSI/TIA/EIA-568 and the plastics flammability requirements of UL 94 V-0.
5. Housings shall be manufactured using corrosion resistant aluminum or equivalent for structural integrity and shall be finished with a reflective silver powder coat for durability.
6. The housing shall include field installable slack management brackets at the front of the housing.
7. The hardware shall provide access to each adapter port with no Interference of adjacent ports. In addition, the accessibility to the connectors shall be tool less.
8. The housings shall have two open-ended slots with strain relief, one on each side for quick and easy outside FO cable (FOC 1A-1D) entry and installation. Cable entry brushes shall cover these slots.
9. The housing shall contain front and rear doors. These doors shall be hinged with a pivot point at the bottom of the housing. The doors shall utilize a sliding latch mechanism to provide easy access when opening and closing.
10. The connector housings shall have a labeling scheme that complies with ANSI/TIA/EIA-606.
11. The cassette requirements should allow for up to 144 fiber splicing with maximum 12-splice cassette capacity.
12. Patch panel Should Support Mid-Span Splicing.
13. Space between two Patch panels to be provided for fiber manager.

Splice wallet

1. The cassette shall meet the following approx. dimensions: 6.4" x 1.4" x 7.9" (LxWxD).
2. The cassette shall provide a means for splicing cables entering at the back of the cassette, while providing LC connectivity at the front of the cassette. The Pigtailed Cassette shall allow the elimination of individual splice trays or separate splice housings, as well as allowing splicing to be done away from the rack housing in a suitable workspace as needed. The modular design shall help in access of fiber in an individual cassette without disturbing the other fibers in the housing.
3. Each cassette shall contain 12 or 24 Single mode pigtail for splicing incoming fiber. The cassette shall offer minimum 2-meter pigtail length for multiple re-splices when required.
4. The cassette shall have at least six finger tabs that allow easy routing of pigtail and incoming fiber and help to contain the fibers inside the cassette.
5. The cassette shall have a removable splice organizer that allows the installation of 12 or 24 single-fiber heat-shrink protective sleeves minimum 40 mm.
6. The cassette shall come with a snap on mechanism that allows the installation of the splice organizer into the cassette.
7. The cassette shall come with a removable transparent top cover. Removal of this transparent top cover shall allow access to the inside of the cassette for splicing, and shall be able to snap the cover back onto the cassette after splicing.
8. The cassette shall have internally opening shuttered LC adapters that allow a single-handed operation. The shutter adapter shall eliminate the need to remove and re-install dust caps. The shutter shall be VFL compatible.

Fiber splice closure

The splice closures shall be re-enterable, corrosive resistant and waterproof splice closures. Splice Closure shall be available with mechanical Clamps, shall be designed for splicing fibers in direct buried applications. Splice closure shall be available in configurations that can accommodate 144F single fiber splices. Splice Closure shall have Modular fiber management system, which helps in increased splicing capability in the field as per requirement.

The fiber optic enclosure should be capable enough to splice 144 fibers and it should be IP67 rated and ergonomically designed. It should consists of Integrated storage basket for uncut or expressed loose tubes, hinged splice trays for access to any splice during and after installation. The splice closure should have flash test provision. The fiber optic dome closure should have enough space for cable bend radius as per international standard and should be ready to install (including splice protectors and heat shrinks for cable entries). It also consists of grounding kit and valve. The 144 fiber optic dome Splice closure should be fully assembled with 24F splice trays and cover, Splice protectors (HS), Cable sealing kit for round port, Cable sealing kits for oval ports.

Cable Assemblies (Patch cords- LC-Duplex Uni-boot - LC-Duplex Uni-boot Connector)

The flame retardant and halogen free fiber patch cord shall be factory-assembled with LC-Duplex uni-boot connectors on both ends. It must be optimized for use with permanent connections in distribution patching, to active equipment, and patch panels of high-speed networks.

Fiber		
Sr. No.	Parameter	Detailed Specifications
1	Fiber Type	Single-mode
2	Fiber Core Diameter	9 µm
3	Fiber category	OS2 Bend insensitive
4	Wavelengths	1310 nm / 1550 nm
5	Maximum Attenuation	0.38 dB/km / 0.25 dB/km
6	Serial 1 Gigabit Ethernet	5000 m
7	Cable cutoff wavelength	1260 nm
8	Standards in Compliance	TIA/EIA 492-CAAB, IEC 60793-2-50 Type B1.3, ITU-T

		G.652D, ISO/IEC 11801 Cat.OS2
	Complies with standards	
9	Server Room Cabling	TIA 942 (EN 50173-5 draft)
10	LSZH	IEC 61034 and EN 50286 (Low smoke, zero halogen)
11	FR	IEC 60332-3-24 and EN 50266-2-4 (flame retardant)
12	NC:	IEC 60754-2 and EN 50267 (non-corrosive)
13	Connectors	TIA/EIA-604-10A
	Cable Characteristics	
14	Fiber Count	2
15	Outer diameter	2 mm
16	Outer Jacket Color	Yellow
17	Outer Jacket Material	LSZH™/FRNC
18	Minimum Bend Radius	10 mm
19	Crush Resistance (reversible):	1000 N/10 cm
20	Tensile strength	150 N
	Connector Type: LC-Duplex	
21	Ferrule	Ceramic
22	Housing	Composite
23	Color Housing	Black
24	Uniboot:	Black
25	Insert loss	Max. 0.15 dB
26	Durability according to FOTP-21	≤ 0.2 dB change for 500 re-matings
27	Min. tensile strength	44N < 0.2dB, (reversible according to TIA/EIA-568-B.3 and FOCIS - TIA/EIA-604-10A)

Method Statement and Test procedure

Fiber optic cable installation procedure

1. Precautions and requirements for Pulling fiber Optic Cable in Conduits

The fiber Optic Cable shall be treated with care. The cable shall not be trampled upon, run over by vehicles, pulled along the ground, over fences, rock or asphalt.

The cable shall be carefully inspected and observed prior to and during pulling work.

Bends of small radius and twists that might damage cable shall be avoided during the pulling operation; cable shall not be bent in a radius less than twenty (20) times the outside diameter of the cable.

Pulling tension during all installation operations shall never be allowed to exceed that limit which has been specified by the cable manufacturer.

All cable ends are to be effectively sealed (waterproof) at all stages of use. Sealing shall be performed immediately after a length of cable has been cut from a drum.

Cable to be installed using cable protection guides and every effort must be made to reduce the possibility of damage to cable.

The cable drum set-up and pay-out shall be done in such a manner as to maintain as large a radius as possible.

A clean plastic sheet or tarpaulin shall be placed under the drum so that should the cable touch the ground it will not pick up pieces of grit or dirt, which could be carried into the duct and damage the cable sheath.

A firm pulling attachment shall be made to the cable end using a cable grip. A swivel connector is to be used to attach the grip to the cabling rope to prevent the twisting of the cable rope, during drawing in, from being

imparted to the cable. Care must be taken to ensure that swivel can rotate freely when under load conditions. A power winch and tackle shall be rigged at the hauling end of the conduit in such a fashion that the pull is imparted to the cabling rope in line with the conduit being used.

The pulling-in is to be done at a slow continuous rate (jerking the cable must be avoided). A form of communication shall be provided between the team at the winch and the team at the cable drum to prevent the cable drum from overrunning when the pull stops.

To assist in the pulling-in of the cable, the cable jacket shall be lubricated using approved lubricant. The tension of the cable shall be monitored and controlled during pulling. In case of mechanical pulling, the tension limit mechanism / recorder shall be calibrated and proven, to the satisfaction of customer.

2. Installation procedure

Physical site survey must be carried out to know the path ready ness from termination point to termination point, as per the Latest IFC drawings.

For any link, once found Ok DIT is to be carried out.

For any particular link \ stretch and actual cable length has to be measured including the buffer lengths required at bends, transitions and splicing/termination points.

Relevant RFI drawings and drum test results along with the required drawings has to prepared and submitted before the cable pulling activity. All the relevant work permits must be obtained.

The cable drum must be properly placed at an appropriate location in agreement with the site in charge over a mobile jack before starting of pulling. All the relevant equipment's like cable pulling Jacket, Plastic sheet for coiling the cable loop, work permit copies, Lubricants etc. is to be readily available at site .

Sufficient skilled work force must be engaged for the fiber cable laying activity and MSI/customer representatives will decide the span of single laying. Relevant slack cable to be left at Splicing/termination and other locations as per instruction of site in charge from Customer.

Once the complete cable pulling for any link is completed all the sub ducts must be sealed with split plugs, vacant ducts to be sealed with end plugs in all MH/HH/Building entries. Proper tagging of cables to be done in the MH / HH /Service area buildings with permanent tags as per ITU-T standards/ Customer approved tagging.

Once the FO cable laying is completed for any link, MSI must submit the Measurement sheet and relevant red line diagram for the same, duly signed by the concerned site in charge. MSI need to maintain the up-to-date cable consumption tracker and cut length tracker.

3. Trenching/cable installation for backbone

Responsibility for the oversight of everything from detailed implementation plans to community relations, ensuring sufficient materials are ordered in a timely manner to safety and environmental concerns to be taken care by MSI before start of the trenching activity. Method statement to be submitted and approved by customer.

Areas where work is to be performed shall be cleared of all trees, shrubs, rubbish, and other objectionable material of any kind. No excavation work shall commence without having a copy of the approved wayleave/s on site.

Cross pits need to be dug at 30 - 50m intervals, particularly at points where the new trench crosses existing services. The cross pits should be at least 150mm deeper and wider than the proposed trench. Cross pits are one of the most effective methods utilized not only for the location of services, but also to determine the position of a trench, relative to other services.

Locating other existing Services is the responsibility of the MSI and Utility Representative can be asked to point out the position of services or by using Cable Locators. Any damage to existing services should be reported immediately to the customer.

Trenches must be excavated to a depth that the crown of the duct has to be 1500 mm of backfill cover, in all soil conditions, except for where hard rock conditions are encountered. Where it is not possible to obtain the specified minimum trench depth, the customer must be consulted. The trench depth in hard rock conditions can be relaxed (i.e. apply for a concession) to a minimum depth of 300mm backfill cover over the uppermost duct. However, this being said it requires protection in the form of a GI/ concrete encased DWC, placed on top of the padding material.

High-density polyethylene (HDPE) duct of 40 mm OD to be placed into the trench, 12 no's of HDPE ducts to be placed at a depth of 1.5 Mt and spacers to be placed at every 3 meters. Duct uncoils to be used to uncoil the ducts. The HDPE ducts to be of 500mts coils.

At Major / Minor road crossings ducts are installed by Boring (HDD/ Mauling) method. If open cut method is used, the HDPE ducts to be placed inside DWC ducts. For culvert crossings existing ducts or service culverts within bridges must be fully used. Not all bridge structures will have the exact same installation configuration and procedures may vary to accommodate specific requirements.

At every 1 KM, concrete chambers to be provided for keeping spare loop or splice closures. As armored cables are used for Backbone, Earthing must be done as per IEC standards. Electronic locaters/route markers to be installed in each of these chambers.

Warning tapes to be laid 300 mm above the top most duct and route markers to be placed at every 200 meters distance. Also, route markers to be provided at both ends of and Major road crossing/bridge /culvert and at places where the trench takes a major deviation for any reason.

Cables in HDPE ducts to be installed by blowing method using an approved Blowing Machine, the cable blowing length to be not less than 1 KM and before blowing DIT for the duct to be done and accepted by customer representative. Once the cable is blown sealing of ducts to be done using appropriate Split / end plugs.

Fiber optic cable splicing

All splices must be fusions splices. Splices shall conform to ANSI/TIA/EIA standards/ international telecom standards. Each spliced fiber will be packaged in a heat shrinkable splice protection sleeve with strength member. The protection sleeve will cover the splice any bare fiber stripped of its coating. The use of RTV or silicone is strictly prohibited.

All the splicing, termination and testing to be carried out with customer approved test equipment's. Splicing activity to be carried out in a dust proof environment by Certified Splicing personnel.

The fiber Optic cable splicer to be certified by Customer. Splicing of fiber optic cables shall be done by arc fusion method using the latest model, fusion splicer as approved by Customer, in compliance with international Telecommunication standards engineering and construction standards.

MSI shall test and record losses of all splices as they (splices) are being done using an Optical Time Domain Reflectometer (OTDR) or an approved attenuation test set. The average splice loss shall be 0.05 dB or less. No single splice shall have a loss greater than 0.10 dB

MSI shall supply all tools and necessary equipment to perform splicing Work and performance acceptance testing.

The fusion splicing equipment to be used by MSI shall be of the highest optical quality to assure uniform, low-loss splices. The splicing equipment shall employ automatic, high-resolution fiber alignment technology based on pre-splice least-loss criteria established by the machine itself. The splice machine(s) shall have a visual monitor by microscope or miniature CRT / LCD viewing screen and shall provide a read-out estimate of the splice loss. The fusion splice machine must have the latest version of software available.

The fiber cleaver(s), provided by MSI shall be of the highest quality to assure uniform, clean, ninety degree (90°) cleaved fiber ends.

TESTING OF FIBER OPTIC CABLES

Prior to installation of the cable, MSI shall as a minimum, perform an Optical Time Domain Reflectometer (OTDR) measurement test on each fiber of each cable reel at a designated warehouse area to confirm that the fiber cable is acceptable for installation. The OTDR shall provide a permanent computer disk record of the test. Results of the test shall be provided to customer upon their completion. The customer / Representative(s) or his designee shall witness these tests. Any cables that are damaged or defective shall be brought to the attention of the customer representative and shall be replaced by MSI at as part of original scope to the customer. MSI may perform other tests at his discretion to verify that cables meet specifications. Test procedures for any such tests shall be submitted to customer for review and approval prior to testing. MSI shall provide certified summaries of factory test results for each cable drum. The first factory test shall include type tests of the cable being provided. Procedures for all factory field and type tests shall be included in the Systems Design.

Testing and inspection of the optical cables shall be performed in accordance with standards /international telecommunication standards. Test procedures for cable receiving / inspection shall be submitted to customer. All procedures shall have to be reviewed and approved in writing by customer.

After cable installation, MSI shall perform a fiber Cable Loss Test (end-to-end) on all fiber optic cables by means of an optical power meter and using an Optical Time Domain Reflectometer (OTDR), for each fiber in the cable, in both directions for any completed link. The OTDR shall provide a permanent computer disk record of the test. ITU-T acceptance test requirements shall be the basis for cable testing and acceptance.

All fibers shall meet acceptance test requirements. End-to-End loss test, the maximum attenuation of each fiber within a cable at wavelength 1550 nm shall be 0.3dB/km and 0.5 dB/km for 1310 nm. Individual splice insertion loss shall be 0.05dB average link splice loss with no single splice loss above 0.1db. Connectors shall have insertion loss of 0.5dB or less. Power meter test (from both ends) has to be carried out for both 1310 and 1550 nm, OTDR traces for each fibers to be submitted customer for approval (both soft and hard copies).

- MSI shall provide all the Test Equipment required to complete the Work in accordance with customer approved Test Plan and Procedures. MSI shall ensure that all the Test Equipment will operate correctly under the all environment and other external conditions of the Work Site.
- MSI shall provide all test equipment required for timely and uninterrupted start-up and performance testing/acceptance and for warranty-period test of the cable systems and related facilities.
- MSI shall provide Customer with written certification that all test equipment used to perform the tests is calibrated in accordance with the manufacturers' recommendation and applicable industry standards prior to the start of the test. Documentation of the fiber optic cable plant (test results)

should follow ANSI/TIA/EIA-606 Administrative Standard for Telecommunications infrastructure of commercial Buildings. This documentation shall include the insertion loss data.

Testing / Acceptance Criteria, Documentation

MSI has to submit the detailed design as per RFP requirement

All materials, equipment, systems, manufacturing or configuration processes, or other items to be provided under the Contract shall be inspected and tested in accordance with the requirements specified in this document and will be subject to approval.

MSI shall be responsible for conducting

1. Prototype Acceptance Tests
2. Factory Acceptance Tests (FAT):
3. Pre-Installation Testing (PIT
4. Installation Acceptance Tests (IAT):
5. Proof of Performance Testing (POP):
6. System Integration Testing (SIT):
7. System Acceptance Tests (SAT):

The test schedule shall be mutually agreed between the MSI and the DICDL or representative of the DICDL

There should be separate teams for Deployment, commissioning and operations. After successful completion of the acceptance test, the network shall be handed over to O&M teams with all the as built drawings and related data.

The MSI shall be responsible to maintain all the site data and user related data. Like as build drawings, ROW permission documents, monthly maintenance manuals etc.

The MSI shall be responsible to maintain the documents like KPI reports, Inventory reports, all HLD and LLD documents.

MSI shall be responsible to provide proofs of all the certifications and standards mentioned in the RFP.

The MSI shall be responsible for the overall management of the city- wide fiber optic network and passive cabling infra inside ABCD complex buildings, Service area buildings, utility buildings and Street light poles etc. Network Infrastructure and enabling infrastructure maintenance services at all site locations for ensuring adherence of SLAs. MSI shall provide the Operations and Maintenance Services for a period of 5 years following the award of the contract. The MSI shall be responsible for following but not limited to:

1. Warranty support
2. Network operations, services and management
3. NMS for SLA and Performance Reporting
4. Alarm Correlation & Root Cause Analysis Capabilities
5. Network faults and performance management
6. Network Performance Reporting
7. Service level Management
8. MIS reporting
9. O&M of physical infra
10. Manpower requirement fulfillment

The MSI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security

requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected MSI. The MSI is responsible for all tools/environment required for testing and sufficient training shall be given to the MS teams. The MSI shall provide a well-prepared documentation for users in the manual, a clear plan for training, education & hands on to the users

MSI shall have an effective Service level management solution having very professional approach in the project implementation and its operations. MSI is expected to match these expectations of the service levels given in the RFP, Any non-adherence to the SLAs would lead to the penalty, to be calculated as per the details given in the RFP.

Proposed ICT duct Bank allocation:

The bottom most 5 ducts on both sides of the road to be reserved for Backbone, utility services and policy/fire station services. The second row of 5 ducts from bottom to be reserved for distribution network and third row of 5 ducts to be reserved for FTTx services and the remaining 15 ducts are reserved for future use as shown below.

Proposed ICT Duct Reservations Drawing

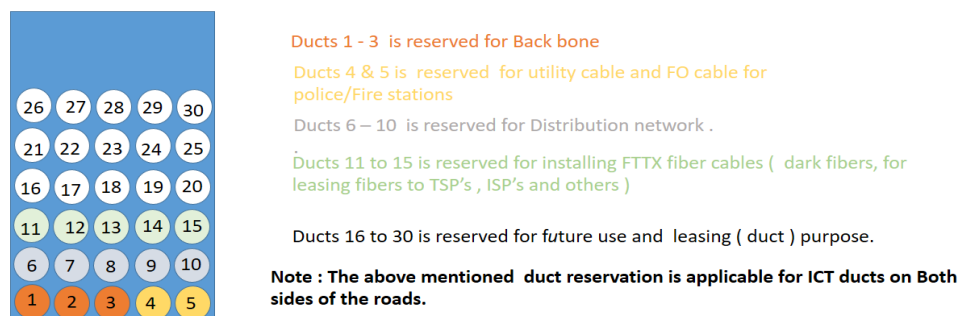


Figure 11 – ICT Ducts Reservation proposal

Project management and Operation Teams

Implementation: MSI shall provide dedicated project management team for passive cabling implementation as a part of Project Management office to be set up during the start of the project. This team as a minimum shall include a designated OSP design expert/solution architect along with CAD drafts men, Site engineers, etc. as required for catering to scope of project with relevant Experience and Qualifications.

The team shall maintain weekly status, minutes of the meetings, weekly / monthly project plans, etc. Meet formally on a weekly basis covering the following agenda items:

- Project Progress
- Delays, if any – Reasons thereof and ways to make-up lost time
- Issues and concerns
- Performance and SLA compliance reports;
- Unresolved and escalated issues;
- Project risks and their proposed mitigation plan
- Discussion on submitted deliverable
- Timelines and anticipated delay in deliverable if any
- Any other issues that either party wishes to add to the agenda.

During the development and implementation phase, there may be a need for more frequent meetings and the agenda would include:

- Target dates for connectivity to prioritized locations specified by customer.
- Scope / design changes in fiber routes due to any field constraint / feasibility issue.
- OSP infrastructure procurement and deployment status
- Any other issues that either party wishes to add to the agenda.

The MSI shall also circulate written progress reports at agreed intervals to customer/customer representative and other stakeholders. Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the customer. customer reserves the right to ask the MSI for the project review reports other than the standard weekly review reports. In addition, the team shall perform following activities but not limited to,

- Supervise ongoing work to ensure that all specifications, standards and quality norms are followed.
- Preparation of ITP (Inspection and Test Plans) reports, splicing reports, LSPM and bidirectional OTDR reports.
- Provide progress reports to Site Manager along with critical field issues and support required.
- Coordinate timely active and passive material delivery at site.
- Coordinate availability of all resources like OFC blowing machine, splicing machine, testing tools, labors, safety/housekeeping team etc. as per requirement.
- Installation and commissioning of all active elements with required specifications.
- Supervise establishment of all major PoP inside existing facilities and any additional set up required in existing NOC and Data Centre etc.
- Handing over the entire customer certified test reports, as build drawings, Acceptance test reports etc. to Operations team after implementation of the network and take sign off from Operations team /Customer. Also the submitted as build drawings to be mapped onto GIS platform.

Operation & Maintenance (O&M)

MSI shall be responsible for carrying out required project work as part of O&M for the period of 5 years. O&M would entail undertaking all activities to ensure uptime of the network as per agreed SLAs defined as per RFP. This shall also apply to the entire supporting infrastructure such passive OFC cabling system of entire city and passive infra inside of buildings like Service areas, Utility buildings, ABCD complex, etc. The O&M shall also cover the maintenance of infrastructure of any additional locations that may be added to OFC

network in future as per customer requirement.

MSI shall be responsible for fulfillment to provide number of ISP pipes and the respective bandwidths at all the required locations as per detailed designing and engineering. Also MSI to provide the required PRIs (from TSPs) for CIOC, police control room, etc. including all types of costs for installation, commissioning, service, operations, etc.

MSI will be responsible for the entire operations and maintenance/upkeep of entire network (including fiber tubes) infrastructure being deployed for various purposes specified in this document

MSI to estimate the exact number of personnel to maintain the SLA requirement mentioned above. MSI shall also work out other resources required for maintenance of the network and get it pre-approved from customer. Resources for Operation and Maintenance of passive network elements would include following but not limited to:

- Field engineers with dedicated FRTs (Field Restoration Team)
- MSI shall use two-wheeler for patrolling and four-wheeler for FRT teams having tools & mobilization of other necessary resources Communication devices to issue reporting and resolution.
- Equipment like splicing machine, OTDR, LSPM, Visual fault locators, Fiber microscope, Fiber optic cleaning kits, red light source, spare cables etc. required for maintenance.
- Material storage locations with adequate capacity in different areas of the city to speed up material delivery during fault to reduce MTTR.
- Spare material including all required elements in adequate quantity to be maintained at all time at all storage locations.
- Field engineers with relevant experience.
- Tools and equipment has to calibrate on regular basis as per standards.

3.1.2. City wide networks - Network Active

Solution Design- Smart city network for all ICT enabled city provided services

DSIR ICT network architecture design needs to factor in important aspects like size of the city, geographical diversity and also e-readiness levels amongst the States. It is proposed to create a reliable, high speed, scalable and secured network to connect geographically distributed nodes across state to provide citizens, government functionaries and private organizations with access any application from anywhere.

Based on the objectives laid out it is essential that a scalable architecture to meet the future bandwidth requirements and traffic needs of the state is created. In order to achieve this, it is necessary that bandwidth patterns are monitored and nodes are made configurable to achieve maximum efficiency.

The Citywide fiber optic network for Activation area, Dholera consists of following elements.

- Back bone Network
- Distribution Network
- Access & Drop connections

A set of central nodes, called the Backbone network, will connect the Server Room in ABCD complex to Primary POP-1, with 144-core fiber cable. The distribution network will have 7 service area's which will be distributed across 2 rings and finally terminating on the back-bone network. One service area building will be hosting Primary POP and will be among the same building which will also act as service area distribution network. The access network will have Power distribution RTU's which will 144F dedicated cable. The utilities like SCADA will have separate 144F cable which will be terminated across service area's and the Govt/Public Building's will also have dedicated 144F cable which will be connected across service area's

Topology should be designed in such a way to provide resiliency, robust connectivity and ensure seamless service delivery. Ring topology would be an ideal solution in such a scenario where each node will have a redundant path. It is proposed to create a physical network between Core/Distribution/access and connect them to their respective hierarchical parents at the Core/Distribution/access. This will ensure that the required vertical connectivity is available even when the direct link between the topological parents is disrupted / broken due to any reasons whatsoever (like fiber cut, nature calamity, etc.).

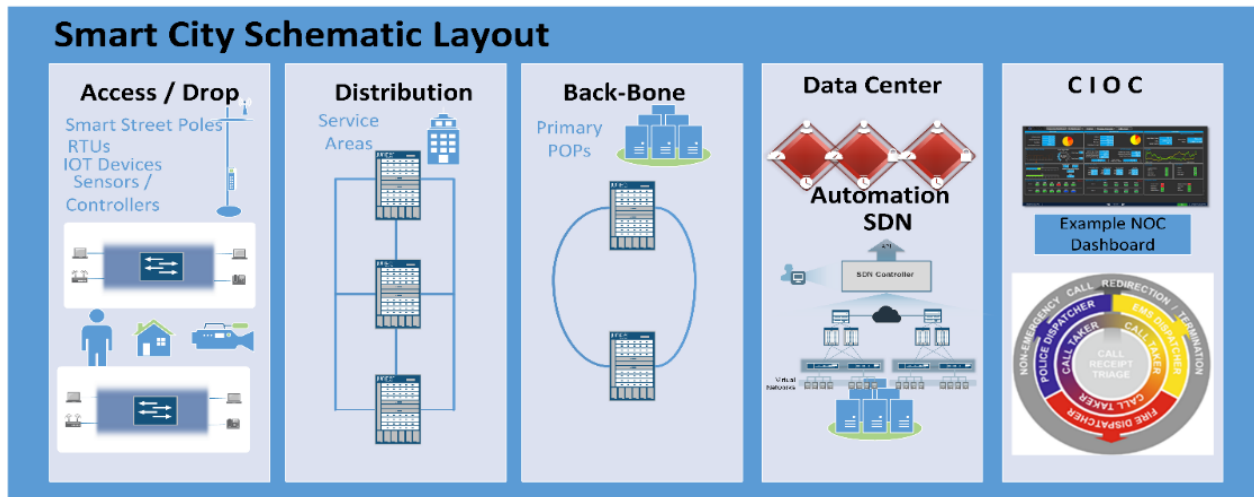


Figure 12 – Smart City schematic layout

Switching and routing

Core functions as a switching network only and do not provide direct access to the end-users. Three Core Nodes are positioned for better and more reliable connectivity and amount of network traffic generated. Gaining efficiency through flatter networks and Converged Super-Core.

Emerging traffic dynamics for a smart city such as sensors, cameras, video, mobility, and cloud-based services are transforming the way networks to operate. Unable to accurately predict shifting traffic patterns and volumes, network operators are forced to over-provision their systems to accommodate peak use periods. One needs to transition to a more agile, intelligent and responsive infrastructure that leads to enabling and delivering new, customizable services.

The data center would be hosted in Government owned Private/ Public Cloud at GSDC, Gandhinagar and Server room would be hosted in ABCD complex at Dholera, Gujarat. Data center will host all the smart city applications except Surveillance, etc. will be hosted in Server Room.

Primary POP will be in service area no 25 as distribution building. Service areas building will host distribution devices and devices meant for the Primary POP.

Fiber Optic Cable Schedule for Cluster A1

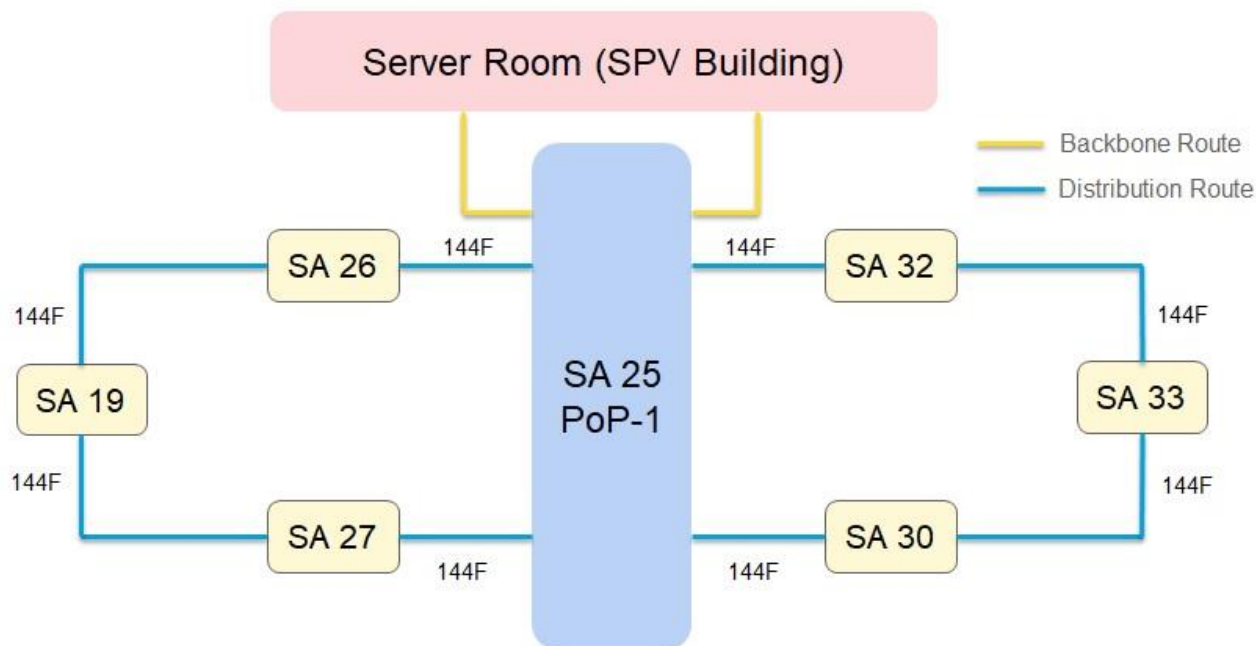


Figure 13 - FOC schedule for Cluster A-1

The Access network covering the services like Wi-Fi / RTU / Transportation / Public Buildings etc.

At access layer there would be a fiber optical cable ring covering 8 smart poles. On smart poles there would be industrial Ethernet switch with two 1G uplinks. This industrial Ethernet switch will provide the connectivity to the CCTV and uplinks from this switch would go to services areas building and terminate on the distribution switch.

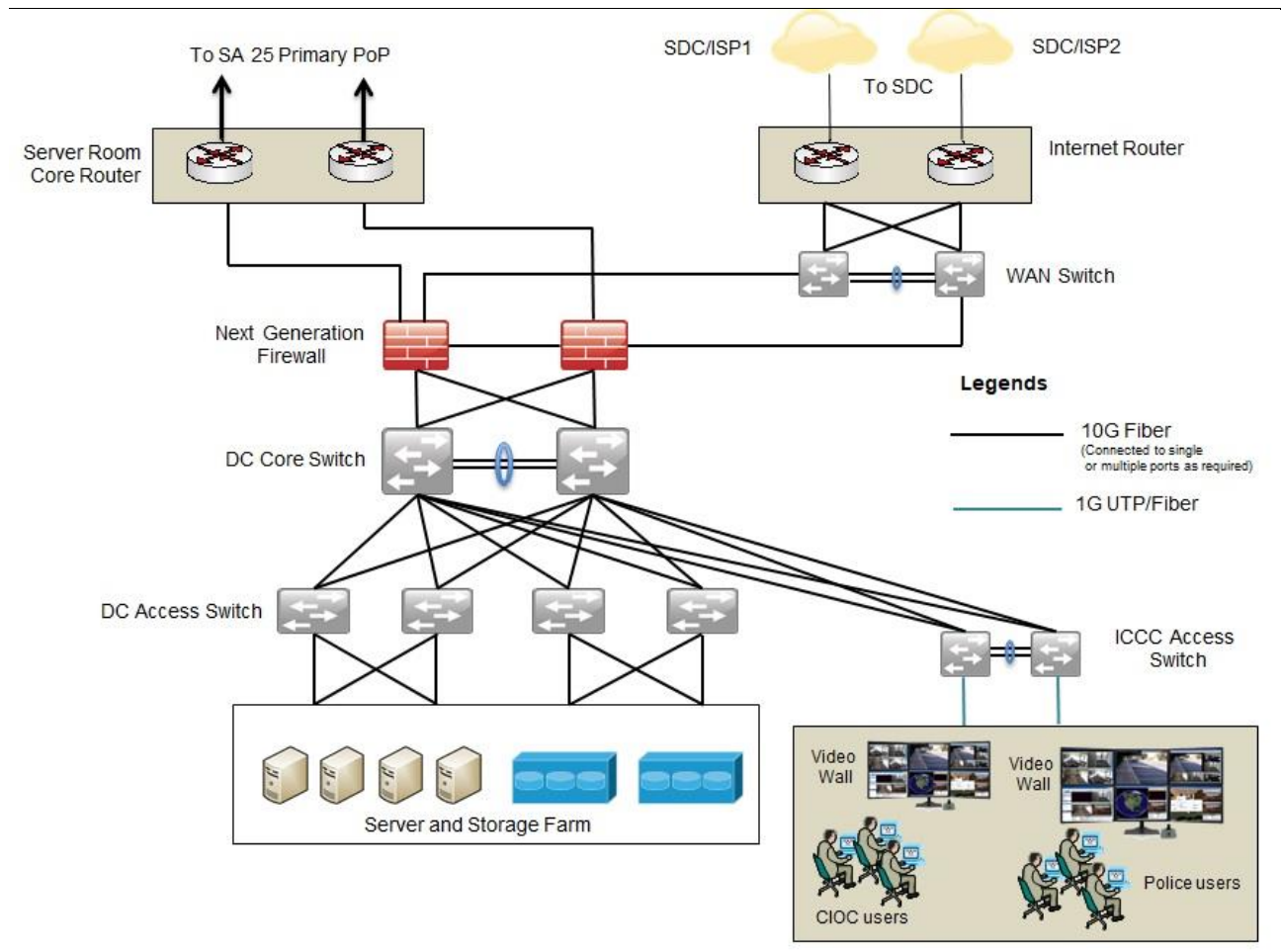


Figure 14 – Server Room (SPV Building) Network Architecture

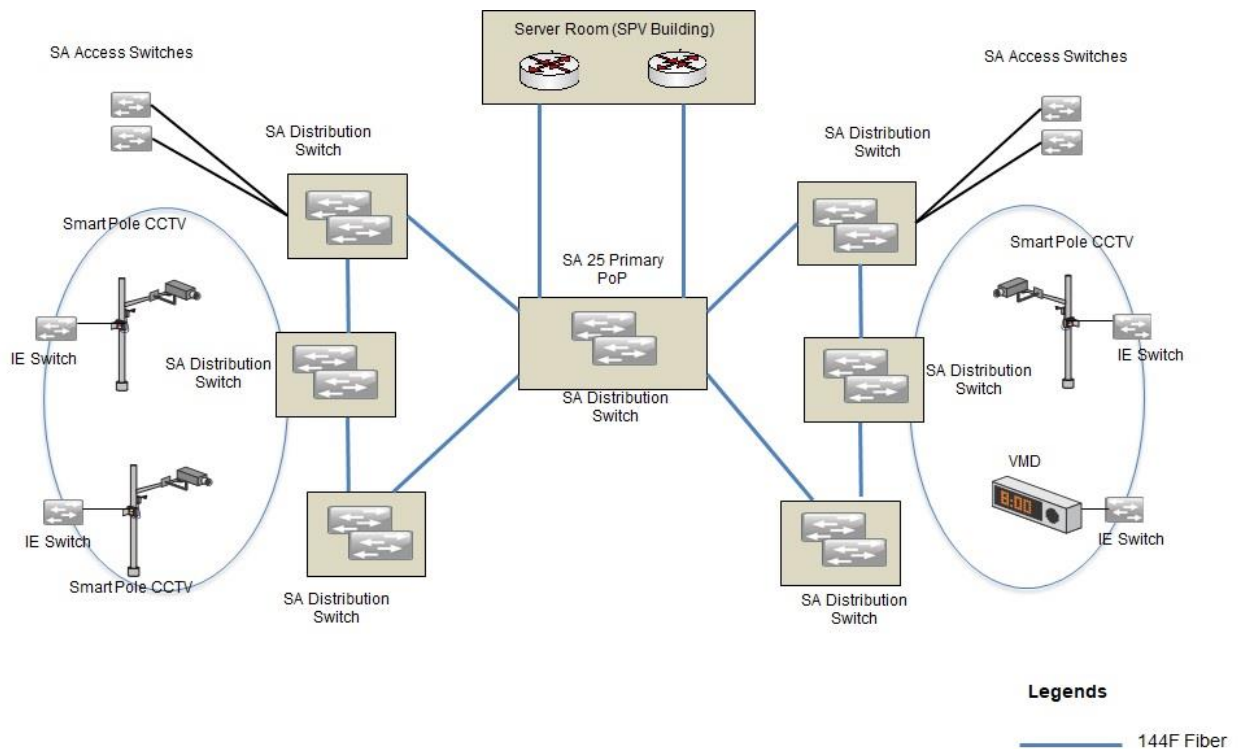


Figure – 15 City Wide Area Network and Integration Points

ABCD Complexes

Purposed network architecture for the ABCD complex is a two-tier architecture. Network designed is highly scalable, modular, simple, meant to be for the bandwidth intensive users and devices. All the access layers would reside on the individual floors; connect to the core with high throughput 10G backbone. For redundancy, there would be two 10G uplinks from each and every floor access layer to core switches, providing high throughput and redundancy as well.

Scope of Work

MSI has to conduct detailed site survey to confirm the site readiness for each and every hub room / location and prepare a comprehensive BoQ accordingly. MSI has to check if everything is in place for the installation of active devices. The details will be captured in pre agreed Survey report format. MSI shall have to take all required approvals from respective authorities.

MSI shall submit detailed architecture of the network. All the equipment shall comply with the specifications given in RFP. MSI shall have to prepare and submit High-level network architecture, Low level Network architecture, detailed implementation plan. High-level design, Low-level design and network implementation plan has to be submitted for each and every network type separately.

Functional, technical and non-functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NET-1.1	Network Active	City wide Network	General	The document outlines architecture and components of the network that shall be deployed by the MSI for the provision of State-wide next Generation network specifically for smart city. The MSI is to integrate all hardware, software and equipment procured as part of this tender and provide a fully functional and operational network for DSIR.
NET-1.2	Network Active	City wide Network	General	The solution should be offered based upon the state of the art and cutting edge technology which should provide State an edge for delivering the current and future services in the most efficient way. The proposed design should be aligned with the emerging service delivery models and should be able to deliver all the next gen services as and when they evolve.
NET-1.3	Network Active	City wide Network	General	All the proposed equipment's should be carrier class and capable of providing 99.74% uptime.
NET-1.4	Network Active	City wide Network	General	The network should be implemented with standard based protocols.
NET-1.5	Network Active	City wide Network	General	The network equipment's should perform as per the performance parameters mentioned in the RFP for IPv4 and IPv6 both.
NET-1.6	Network Active	City wide Network	General	All the network equipment should be IPv4 and IPv6 fully capable and should fully support IPv4 and IPv6.
NET-1.7	Network Active	City wide Network	General	The Operating System should be modular. The processes should run in parallel and failure of one process should not affect other processes.
NET-1.8	Network Active	City wide Network	General	The equipment's deployed in the network shall have wire speed, non-blocking and line rate for all present and future interfaces for 64 byte packet.
NET-1.9	Network Active	City wide Network	General	High Availability features like node protection, path protection, link protection, and critical components should be in redundant mode.
NET-1.10	Network Active	City wide Network	General	The proposed network should provide flexibility with subsequent enhancement to traffic engineering, resource reservation, dynamic provisioning, differentiated services and network resiliency.
NET-1.11	Network Active	City wide Network	General	The proposed network solution should provide very high degree of service scalability with millions of connections.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NET-1.12	Network Active	City wide Network	General	Network should provide sub 50 ms of recovery and re convergence at all levels. Should able to support thousands of VPN's for different services with traffic engineering defined.
NET-1.13	Network Active	City wide Network	General	The network should have the capability to grow and expand using open-ended software/hardware. The network must be scalable and should cater for at least 100% expansion by adding additional nodes/routers. The network scalability should also support expansion in number of users for Voice, video, data or any modern day application by a factor of 100%.
NET-1.14	Network Active	City wide Network	General	A single point failure on the equipment should not result in network or network management system downtime. All critical modules will be identified by the MSI and provided in full redundant configuration for high reliability.
NET-1.15	Network Active	City wide Network	General	The system hardware/software should not pose any problem, due to changes in date and time caused by events such as changeover of millennium/ century, leap year in the normal functioning of the system.
NET-1.16	Network Active	City wide Network	General	The network equipment should support online management through MSI Supplied Network Management System for centralized configuration, performance monitoring, fault diagnostics and rectifications.
NET-1.17	Network Active	City wide Network	General	The network should be capable enough to carry voice, video data, or any modern day application from end to end with quality and reliability degradation.
NET-1.18	Network Active	City wide Network	General	The processes, architecture, design approaches should be adaptable, permit timely cost-effective introduction of new technologies, including the reconfiguration of the networks and capabilities. The design of the network should allow a new service to be configured while ensuring that the performance of existing services and subscribers are not affected i.e. ensure predictable performance for services at all times.
NET-1.19	Network Active	City wide Network	General	The network elements or nodes must be able to provide a reliable QoS for all applications that are transported across the network infrastructure end to end.
NET-1.20	Network Active	City wide Network	General	The success of operations in a network would largely depend on the methodology that is followed to create the design and the translation of this robust design into operational model. Towards this end, this tender requires that the professional services from the respective OEMs would have to be engaged in implementation and the management of the project.
NET-1.21	Network Active	City wide Network	General	The MSI will ensure configuration of the equipment so as to achieve the overall system reliability as stated above.
NET-1.22	Network Active	City wide Network	General	The MSI will ensure planning and placement of spares for all equipment so as to achieve the required up time of the network.
NET-1.23	Network Active	City wide Network	Security	The Solution must support identification and control of all types of applications (Business, Social, Encrypted and Custom) within the Network environment without requiring any license/subscription/blade. It should provide detailed analysis on sessions consumed, data transferred and threats involved through the applications.
NET-1.24	Network Active	City wide Network	Security	The proposed solution must allow free custom application signatures for Homegrown and custom applications (both current and future) that are running in the network.
NET-1.25	Network Active	City wide Network	Security	The solution must provide real time traffic logs based on applications irrespective of ports. While monitoring real time traffic logs, solution must provide detailed view of Defense Services application and Users, not just ports and IP addresses. E.g. the solution must distinguish between telnet on port 80 and http traffic between same pair of source and destinations.
NET-1.27	Network Active	City wide Network	Security	Solution must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must not use proprietary ASIC chips.
NET-1.28	Network Active	City wide Network	Security	Solution must support Full tunnel, split tunnel and application specific tunnel for client to site VPNs. Solution must allow custom policies to control VPN traffic based on users, applications. It must allow different policies for different users groups for threat (Viruses, vulnerabilities, malware) within VPN traffic.
NET-1.29	Network Active	City wide Network	Security	Security is the primary consideration in ensuring stable and secure operation for smart city network. Threats such as worms, viruses, denial-of-service (DoS) attacks and other malicious activities must not degrade the network or service stability.
NET-1.30	Network Active	City wide Network	Security	Network element security should Provide strong security starts at the node level. Every network element must provide sufficient protection of its own resources and services.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NET-1.31	Network Active	City wide Network	Security	Network and IP spoofing protection includes blocking access to internally used subnets, IP spoofing protection and blocking, DoS protection and tracking and more. IP spoofing- using both registered and unregistered address space- is the most common transport vehicle for malicious activities.
NET-1.32	Network Active	City wide Network	Security	Protected control-plane operation is imperative to ensure stable operation of the entire network. This protection includes both internal and external protection policies, because attacks originate from both ends. Service protection-Enabling service-specific security policies to provide effective threat mitigation strategy. Access to nodes or segments that are service-specific should be controlled from the rest of the network; to achieve a high degree of protection.
NET-1.33	Network Active	City wide Network	Core and Distribution network	DSIR network should be able to deliver the following network based services but not limited to, anywhere on all ports of all core & distribution routers - IPv4 and IPv6 transport, MPLS Layer 3 VPN (Intranet, Extranet), Layer 2 VPN Point-to-point, Layer 2 VPN Point-to-multipoint, Layer 2 VPN multipoint, Carrier Ethernet Services (E-LINE, E-LAN, E-TREE), 6PE/6VPE, Multicast VPN, IP Multicast like PIM SM, PIM SSM, MSDP routing, Inter-AS MPLS L3 VPN, Inter-AS L2VPN, MPLS Carrier Supporting Carrier, Data center interconnection and 3 level H-QoS (per-subscriber, per-application QoS) for all subscribers. The proposed network architecture shall allow provisioning of all these services on any port of all core and distribution routers while the core performs high speed IP/MPLS interconnection and switching. The core and distribution router shall provide IEEE 802.ah, 802.1ag. The access network should be able to deliver Carrier Ethernet Services E-LINE, E-TREE, E-LAN within a city, region and across the city amongst multiple locations.
NET-1.34	Network Active	City wide Network	Core and Distribution network	The routers would be configured to provide the defined IP/MPLS QoS support. The network should provide MPLS Traffic Engineering, path protection and node protection features for Access node originated traffics. The core network must provide MPLS fast reroute features for traffic engineering LSP/Tunnels. The network must not take more than 50ms for traffic reroute for a six hop network.
NET-1.35	Network Active	City wide Network	Core and Distribution network	The meaning of "Slot" for of any routers and wherever it appears in this tender document means a main slot (full slot) on the router chassis. Only a main slot on the router chassis shall be counted to fulfil any tender requirements for number of free slots (no sub-slot or daughter slot shall be considered as "Slot")
NET-1.36	Network Active	City wide Network	Core and Distribution network	Should provide 99.74% uptime for working on 24hrs x 365 day's basis. All critical modules/cards such as control cards and power supply cards of Core Network will have 100% redundancy.
NET-1.37	Network Active	City wide Network	Core and Distribution network	The network should support deep packet inspection capabilities to provide clean traffic to the core network.
NET-1.38	Network Active	City wide Network	Core and Distribution network	The network should have multicast capabilities with all the resiliency , traffic engineering parameters defined for the network
NET-1.39	Network Active	City wide Network	Core and Distribution network	The next generation network will be providing bandwidth, connectivity to other existing networks. The next generation network should have capabilities to logically partition/virtualize for existing and proposed separate physical networks.
NET-1.40	Network Active	City wide Network	Core and Distribution network	The network will have real-time and non-real-time services provisioned.
NET-1.41	Network Active	City wide Network	Core and Distribution network	The network should provide services like Intranet, Internet, sensors, Wi-Fi, surveillance, Voice, Video, Multimedia, data applications, conferencing features for both voice and video, VOD, distant learning, e-medicine, IP-TV and any future applications that will be deployed by State.
NET-1.42	Network Active	City wide Network	Core and Distribution network	It should be possible to configure point-to-point, point to multipoint and any to any connection configurations to cater for different user defined network deployment options that can be optimized for different services and application requirement.
NET-1.43	Network Active	City wide Network	Core and Distribution network	End-to-end CoS & QoS, H-QoS capability in order for State to provide differentiated granularity to services like VoIP, Video, and other multimedia and data applications on per port per subscriber per service.
NET-1.44	Network Active	City wide Network	Core and Distribution network	The proposed network should support Traffic engineering and bandwidth guarantee.
NET-1.45	Network Active	City wide Network	Core and Distribution network	The network should have hierarchical management capabilities as mentioned in the RFP.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NET-1.46	Network Active	City wide Network	Core and Distribution network	End-to-end Service Provisioning, Service Assurance and diagnostics platform to manage the network and service.
NET-1.47	Network Active	City wide Network	Core and Distribution network	The network must be able to grow and scale 100% with respect to control-plane and forwarding plane capabilities. The Core routers should be 100G ready.
NET-1.48	Network Active	City wide Network	Core and Distribution network	The Control Plane protection Mechanism like DoS protection, DDoS protection to be supported.
NET-1.49	Network Active	City wide Network	Core and Distribution network	The proposed network should be robust architecture designed with products complying with the IETF / IEEE / ITU standards
NET-1.50	Network Active	City wide Network	Core and Distribution network	The proposed equipment should be NEBS certified.
NET-1.51	Network Active	City wide Network	Access Network	All the industrial Ethernet switches mentioned should have operating temperature minimum -40°C to 80°C without FAN.
NET-1.52	Network Active	City wide Network	Access Network	All the industrial Ethernet switches mentioned should support POE+ IEEE 802.3at interfaces.
NET-1.53	Network Active	City wide Network	DC & DR	The document outlines architecture and components of the Data Centre network that shall be deployed for the provision of next Generation network specifically for DSIR.
NET-1.54	Network Active	City wide Network	DC & DR	The solution purposed based upon the state of the art and cutting-edge technology which would provide an edge for delivering the current and future services in the most efficient way.
NET-1.55	Network Active	City wide Network	DC & DR	The proposed solution aligned with the emerging service delivery models and will be able to deliver all the next gen services as and when they evolve.

Testing / Acceptance Criteria

All materials, equipment, systems, manufacturing or configuration processes, or other items to be provided under the Contract shall be inspected and tested in accordance with the requirements specified in this document and will be subject to approval.

MSI Shall be responsible for conducting;

1. Prototype Acceptance Tests
2. Factory Acceptance Tests (FAT)
3. Pre-Installation Testing (PIT)
4. Installation Acceptance Tests (IAT):
5. Proof of Performance Testing (POP)
6. System Integration Testing (SIT)
7. System Acceptance Tests (SAT)

The test schedule shall be mutually agreed between the MSI and the DICDL or representative of the DICDL. The MSI shall arrange for environments and tools for testing and for training as envisaged. MSI has to do all necessary testing with the help of testers and demonstrate the same. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected MSI. The MSI is responsible for all tools/environment required for testing and sufficient training shall be given to DICDL team. MSI shall provide a well-prepared documentation for users in the manual, a clear plan for training, education & hands On to the users. All the trainings have to be conducted as per the agreement.

Commissioning

There should be separate teams for Deployment, commissioning services. After successful completion of the acceptance testing the network will be handed over to O&M teams. With all the as built drawings and related data.

MSI shall be responsible to maintain all the Site data and user related data. The users activity logs shall be maintained for at least 3 months, the MSI shall be responsible for Logs related to security devices and related to authorization and accounting activities has to be maintain for 1 year or as per the agreement.

The MSI shall be responsible to maintain the documents like KPI reports, Inventory reports, HLD, LLD, transition documents, AT reports as built for each and every component of network.

MSI shall be responsible to provide proofs of all the certifications and standards mentioned in the RFP.

The MSI shall be responsible for the overall management of the Network Infrastructure and enabling infrastructure maintenance services / facility management services at all Site locations for ensuring adherence of SLAs.

Operation and Maintenance

MSI shall provide the Operations and Maintenance Services for a period of 5 years post Go-Live. The MSI shall be responsible for following but not limited to:

1. Warranty support
2. Network operations, services and management
3. NMS for SLA and Performance Reporting
4. Alarm Correlation & Root Cause Analysis Capabilities
5. Network faults and performance management
6. Network Performance Reporting
7. Service level Management
8. Dashboard reporting
9. MIS reporting
10. Database management and administration services
11. O&M of physical infra
12. Manpower requirement fulfillment

The MSI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected MSI.

MSI shall provide a well-prepared documentation for users in the manual, a clear plan for training, education & hands on to the users. All the trainings have to be conducts as per the agreement.

MSI shall have an effecting Service level management solution having very professional approach in the project implementation and its operations. MSI is expected to match these expectations of the service levels given in the RFP, Any non-adherence to the SLAs would lead to the penalty, to be calculated as per the details given in the RFP.

3.1.3. City wide sensors (e.g. sensors network for utilities)

Scope of work and Solution Design

All kinds of sensor locations will be proposed by MSI however ICT consultant/DICDL will approve them and will have the right to change the locations within the city at no cost to DICDL.

Weather, Environmental and water level sensors are part of 'Cluster-A1'. All the sensors within Cluster A1 area will be connected to the city wide fiber. A separate tube has been dedicated for sensors. All the termination equipment for both ends of fiber must be supplied, erected and commissioned by the MSI. The equipment must ensure that there happens no security breach and in this regard any additional devices as needed must be provided and commissioned by MSI.

MSI will also provision display of all the signals captured from all kinds of sensors for display in various dashboards, CIOC, portal and other applications, etc.

All the power sourcing equipment (end to end from cables to MCBs to panels etc.) for all the sensors is in the scope of MSI.

MSI shall be responsible for carrying out all the civil, mechanical, electrical works required for setting up all the field components of the system including:

- a) Preparation of concrete foundation for MS-Poles & cantilevers
- b) Laying of GI Pipes complete with GI fitting (GI pipe to be considered as per IS 1239 standard)
- c) Hard soil deep digging and backfilling after cabling
- d) Soft soil deep digging and backfilling after cabling
- e) Chambers with metal cover at every junction box, pole and at road crossings
- f) Concrete foundation from the Ground for outdoor racks

MSI shall carry out all the electrical work required for powering all the components of the system.

Electrical installation and wiring shall conform to the electrical codes of India.

MSI shall make provisions for providing electricity to the field devices via JB (Junction Box), housing the UPS/SMPS power supply, with minimum backup as defined in this RFP.

Registration of electrical connections at all field sites shall be done in the name of DICDL as agreed and finalized in the contract agreement.

Though not specified all sensors will be provided with end-to-end equipment from sensing to writing into database and displaying onto dashboards, etc. would be part of MSI's scope of work. The sensors must be connected in the secured way so that the malicious attacks such as DDoS, etc. from sensors end cannot take place. This should also include binding of sensors, MAC address on to upstream switch and other measures as required.

Earthing and Lightning Proof Measures

1. MSI shall comply with the technical specifications taking into account lightning-proof and anti-interference measures for system structure, equipment type selection, equipment earthing, lightning arrester, power and signal cable laying. MSI shall describe the planned lightning-proof and anti-interference measures in their technical bid.
2. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables.
3. All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS chip due to the surge suppression.

4. Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards.
5. The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized.

There are different types of systems that need to be in place for city wide sensors:

Environmental Monitoring System:

Environmental parameters, specifically air and noise pollution, are a major concern for the citizens and administrators of any city. As DSIR aspires to also be an environmentally sustainable smart city, integrated environmental monitoring stations comprising of various sensors shall be implemented at Dholera. The business requirements of environmental monitoring system is given below:

Integrated ambient air and noise pollution monitoring stations comprising of various environmental sensors shall be implemented in Dholera for monitoring and trending of various ambient air and noise parameters.

Environment monitoring shall be done for tracking that the pollution and noise levels are within the acceptable limits.

Display of parameters to citizens to create awareness and support 'open data' initiatives.

Establish frameworks for regulating these parameters in terms of any supporting initiatives for maintaining acceptable levels.

Central monitoring at CIOC, city application, website and digital display screen in an integrated manner.

The Environmental monitoring system installations shall be provided on streetlight poles or dedicated tripod stands; A Digital Display Screen (DDS) shall also be installed at strategic locations across the City to display environmental parameters to the public.

Environmental Monitoring sensor will be deployed at various locations across the cluster A1. The final locations will be confirmed by the DICDL.

Field Devices – Sensors

Different type of sensors will be deployed in DSIR to monitor certain places in real time for early warning purpose. The data received from sensors will be analyzed to understand the level, frequency of the warning.

Following Sensors will have to be deployed in DSIR:

Gas Sensor:

Gas Sensors will be deployed for sensing the air quality majorly in the Industrial Zones of DSIR. The sensor sends signals to the control center at continuous time intervals. The transmitted data can be analyzed on the monitor in control center. The gas sensor shall cover an area of at least 500 Mtr in diameter at normal wind speed.

The Gas Sensing System shall conduct measurement of various gaseous parameters but not limited to like CO₂ / CO / SO₂ / NO₂ / NO / O₃ / H₂S / NH₃ / CH₄ / VOC / PM 2.5 / PM 10 / HCL etc.

Gas Level sensor will be deployed at following locations. The final locations will be confirmed by the DICDL.

Gas Level		
Sr. No.	Device Locations	Quantity

1	In Industrial area at location around roads	1

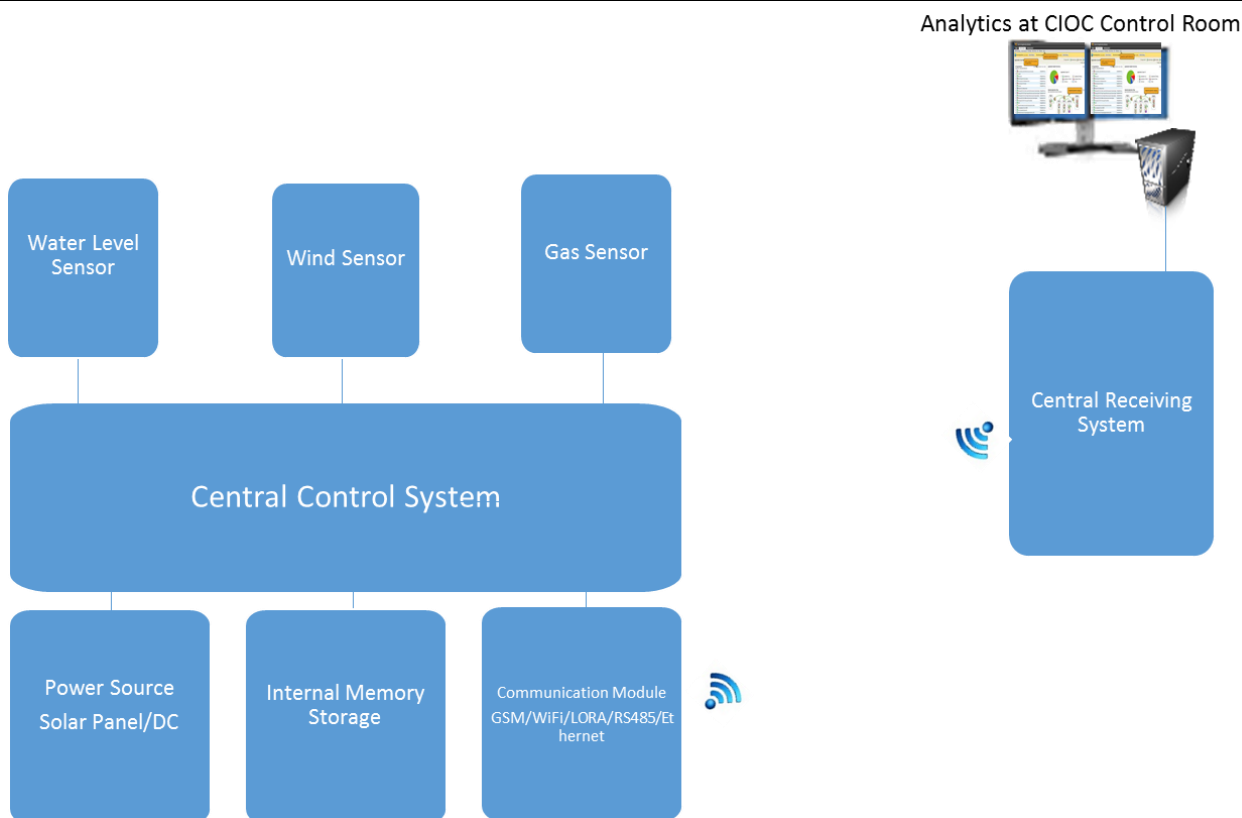


Figure 16 - Logical diagram for early warning sensors

Functional, Technical and Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
SEN-EW 1.0	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must be able to detect the quantity of industrious gas in the air.
SEN-EW 1.1	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must be able to record the data locally in the device and send continuous real time information in defined time intervals on the level of water to central receiving unit.
SEN-EW 1.2	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must have solar panels in order to generate the power required for its functioning and backup for minimum 72 hours.
SEN-EW 1.3	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must have network connectivity like Wi-Fi, GSM, Ethernet
SEN-EW 1.4	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System outdoor unit must be housed in IP-67 enclosure
SEN-EW 1.5	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must raise alarm and alert on the monitoring screen at the time when the gas level is at set alarming level
SEN-EW 1.6	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must be able to generate reports when required.
SEN-EW 1.7	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must have a Mobile Application for smart phone, devices.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
SEN-EW 1.8	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must have Theft Alarm
SEN-EW 1.9	Emergency & Disaster Management	SEN-Early Warning	Gas Sensor	System must be able to integrate with third party application deployed for Emergency and Disaster Management like Computer Aided Dispatch, GIS etc.

3.1.4. City Integrated Operations Platform

High-level Reference Architecture

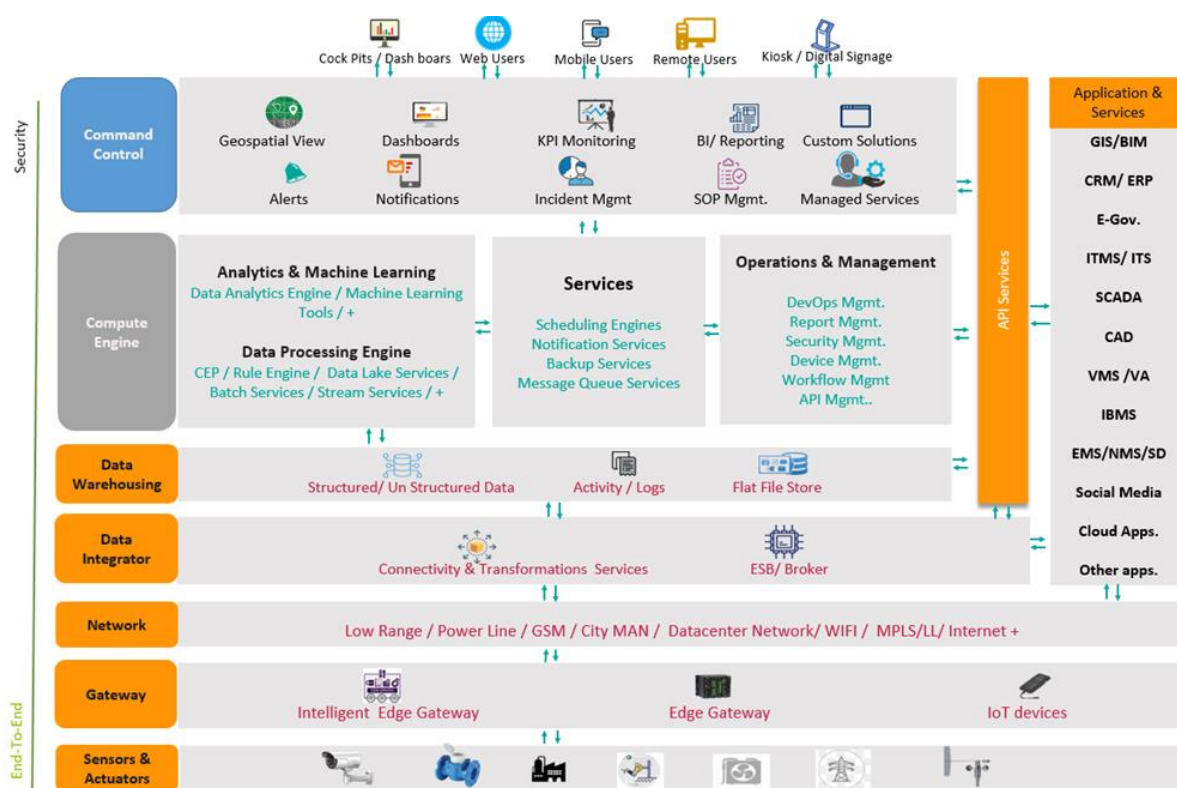


Figure - 17: Architectural Overview of City Integrated Operations Platform

The need of City Integrated Operations Platform reference architecture (RA) should provide a guidance to build custom applications or integrate COTS applications to monitor and analyze all city level operations using a standard framework for CIOC. RA and its layers should give a bird's eye view of the whole underlying platform system. Architecture should be designed in a way that allows changes without damaging the integrity of the system, which can evolve in controllable way.

The architecture should be designed for future needs and growth of City level operations in DSIR. Architecture for City integrated operations platform explains respectively what the layered framework does, how components interact with each other, the generation and flow of information, and the necessary mechanisms must address concerns about integrating applications and solutions which are deployed or to-be deployed in DSIR.

Architecture should abstract the flow of information from solutions and services to the platform for the purpose of analysis, control, and business process integration about city level operations in DSIR. Architecture should aim to be neutral with regard to particular industries and use-case scenarios for integrating new or existing systems. Architecture must provide flexibility for composability and extensibility to allow for a variety of technology choices driven by the specific solution requirements

The Architecture should compose of core platform layers and components to facilitate the processing needs across four major areas,

- Application Integration
- Data Integrations
- Data processing, analytics, and management
- Presentation and business connectivity

Architecture of a CIOP should describe the scope of the innovations expected from the Dholera project and the way they are integrated together in a coherent conceptual system

Architecture should address a new concept and a new model, which applies the new generation of information technologies, such as the internet of things, hybrid computing, Blockchain, Big data, Geographical information System integration, etc. to facilitate the planning, construction, management and smart services of DSIR.

Architecture could be used by Dholera Smart city stakeholders and other interested parties when engaged in technical discussions about smart city services

Architecture should support the city authorities, businesses and the citizens need to address a few fundamental challenges:

- To integrate large number of heterogeneous and distributed information across the systems and services
- Capturing real-time status of the city
- Generate city related information through social media

Layers of the reference architecture

Sensors and Actuators

Sensors, actuators and motes are expected to be deployed across DSIR to sense environment and control the operations on assets.

Sensors should measure/sense the ambient city condition such as

- Monitoring the traffic status,
- Environmental and pollution status,
- Machineries or assets operational status.
- People health status
- Building health condition

Actuators should control/manage the operational conditions of assets / machines such as

- Turn on / off Street lights
- Controlling Traffic signals
- Controlling values on utility pipelines remotely

Motes, are tiny devices / low power computers where it should manage sensors and actuators which are connected to it, whereas this device can transfer the data to the external world through radio links. Motes are typically used as

- Embedded in bridges, to monitor the structural health status
- Monitors condition of machineries

Network Layer

This layer should bridge communication infrastructure for Dholera through the high-capacity, high-bandwidth and high reliable optical networks and wireless network

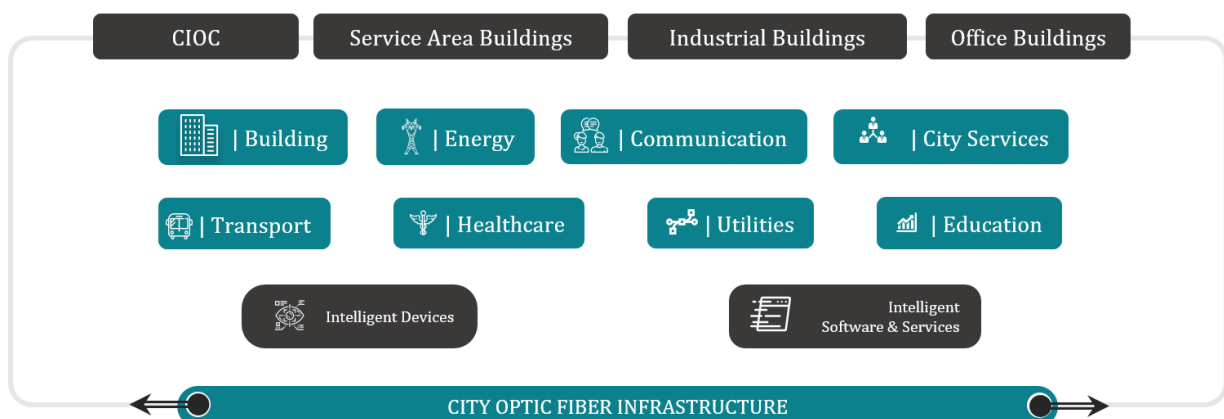


Figure-18 Network layer of City Integrated Operations Platform

Notes

Last mile connectivity:

Connects sensors, actuators, devices, control systems, and assets, which are collectively called edge nodes, whereas Dholera completely runs on captive fiber optic network, Sub Giga hertz frequency network can be used at later stage as option for meter data services. Usually Low frequency RF networks are more constrained by antenna distance (and sometimes battery life).

GSM/CDMA/LTE connectivity:

Provide connectivity for data and control flows between the endpoint IoT devices and the cloud based IoT applications. They may be private networks over the public Internet, 4G/5G mobile networks, or even satellite networks.

Data Integration Layer

DSIR includes various data formats using a wide variety of intelligent objects embedded throughout the city. CIOF should facilitate in integrating such a large amount of data from multiple sources; data integration within the CIOF is one of the important challenges. CIOF platform should facilitate to bring

the Data quality while any data integration mechanism, especially if the data are incorrect, missing, use the wrong format, and/or are incomplete.

Data Integration Layer would be data exchange layer between the Platform, Edge Devices, various COTS and other applications.

ESB - communications between mutually interacting Enterprise software applications including ERP, E-Gov, COTS, non-COTS applications, Surveillance, SCADA applications, etc.

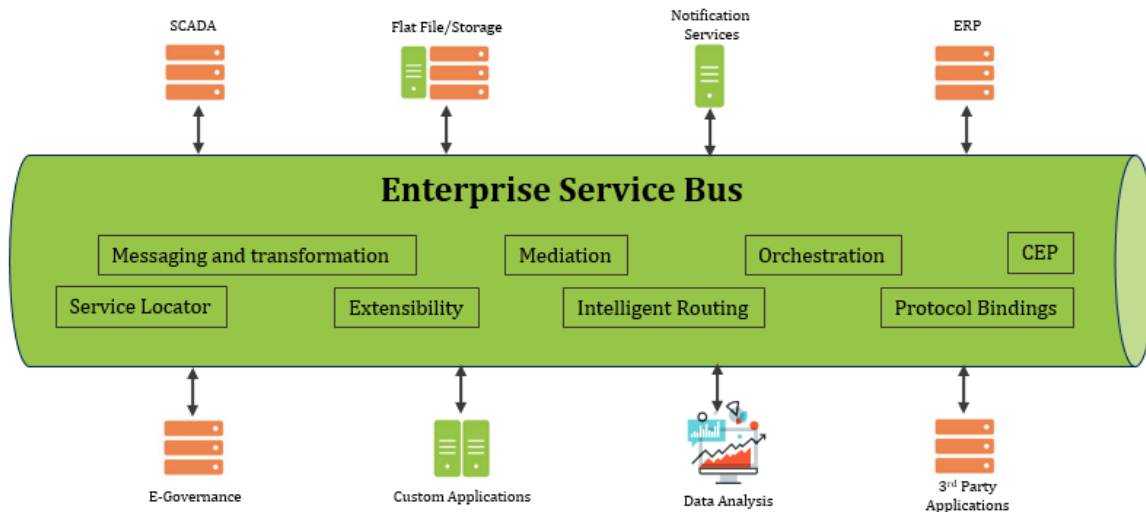


Figure – 19 Enterprise Service Bus for CIOP

Transformation and Connectivity - enables secure connections to enterprise systems and the ability to filter, aggregate, or modify data or its format as it moves between platform and systems components and enterprise systems (typically systems of record). Within the reference architecture the transformation and connectivity component sit between the Platform operations and edge and enterprise network. The Transformation and Connectivity component includes the following capabilities:

- **Enterprise Secure Connectivity** - integrates with enterprise data security systems to authenticate and authorize access to enterprise systems.
- **Transformation** - transforms data between enterprise systems.
- **Enterprise Data Connectivity** - enables provider platform components to connect securely to enterprise data.

Exchange/Message Broker

CIOP should exchange data between Edge layer / Enterprise Applications / 3rd Party services using Publish and Subscribe mechanism.



Figure-20 Exchange/Message Broker for CIOP

API Services – Secured REST API services should enable to integrate, share and exchange data between CIOP and heterogeneous applications like Utility Scada, E-Governance, ERP, Environmental monitoring, Parking, IBMS, GIS, etc. The data generated by systems could be shared to other systems which is deployed or yet to be deployed in DSIR must adapt to the standard patterns.

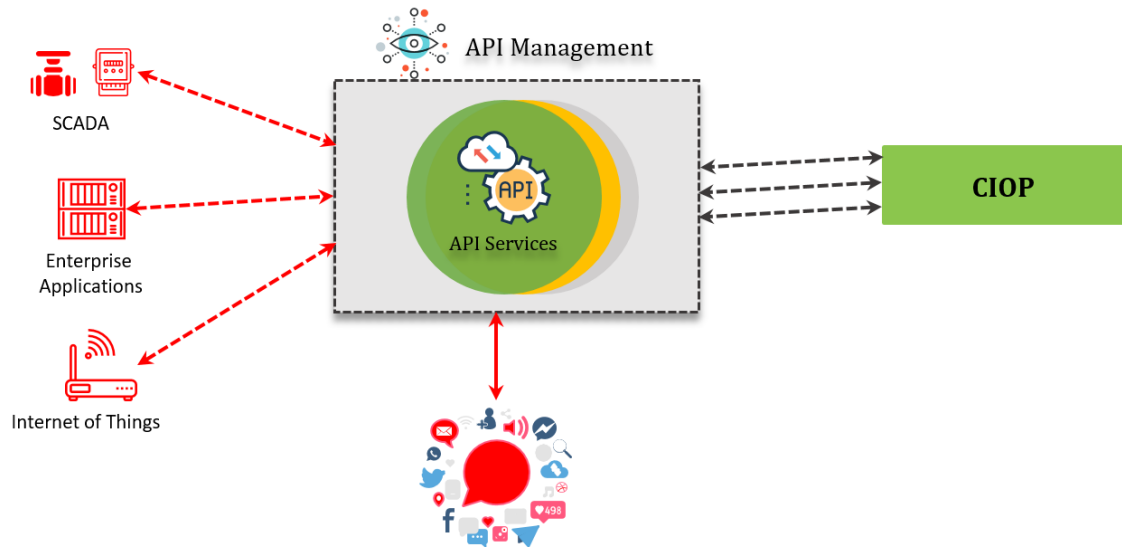


Figure-21 API Service Management

Data Compute Layer

Compute layer / middleware layer should store, analyze, and process huge amounts of data that comes from the heterogeneous devices, applications and services deployed across DSIR. It should manage and provide a diverse set of services to the lower layers. It should employ many technologies such as databases, computing, and big data processing modules.

Data Lake

Data Lake should be a central repository of integrated data from one or more disparate sources in DSIR. Data Lake should allow to persist vast amounts of relational and non-relational data that has been generated from heterogeneous data sources in DSIR without transformation or schema definition. Data Lake should allow to handle high volumes of small writes at low latency, is optimized for massive throughput, and well suited for event streams in IoT scenarios.

Complex Event Processing (CEP)

CEP in CIOP should support to identify the most meaningful events and patterns from multiple data sources, analyze their impacts, and act on them. The main objective of a CEP engine should be to detect the occurrence of event patterns on the incoming streaming data. CEP should facilitate real time event detection, correlation and notification of alerts

Batch Processing

CIOP should be provisioned for batch processing facility to gather data over a period and sent together as a batch. Batch processing must suite for workloads that require running lots of automated tasks, such as performing regular (such as monthly or quarterly) processing, risk calculations, or different types of computations to detect operational behavior of assets or operations around DSIR.

Business Intelligence / Data Analytics

In DSIR, data analysis would be considered as the main source of promoting growth and wellbeing. Heterogeneous data, which will be generated from multiple sources in DSIR, has come with processing challenges to increase citizen's quality of life and sustainable city operations efficiently.

In DSIR, the data should be gathered from various objects; gain insights from the data and making decisions require novel algorithms and visualization techniques, which affect smart city-focused activities.

CIOF facilitates on-the-fly processing of data and traditional store-then-process approach.

City Integrated Operations Center (CIOF) is the nerve center of any Smart City and will provide a platform for intelligent city management. It will consist of Surveillance data, sensors data, spatial data from GIS system, BIG Data, Analytics and Visualization for smooth operations and quick decision-making.

CIOF will leverage information provided by multiple systems to help in providing an integrated, seamless, proactive, and comprehensive response mechanism for day-to-day city operations and challenges. Apart from the city integrated operations platform, it will also make use of advanced analytics capabilities to enhance city's Intelligence and better manage services provided to the citizens.

The cross platform advance analytics shall be used to help the smart city in:

- Extract meaningful insights from Data
- Provide forward looking inputs for smoother operations of the city
- Take preventive Action
- Forecast the requirement and enable effective planning
- Understand Priorities, Convenience and Sentiment of the citizen

Analytics can make a city truly smart by providing the efficiencies in managing huge amount of streaming data and providing insights for more optimized city operations.

Business Intelligence and Analytics solution shall help city to;

- Reduce cost and raise productivity by collecting, managing and analyzing data in real time, streaming real-time analytical data helps in prompt decision making
- Respond quickly and confidently to changing conditions, as you tap into the full potential of all your data to make better-informed business decisions.
- Skip complexity when you streamline and automate processes across any IoT enabled infrastructure for incremental and long-term efficiencies.

MSI shall design and develop a analytics application/system that should have the facility/provision for;

- Streaming Data Analytics – Provides capabilities to process, filter, transform, and score (with the help on analytical model) millions of events per second.
- Data access, Cleansing and loading – Provides the capability to access process and cleanse structured, unstructured and streaming data.
- Self Service Analytics – Provides capability to generate analytics on the fly by dragging and dropping parameters.
- Forecasting – Provides the capability to forecast future trends based on historic patterns and trends
- Predictive Analytics - Provides the capability to do what if and scenario based analysis which aid to proactive actions
- Optimization - Provides the capability to maximize or minimize KPI based problems
- Text Analytics with English/Hindi Language Plug-in - Provides the capability to analyze free text in multiple languages and tap into current trends, complaints, sentiment and citizen view

It has been envisaged that MSI should implement a common analytics application/system to facilitate the key stakeholders of DICDL in getting real time and batch data to act on smart and corrective decisions within stipulated time duration.

Through the help of a common analytics/BI application DICDL can get benefited by getting insights and real-time data from IoT, Surveillance, ERP, eGovernance system, etc. as part of smart city program. The common BI/analytics system should integrate with both historical as well as real time streamed data from various utilities (water, power, gas, etc.), transport, parking, lighting along with other sources of data from smart city and batch data and from ERP / eGovernance applications responding to citizen-provided information with business intelligence as well as analytics driven insights.

The BI/analytics system should be able to provision capabilities such as real-time analytics of streaming data, Data Quality, reporting, data exploration, forecasting, predictive analytics, optimization as well as other functionalities as requires/requested by DICDL officials during the project/contract duration.

Rule Engines

CIOF should manage all the rules, which are necessary for context evaluation. Platforms rule engine should allow to process data from various sources with a configurable set of rules. Rule engine should

- Trigger a notification when critical event raised.
- Trigger alarm when value of a parameter exceeds certain threshold
- Trigger platform services to automate certain workflows

Big Data Management

The huge amount of data will be generated in DSIR from all heterogeneous smart systems like ITMS, BMS, City Utility (water, sewage, CETP, etc.), Parking, environmental monitoring and 3rd party services like Social Media.

To handle various types of data, with varying velocity an efficient big data management system is required.

Bigdata management system should be reliable and scalable with no downtime. Continuous generation, collection, processing and storage of massive heterogeneous data from countless smart city sensors has its own intrinsic challenges. Big data collected across city is extremely useful and is vital for achieving objective of smart city

Command control Layer

CIOC should integrate with systems providing visibility of overall city operations and helping optimize operational efficiency. Integrated data visualization, real-time collaboration, and deep analytics should help city administrators to prepare for problems, plan for growth and coordinate & manage response efforts. Dholera CIOC should effectively deliver services in a more sustainable fashion, enhancing the ongoing efficiency of city operations while protecting citizens and driving economic growth.

The command center will enable Government agents, Operator and city administrators alike to get a holistic view of city conditions, and make informed decisions

Data visualization

CIOOP should enable collaborative dashboard to visualize data using charts, graphs, gauges, maps, tables, and controls. The CIOOP dashboard should enable customizable visualization can be used to quickly and easily build or edit dashboards widgets for any group or department in CIOOP.

GIS

CIOOP should have the capability to generate as well as integrate with Geographic Information System (GIS component) to store, retrieve, manage, display, and analyze all types of geographic and spatial data related to Dholera. It should have the functionality to integrate with GIS software basemap, multiple layers and other graphic displays for analysis and presentation. GIS should be provisioned to

- Mapping where things are
- Mapping Quantities
- Mapping Densities
- Finding what is inside
- Mapping Events, etc.

KPI

Key Performance Indicators are quantifiable metrics (values that can be measured) that should reflect the performance of a city efficiency in the context of achieving its wider goals and objectives. KPIs should help city administrators to implement strategies by linking various levels of a city activities with clearly defined targets and benchmarks.

BI/Reporting Tools

Business Intelligence tools should leverage information across DSIR city applications and departments to coordinate resources to respond the issues rapidly and effectively. BI should include gathering, storing and providing access to data through applications such as decision support systems, query and reporting, online analytical processing, statistical analysis and forecasting.

Alerts/Notifications

Should Trigger alerts based on threshold defined for devices using rule engines and notifies the concerned user through SMS, Call, Web Notify, Push Notification, Email.

Incident Management

Incident management should help to keep track of the activity by raising tickets and assigns to respective operational team in DSIR to get issues resolved.

SOP Management

SOP Management should provide step-by-step instructions based on the Authorities policies and tools to resolve the situation and presents the relevant situation information in a quick and easily digestible format for an operator to verify the situation.

Work Flow Management

CIOOP WFM should enable the following features in CIOOP like

- Automatic Resource Management
- Auto Horizontal Scaling
- Rebalancing Dynamic Works
- Exactly once processing

Application & Service Layer

The COTS/customized based DSIR city applications like ERP, eGovernance, SCADA, IoT and Services like GIS, Notifications should be integrated with CIOP through API services. Each application deployed should have its own unique set of operations and process. Each application or services must interact with each other through secured API services.

IoT Architecture

IoT architecture should provide a guidance to integrate custom IoT systems like Smart Parking, Solid Waste Bins and complex SCADA Systems like Water, Gas, Sewage, CEPT etc., to CIOP

Connectivity Blocks

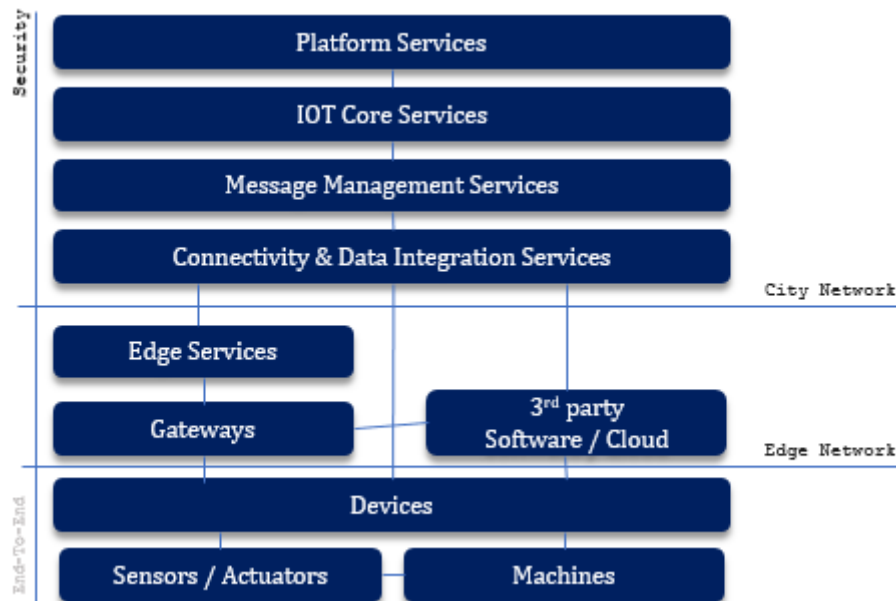


Figure- 22 Connectivity Blocks for CIOP

Architecture connectivity blocks should be followed while integrating IoT services with CIOP.

- Sensors and actuators should connect with devices
- Devices which collect data from sensors and communicate either to gateways or to CIOP or to cloud
- Gateways collect data from multiple devices on field and perform data transformations and analytics.
- Gateway shall communicate for data to platform through edge API services exposed by CIOP
- CIOP or COTS/other applications should enable APIs as per the cloud vendor specification to share the data from cloud.
- Connectivity and Data Integration services enable necessary services to receive and process data from DSIR field Gateways/Devices/Cloud Services
- Message Management Services in COTS/customized applications and CIOP perform data normalization and storage
- IoT Core services enable device governance services, device management services and Security services to manage devices in remote field of DSIR like monitoring the status of devices, Over the upgrades, controlling the values of pipelines, controlling the power supplies etc.

IoT building blocks

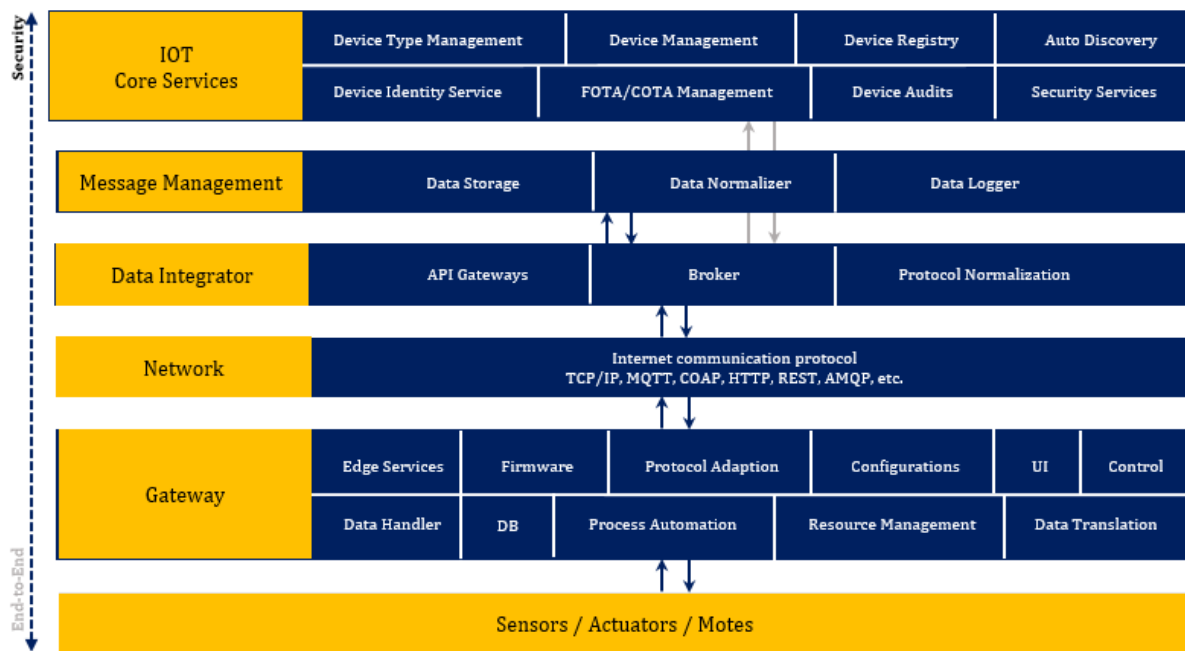


Figure-23 IoT Building Blocks

IoT building blocks should expose all necessary operations and components involved in each layer. Each layer represented with the communication flow between other layers. These building blocks are one of the segment of CIOP layers, details specific to integrating all IOT elements deployed across DSIR.

Gateway Layer

Gateway should collect data from on field devices deployed across DSIR. Layer should enable processing like Data handling, Data translation, Control, Process automation, resource management, etc. Gateway layer must communicate processed data through API services exposed by CIOP or through message brokers.

Network Layer

Should enable connectivity and transfer data to CIOP and COTS/other applications through deployed city wide optic fiber or through GSM/GPRS/LTE network.

Data Integration Layer

Data integration layer from CIOP should receive data from gateways and allow authorized source of data for further level of processing in CIOP.

Central hardware where system applications and other system specific data are stored and retrieved. This includes a combination of data hosted on cloud and some on-premise data processing and storage as per the requirements of this RFQ cum RFP.

Message Management Layer

Message Management Layer should convert and normalize data as per CIOP one format and logs & stores it.

IoT core services Layer

IoT core service layer must play an orchestration role in CIOP to manage devices, enables secure connection, logs device activity, controls device operations like FOTA/COTA.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-AS 1.1	CIOP	CIO-Attribute of System	Interoperability	Systems must exchange information between systems, services and also use the information that has been changed
CIO-AS 1.2	CIOP	CIO-Attribute of System	Interoperability	System must not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific product
CIO-AS 1.3	CIOP	CIO-Attribute of System	Interoperability	System must syntactically interoperable which is associated with data formats. Data being transferred must have well-defined syntax and encoding
CIO-AS 1.4	CIOP	CIO-Attribute of System	Interoperability	Systems must enables to combine received information from other information resources and must process it in a meaningful manner
CIO-AS 1.5	CIOP	CIO-Attribute of System	Interoperability	Systems must link processes among different systems. Platform must have interconnection between multiple other city solutions from a variety of vendors.
CIO-AS 1.6	CIOP	CIO-Attribute of System	Evaluability	Platform components, modules and services should be modular and modifiable.
CIO-AS 1.7	CIOP	CIO-Attribute of System	Evaluability	Platform should adapt to new requirements and changes, which is inherent in a system that has high evaluability.
CIO-AS 1.8	CIOP	CIO-Attribute of System	Performance	System should measure time-behavior, resource utilization and capacity
CIO-AS 1.9	CIOP	CIO-Attribute of System	Performance	Platform should facilitate the responsiveness and stability of a system.
CIO-AS 1.10	CIOP	CIO-Attribute of System	Performance	Performance should measure response time, throughput (number of transactions per time unit), resource, efficiency and scalability for applications, services deployed in CIOC.
CIO-AS 1.11	CIOP	CIO-Attribute of System	Scalability	Important technical components of the architecture must support scalability (horizontal, vertical), failover to provide continuous growth to meet the growing demand of DSIR.
CIO-AS 1.12	CIOP	CIO-Attribute of System	Scalability	The Platform should also support vertical and horizontal scalability so that depending on changing requirements from time to time in CIOC, the system should be scaled upwards
CIO-AS 1.13	CIOP	CIO-Attribute of System	Scalability	Main technology components should facilitate scalability in storage, bandwidth, computing performance
CIO-AS 1.14	CIOP	CIO-Attribute of System	Scalability	The architecture should be scalable and capable of delivering high performance till the platform system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers, data source connector and all other solution components. Scalability should have ability to expand the system to catch up to the ever-increasing data streams, so that the promise of the Quality of Service (QoS) or Service Level Agreement (SLA) could be honored.
CIO-AS 1.15	CIOP	CIO-Attribute of System	Security & Privacy	The architecture adopts an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, hacks, natural disasters etc. Platform provision for security of field equipment as well as protection of the software applications, services from hackers and other threats.
CIO-AS 1.16	CIOP	CIO-Attribute of System	Security & Privacy	Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism appropriate insurance cover must be provided to all the equipment supplied under this

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				project. All the system implemented for DSIR should be highly secure, with adequate security & protection of the sensitive data.
CIO-AS 1.17	CIOP	CIO-Attribute of System	Security & Privacy	Applications hosted in the central data center/Server Room should support multi-tenancy with adequate authentication and Role based access control mechanism for each user pertaining to their respective line department infrastructure
CIO-AS 1.18	CIOP	CIO-Attribute of System	Security & Privacy	The smart city architecture should be capable of managing and integrating heterogeneous data (structured/unstructured), which would be continuously communicated through numerous devices/applications following different protocols. In order to ensure that the flow of data between devices/application does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency.
CIO-AS 1.19	CIOP	CIO-Attribute of System	Security & Privacy	From a network security perspective, all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices/applications/services at each endpoint of the network should be authenticated
CIO-AS 1.20	CIOP	CIO-Attribute of System	Security & Privacy	The authentication system so used on these endpoint devices should ensure that only authorized users/devices/applications/services are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems
CIO-AS 1.21	CIOP	CIO-Attribute of System	Manageability	System must be easy to configure with a user friendly UI and single screen interface.
CIO-AS 1.22	CIOP	CIO-Attribute of System	Manageability	Platform should monitor ongoing health of applications and solutions
CIO-AS 1.23	CIOP	CIO-Attribute of System	Manageability	Systems must detect failure.
CIO-AS 1.24	CIOP	CIO-Attribute of System	Heterogeneity	CIOP must accommodate for a vast variety of scenarios, environments, devices, processing patterns, and standards. It should be able to handle vast hardware and software heterogeneity
CIO-AS 1.25	CIOP	CIO-Attribute of System	Real-Time	The platform need to be able to process data/events in real-time, i.e. providing a fast analysis and responses for situations of urgency.
CIO-AS 1.26	CIOP	CIO-Attribute of System	Availability	The platform components/services/applications should be redundant and ensure that are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology disruption. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The Platform provisioned for high availability for all the services of the system. Redundancy has to be considered at the core / data center /server room components level.
CIO-PI 2.1	CIOP	CIO-Platform	Integration	The platform shall have ability to connect and integrate other technologies, services and third-party software systems. In addition, act as a singular platform for entire DSIR. The system should be able to bi-directionally and dynamically exchange data between various software applications in real-time as well as schedule transfer. Platform should Support for unlimited applications, services, servers, data source connectors, users, reports and clients. Support for storage expandability.
CIO-PI 2.2	CIOP	CIO-Platform	Integration	Platform should be able to integrate, connect, and correlate information from various applications, and other IT & non-IT systems, providing rule-based information drawn from various sub-systems for alert generations.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-PI 2.3	CIOP	CIO-Platform	Integration	Platform data processing engine should process (Extract, Transform, Load) and then normalize and integrate / ingest the data coming from different sources and provide secure access to that data (both structured and unstructured) using data API(s), ESB (Enterprise Service Bus), Message Brokers and scripts etc. to application developers for various devices being used by the city for various urban as well as smart city related services.
CIO-PI 2.4	CIOP	CIO-Platform	Integration	This Platform should be able to use standardized data model for each smart urban service as needed for the city and map the data from different devices to the common data model, with the help of built-in modelling and simulation tools. This will enable in avoiding the complexity of various data formats and carry advance data intelligence from time to time to generate reports and create dashboards for various connected / inter-dependent city operations.
CIO-PI 2.5	CIOP	CIO-Platform	Integration	Data from the edge applications, edge services must be exposed to application eco system using secure APIs using API keys, message brokers or using ESB tools
CIO-PI 2.6	CIOP	CIO-Platform	Integration	Attributes of API key(s) or ESB tools must restrict / allow access to relevant data based on various attributes, domains and tenants.
CIO-PI 2.7	CIOP	CIO-Platform	Integration	Should be able to integrate with any type of application platform being used for the smart urban services irrespective of the technology used, agnostics to various technologies and allow the OEMs to develop integrations using API's, SDKs, ESBs, Scripts, etc. without affecting the existing application and integration.
CIO-PI 2.8	CIOP	CIO-Platform	Integration	Should support distributed deployment of functions (workflows & policies) across city's infrastructure with centralized management and control.
CIO-PI 2.9	CIOP	CIO-Platform	Integration	System must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM.
CIO-PI 2.10	CIOP	CIO-Platform	Integration	Platform should be implemented and complied to the industry open standards based Commercial-of-the-shelf (COTS) products and should provide data ingestion, analysis and visualization using the same platform
CIO-PI 2.11	CIOP	CIO-Platform	Integration	Should have out of box support for multitenant environments to provide support for multiple departments using a single deployment while ensuring that each tenant user can access only the data that they are authorized to use and super tenant can use all the data.
CIO-GIS 3.1	CIOP	CIO-Platform	GIS	System should support various open standard GIS systems as per city specific requirements.
CIO-GIS 3.2	CIOP	CIO-Platform	GIS	System should expose secured API to access GIS related services
CIO-GIS 3.3	CIOP	CIO-Platform	GIS	System should provide geographical coordinates of specific objects / facilities, roads, and city infrastructure assets, as well as unmapped facilities.
CIO-GIS 3.4	CIOP	CIO-Platform	GIS	System should calculate distance between two, or more, locations on the map.
CIO-GIS 3.5	CIOP	CIO-Platform	GIS	System should locate, trace and search for objects on the map.
CIO-GIS 3.6	CIOP	CIO-Platform	GIS	Should support the following but not limited to 3d models, Geometry models, Point of Interest, Schedule Data
CIO-GIS 3.7	CIOP	CIO-Platform	GIS	The platform shall integrate with GIS, map information, and be able to dynamically update information on the GIS maps to show status of resources.
CIO-GIS 3.8	CIOP	CIO-Platform	GIS	The system shall have GIS Maps, Geo fencing tools and GIS engine
CIO-GIS 3.9	CIOP	CIO-Platform	GIS	System should visually display an alarming sensor on map
CIO-GIS 3.10	CIOP	CIO-Platform	GIS	System should visually differentiate sensor alarm severities on map through different color and icon identifiers
CIO-GIS 3.11	CIOP	CIO-Platform	GIS	System should immediately view alarm details (including description, asset details, etc.) and investigate the alarm from the map.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-GIS 3.12	CIOP	CIO-Platform	GIS	Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.
CIO-GIS 3.13	CIOP	CIO-Platform	GIS	The Platform should be able to generate heat maps, vectors, dashboards, layer widgets, etc.
CIO-GIS 3.14	CIOP	CIO-Platform	GIS	The Platform should be accessible anywhere by any devices like desktop, tab, mobile etc.
CIO-GIS 3.15	CIOP	CIO-Platform	GIS	The CIOP should have geospatial visualization layer compliant to industry open standard applications
CIO-RE 4.1	CIOP	CIO-Platform	Resiliency	System should support standard Authentication and Authorization and Accounting for access.
CIO-RE 4.2	CIOP	CIO-Platform	Resiliency	System should provide appropriate resiliency for the system to ensure high availability and trouble-free operations for users
CIO-RE 4.3	CIOP	CIO-Platform	Resiliency	Platform should ensure ways and means to define policies that make applications or objects respond to various external eco system.
CIO-RE 4.4	CIOP	CIO-Platform	Resiliency	System would provide scheduled services for future actions.
CIO-RE 4.5	CIOP	CIO-Platform	Resiliency	System should integrate with collaboration tools to bring multiple stakeholders and responders to respond an emergency or an urban/smart city services event.
CIO-RE 4.6	CIOP	CIO-Platform	Resiliency	System should provide different tier of user categorization, authentication, authorization, and services.
CIO-RE 4.7	CIOP	CIO-Platform	Resiliency	System should provide role-based access view to applications.
CIO-RE 4.8	CIOP	CIO-Platform	Resiliency	System should support multitenancy access
CIO-RE 4.9	CIOP	CIO-Platform	Resiliency	System should ensure time shifted and real-time data (structured and unstructured) available for intelligence and correlations using BI platform (with ETL, Integration, Modelling & Simulation, Dashboard functionalities) and Bigdata Processing Engines.
CIO-RE 4.10	CIOP	CIO-Platform	Resiliency	Should also be able to ingest other utilities, surveillance, ERP, e-governance and other applications data. It should also include scalability for future deployment
CIO-RE 4.11	CIOP	CIO-Platform	Resiliency	OEM should be able to securely access the system remotely for updates / upgrades and maintenance for the given duration.
CIO-RE 4.12	CIOP	CIO-Platform	Resiliency	The system should be able to be deployed across multiple sites and on cloud for operations and disaster recovery purposes
CIO-RE 4.13	CIOP	CIO-Platform	Resiliency	Platform shall run applications in a distributed environment with fault-tolerant, high-availability and scalability.
CIO-API 5.1	CIOP	CIO-Platform	API Management	CIOP should facilitate an end-to-end API Management solution for designing, implementing, securing, managing, monitoring, and publishing APIs. API management facilitates to reach any services, applications deployed in DSIR to visualize the data or control the entities like devices, gateways or to retrieve data from database.
CIO-API 5.2	CIOP	CIO-Platform	API Management	Platform should facilitate to securely access API's to protect sensitive data.
CIO-API 5.3	CIOP	CIO-Platform	API Management	Platform should facilitate to control the traffic inflow and outflow through APIs
CIO-API 5.4	CIOP	CIO-Platform	API Management	System should govern complete API operations and services.
CIO-API 5.5	CIOP	CIO-Platform	API Management	System should provide documentation, to create and manage API

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-API 5.6	CIOP	CIO-Platform	API Management	System should facilitate an analytical view for API usage and support to generate report
CIO-API 5.7	CIOP	CIO-Platform	API Management	System should support multi-type API gateways
CIO-API 5.8	CIOP	CIO-Platform	API Management	System should manage complete API lifecycle
CIO-API 5.9	CIOP	CIO-Platform	API Management	System should support pre/post processing of data at the API level
CIO-API 5.10	CIOP	CIO-Platform	API Management	System should facilitate data mediation to convert format like JSON to XML, Streams to JSON, XML to JSON
CIO-API 5.11	CIOP	CIO-Platform	API Management	System should facilitate to blacklist or whitelist IP to allow selected resources wherever applicable.
CIO-API 5.12	CIOP	CIO-Platform	API Management	System should provide secure authentication and Authorization policies.
CIO-API 5.13	CIOP	CIO-Platform	API Management	System should Facilitate to test API services without affecting existing operations
CIO-API 5.14	CIOP	CIO-Platform	API Management	System should Facilitate to monetize data usage by external services wherever applicable.
CIO-API 5.15	CIOP	CIO-Platform	API Management	System should include availability of vendor/platform agnostic APIs to control all application functionality.
CIO-API 5.16	CIOP	CIO-Platform	API Management	Platform should enable access to the platform API(s) using secured API keys.
CIO-API 5.17	CIOP	CIO-Platform	API Management	System should facilitate relevant and appropriate APIs made available for all the application domains to monitor, control app developers to develop apps and connectors / adaptors to the platforms.
CIO-API 5.18	CIOP	CIO-Platform	API Management	Platform should facilitate APIs enabling contextual information and correlation across domains and verticals for multiple platforms and multiple sensors, as and when needed in future
CIO-API 5.19	CIOP	CIO-Platform	API Management	API management and gateway should provide secure API lifecycle, monitoring mechanism for available APIs.
CIO-API 5.20	CIOP	CIO-Platform	API Management	System should expose data to application ecosystem using secure APIs using API keys or other appropriate connectors/protocols/scripts.
CIO-API 5.21	CIOP	CIO-Platform	API Management	System must restrict / allow access to relevant data using secured API key(s) or other appropriate connectors/protocols/scripts
CIO-EDM 6.1	CIOP	CIO-Platform	Events & Data Management	System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should be a set of conditions that activate the behavior it provides.
CIO-EDM 6.2	CIOP	CIO-Platform	Events & Data Management	System should allow Default, Time-based, Event-based and Manual override policies creation.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-EDM 6.3	CIOP	CIO-Platform	Events & Data Management	System should have a provision to define a set of conditions that can be used to trigger an event-based policy along with correlations.
CIO-EDM 6.4	CIOP	CIO-Platform	Events & Data Management	System should provide the capability for the events that are produced from subsystems and are forwarded to the CIOC. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the CIOC, the event should be displayed on an operations dashboard and analyzed to determine a proper directive.
CIO-EDM 6.5	CIOP	CIO-Platform	Events & Data Management	System should provide an event reporting and data tracking mechanism to enable identification and understanding across underlying domains. Shall provide capability to manage predicted events, planned events, and current events as they evolve.
CIO-EDM 6.6	CIOP	CIO-Platform	Events & Data Management	System should provide an integrated geographic information system (GIS) or location plan maps events visually.
CIO-EDM 6.7	CIOP	CIO-Platform	Events & Data Management	System should provide capability to gauge the impact of events through interactive mapping and scenario analysis.
CIO-EDM 6.8	CIOP	CIO-Platform	Events & Data Management	System should provide capability to filter information about events that are based on date and time, location, and other categories that you define.
CIO-EDM 6.9	CIOP	CIO-Platform	Events & Data Management	System should provide capability to view the filtered information either highlighted on a map, listed in a table or in a calendar, or chronologically on a timeline. The information is easy to access when and where you need it
CIO-DB 7.1	CIOP	CIO-Platform	Dashboard	System should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance
CIO-DB 7.2	CIOP	CIO-Platform	Dashboard	System should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of CIOC
CIO-DB 7.3	CIOP	CIO-Platform	Dashboard	System should Provide interactive graph of readings that are obtained over time in context to individual devices (e.g. Sensors, bulk flow meters, Power meters)
CIO-DB 7.4	CIOP	CIO-Platform	Dashboard	System should provide historical reports, event data & activity log. The reports can be exported to pdf or html formats.
CIO-DB 7.5	CIOP	CIO-Platform	Dashboard	System should provide mechanism to define association between assets / incidents
CIO-DB 7.6	CIOP	CIO-Platform	Dashboard	System should provide capability to filter information about event based on boundary area defined by operator
CIO-DB 7.7	CIOP	CIO-Platform	Dashboard	System should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details
CIO-DB 7.8	CIOP	CIO-Platform	Dashboard	System should be able to correlate data coming from different sources and create automated actionable items
CIO-DB 7.9	CIOP	CIO-Platform	Dashboard	System should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details
CIO-OP 8.1	CIOP	CIO-Platform	Operations	The CIOP shall provide operators and city administrators with a management dashboard that provides a real-time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-OP 8.2	CIOP	CIO-Platform	Operations	The platform shall provide the day-to-day operations and situational awareness to the participating agencies during various modes of operation.
CIO-OP 8.3	CIOP	CIO-Platform	Operations	Platform data processing engine should process data and then normalize for sensor applications and integrate / ingest the data coming from different sources and provide secure access to that data (both structured and unstructured) using API(s), ESB (Enterprise Service Bus), Message Brokers and scripts etc. to application developers for various devices being used by the city for various urban services.
CIO-OP 8.4	CIOP	CIO-Platform	Operations	Shall provide a uniform, coherent, user-friendly and standardized interface.
CIO-OP 8.5	CIOP	CIO-Platform	Operations	Shall provide possibility to connect to workstations, video walls and accessible via web browser.
CIO-OP 8.6	CIOP	CIO-Platform	Operations	Dashboard content and layout shall be configurable, and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard.
CIO-OP 8.7	CIOP	CIO-Platform	Operations	The platform should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for intelligence and correlation purposes.
CIO-OP 8.8	CIOP	CIO-Platform	Operations	System shall be possible to combine the different views onto a single screen or a multi-monitor workstation or video walls.
CIO-OP 8.9	CIOP	CIO-Platform	Operations	Should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.
CIO-OP 8.10	CIOP	CIO-Platform	Operations	Should provide ability to extract data in desired formats for publishing, reporting and interfacing purposes.
CIO-OP 8.11	CIOP	CIO-Platform	Operations	Should have out of box support for multiple zones/user environments to provide support for multiple departments using a single deployment while ensuring that each tenant user can access only the data that they are authorized to use and super user can use all the data
CIO-OP 8.12	CIOP	CIO-Platform	Operations	Should provide ability to attach documents to incidents and other entities.
CIO-OP 8.13	CIOP	CIO-Platform	Operations	The platform should issue, log, track, manage and report all activities underway during the various modes of operation.
CIO-OP 8.14	CIOP	CIO-Platform	Operations	System should support centralized logging & auditing framework.
CIO-OP 8.15	CIOP	CIO-Platform	Operations	System should have policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g. SLAs).
CIO-OP 8.16	CIOP	CIO-Platform	Operations	System should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, software licenses etc.
CIO-OP 8.17	CIOP	CIO-Platform	Operations	System shall provide integrated tool for evidence management of critical events and incidences digitally with provision for long term tamper proof data preservation
CIO-OP 8.18	CIOP	CIO-Platform	Operations	System should be able to package related critical documents, video clips, audio clips, playback events etc. required as proofs, and create storage media for submission to administration or judiciary for critical matters. Provisions should be made for such data to be preserved with storage sub-system level metadata search facilities only on disk based self-healing storage systems that are tamper proof and with hardware level WORM and ensure that integrity and quality of critical data pertaining to city operations, is appropriately maintained.
CIO-OP 8.19	CIOP	CIO-Platform	Operations	Platform should ensure fault free functioning and maintain data integrity.
CIO-VDS 9.1	CIOP	CIO-Platform		The platform shall provide camera search including its location using latitude/longitude.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
			Video data Smart Search	The user should have a simple search dialog, which allows them to provide a keyword search across all objects and events. The system should be able to determine from the keywords entered if this is an address in which case the system would return a list of possible addresses
CIO-NAA 10.1	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Field Responder Mobile App if required.
CIO-NAA 10.2	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System must facilitate all system messages (notifications, alerts and alarms) always be visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.
CIO-NAA 10.3	CIOP	CIO-Platform	Notifications, Alerts & Alarms	Systems should deliver message to a set of users. The Notification service should support notification methods such as Email and SMS
CIO-NAA 10.4	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System should have an ability to display alarm condition through visual display and audible tone
CIO-NAA 10.5	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System should have an ability to simultaneously handle multiple alarms from multiple workstations
CIO-NAA 10.6	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, device, severity, etc.
CIO-NAA 10.7	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System should have an ability to view historical alarms details even after the alarm has been acknowledged or closed
CIO-NAA 10.8	CIOP	CIO-Platform	Notifications, Alerts & Alarms	System should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location
CIO-IMS 11.1	CIOP	CIO-Platform	Incident Management System	The system must provide Incident Management Services to facilitate the management of response and recovery operations
CIO-IMS 11.2	CIOP	CIO-Platform	Incident Management System	System should support comprehensive reporting on event status in real time manually or automatically by a sensor/sub-system.
CIO-IMS 11.3	CIOP	CIO-Platform	Incident Management System	System should support for sudden critical events and linkage to standard operating procedures automatically.
CIO-IMS 11.4	CIOP	CIO-Platform	Incident Management System	System should support for multiple incidents with both segregated and/or overlapping management and response teams.
CIO-IMS 11.5	CIOP	CIO-Platform	Incident Management System	System should support Geospatial rendering of event and incident information.
CIO-IMS 11.6	CIOP	CIO-Platform	Incident Management System	System should support plotting of area of impact using lines and circles to divide the area into multiple zones on the GIS maps. Should support overlapping and exclusion on top of overlapping.
CIO-IMS 11.7	CIOP	CIO-Platform	Incident Management System	System should support incorporation of resource database for mobilizing the resources for response.
CIO-IMS 11.8	CIOP	CIO-Platform	Incident Management System	System should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should be captured in standard formats to facilitate incident correlation and reporting.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-IMS 11.9	CIOP	CIO-Platform	Incident Management System	The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems
CIO-IMS 11.10	CIOP	CIO-Platform	Incident Management System	System should provide detailed reports and summary views to multiple users based on their roles.
CIO-IMS 11.11	CIOP	CIO-Platform	Incident Management System	System must provide posting, updating and disseminating plans, procedures, checklists and other related information.
CIO-IMS 11.12	CIOP	CIO-Platform	Incident Management System	System must provide User-defined forms as well as Standard Incident Command Forms for incident management
CIO-KPI 12.1	CIOP	CIO-Platform	Key Performance Indicator	The CIOP should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies.
				Green indicates that the status is acceptable, based on the parameters for that KPI, no action is required.
				Yellow indicates that caution or monitoring is required, action may be required.
				Red indicates that the status is critical and action is recommended
CIO-UR 13.1	CIOP	CIO-Platform	Users & Roles	Platform should allow different roles to be created and assign those roles to different access control policies. Based on their roles and the permissions, they should be allowed to perform various tasks, such as adding new locations, configuring new devices, managing adapters etc.
CIO-UR 13.2	CIOP	CIO-Platform	Users & Roles	Platform should allow single or multiple users to view and manage alarms in defined domains (areas/locations). User thus can be part of single or multiple domains.
CIO-UR 13.3	CIOP	CIO-Platform	Users & Roles	The platform should support unlimited simultaneous user access.
CIO-UR 13.4	CIOP	CIO-Platform	Users & Roles	The Platform should support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely
CIO-WFE 14.1	CIOP	CIO-Platform	Workflow Engine	System should be available to respond to any event data ingested as mentioned earlier.
CIO-WFE 14.2	CIOP	CIO-Platform	Workflow Engine	System shall provide for dynamic assets(s) selection based on:
				o Geo location of assets and event.
				o User definable ranges or threshold using user definable units of measure
				o Specific assets or sensor selection by external system
CIO-WFE 14.3	CIOP	CIO-Platform	Workflow Engine	System must provide for each user defined range, the following camera movement capability:
				o Dynamic aim to event coordinates (without presets)
				o Move to the closest preset
				o Move to a specific preset
				o Start a specific tour
				o Snap camera to closest N, E, S, W direction after user defined delay
				o Zoom functions adjustable based on user defined scale and event type
CIO-WFE 14.4	CIOP	CIO-Platform	Workflow Engine	System must allow centralized user configurable actions by event and transaction types
CIO-WFE 14.5	CIOP	CIO-Platform	Workflow Engine	System must provide an ability to receive application events through all of the following mechanisms:

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				- o JSON interface using user defined port and IP Address for each transaction type - o Wait and listen for transactions to Initiate data request from external system - o Email interface using any standard off the shelf e-mail system - o Ability to develop custom interfaces as needed
CIO-WFE 14.6	CIOP	CIO-Platform	Workflow Engine	System shall be Self-managed to monitor, manage and execute workflows.
CIO-WFE 14.7	CIOP	CIO-Platform	Workflow Engine	System should include drag and drop UI to define workflow process on certain action on data.
CIO-WFE 14.8	CIOP	CIO-Platform	Workflow Engine	System shall have optional scripting to program a workflow engine.
CIO-WFE 14.9	CIOP	CIO-Platform	Workflow Engine	System should handle all workflows defined by user
CIO-WFE 14.10	CIOP	CIO-Platform	Workflow Engine	System should support sequential pattern when tasks are executed one after another. The next step in a workflow should not start until till the previous is finished.
CIO-WFE 14.11	CIOP	CIO-Platform	Workflow Engine	Platform should provide clear User Interface that guides user to create workflows. UI should have facility to drag and drop the components
CIO-WFE 14.12	CIOP	CIO-Platform	Workflow Engine	System should facilitate the flow of information, tasks, and events. Workflow engines may also be referred to as Workflow Orchestration Engines
CIO-WFE 14.13	CIOP	CIO-Platform	Workflow Engine	System should identify the processes to execute based on context and event.
CIO-WFE 14.14	CIOP	CIO-Platform	Workflow Engine	User should not be limited to define workflows.
CIO-WFE 14.15	CIOP	CIO-Platform	Workflow Engine	Platform should be scalable to execute workflow
CIO-WFE 14.16	CIOP	CIO-Platform	Workflow Engine	System should allow only System Administrators or Operators to create workflows
CIO-WFE 14.17	CIOP	CIO-Platform	Workflow Engine	System should log execution activities of workflows.
CIO-ASM 15.1	CIOP	CIO-Platform	Asset Status Monitoring	System should provide icon based user interface on the GIS map to report non-functional assets.
CIO-ASM 15.2	CIOP	CIO-Platform	Asset Status Monitoring	System should also provide a single tabular view to list all assets along with their availability status in real time.
CIO-ASM 15.3	CIOP	CIO-Platform	Asset Status Monitoring	Platform should provide User Interface to publish messages to multiple assets/devices at the same time
CIO-DBR 16.1	CIOP	CIO-Platform	Dashboards and Reports	Platform should have capability to provide access to real time data and historical data from various connected devices for reporting.
CIO-DBR 16.2	CIOP	CIO-Platform	Dashboards and Reports	Platform should facilitate latest web technology based web Dashboards
CIO-DBR 16.3	CIOP	CIO-Platform	Dashboards and Reports	System should be multi domain specific for operators, business owners, infrastructure maintenance team etc.
CIO-DBR 16.4	CIOP	CIO-Platform	Dashboards and Reports	System should provide trends in graphical representation form.
CIO-DBR 16.5	CIOP	CIO-Platform	Dashboards and Reports	System should allow users to filter content for select time period.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DBR 16.6	CIOP	CIO-Platform	Dashboards and Reports	System should allow monitoring the event details with respect to time and also device performance over time.
CIO-DBR 16.7	CIOP	CIO-Platform	Dashboards and Reports	Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details.
CIO-DBR 16.8	CIOP	CIO-Platform	Dashboards and Reports	System should have ability to generate reports and have provision to create user specific standard list of reports.
CIO-DBR 16.9	CIOP	CIO-Platform	Dashboards and Reports	Should provide historical reports, event data and activity logs. The reports can be exported to excel, PDF or HTML formats.
CIO-DBR 16.10	CIOP	CIO-Platform	Dashboards and Reports	System should be able to display report on monitor / video wall and print report.
CIO-DBR 16.11	CIOP	CIO-Platform	Dashboards and Reports	System should be able to capture Operators response.
CIO-DBR 16.12	CIOP	CIO-Platform	Dashboards and Reports	System should be able to select information and fields to be included in report at time of report generation.
CIO-DBR 16.13	CIOP	CIO-Platform	Dashboards and Reports	System should be able to generate details of alarm including severity, time / date, description, and location.
CIO-DBR 16.14	CIOP	CIO-Platform	Dashboards and Reports	System should be able to associate Map of surrounding area associated with alarm.
CIO-DBR 16.15	CIOP	CIO-Platform	Dashboards and Reports	System should have a facility for operator to transfer the incident report to Mobile Device/another operator's console.
CIO-DBR 16.16	CIOP	CIO-Platform	Dashboards and Reports	System should be able to generate and visualize incident reports.
CIO-DBR 16.17	CIOP	CIO-Platform	Dashboards and Reports	Platform should provide capabilities to build custom widget builder to build customer report widget or should have capabilities to edit customized widgets.
CIO-DBR 16.18	CIOP	CIO-Platform	Dashboards and Reports	Platform should not provide facilities to edit/customize systems standard widgets and reports.
CIO-DBR 16.19	CIOP	CIO-Platform	Dashboards and Reports	Platform shall provide facility to create custom reports and custom widgets without affecting the system integrity.
CIO-DBR 16.20	CIOP	CIO-Platform	Dashboards and Reports	System should support wide variety of Data Source – structured and unstructured.
CIO-DBR 16.21	CIOP	CIO-Platform	Dashboards and Reports	System should be business user friendly like drag and drop, easy access components like filter, search, widget and navigation
CIO-DBR 16.22	CIOP	CIO-Platform	Dashboards and Reports	System should support wide rich selection of widget commonly used in business dashboard, including variety of charts, Gauges, maps and grids
CIO-DBR 16.23	CIOP	CIO-Platform	Dashboards and Reports	System should support insertion of customized widgets to dashboard using few steps

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DBR 16.24	CIOP	CIO-Platform	Dashboards and Reports	System should provide dedicated filter panel to filter widget
CIO-DBR 16.25	CIOP	CIO-Platform	Dashboards and Reports	System should be powered by latest web technology.
CIO-DBR 16.26	CIOP	CIO-Platform	Dashboards and Reports	System shall provide Tabbed view of Dashboards
CIO-DBR 16.27	CIOP	CIO-Platform	Dashboards and Reports	System should support embedding Dashboard with the applications
CIO-SOP 17.1	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	The platform should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.
CIO-SOP 17.2	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	System should be able to edit the SOP, including adding, editing, or deleting activities.
CIO-SOP 17.3	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	System should be able to also add comments to or stop the SOP (prior to completion).
CIO-SOP 17.4	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	System should facilitate SOP to communicate with other heterogeneous applications deployed in DSIR
CIO-SOP 17.5	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	System should support to invoke SOP created in other heterogeneous applications deployed in DSIR through API services
CIO-SOP 17.6	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	System should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.
CIO-SOP 17.7	CIOP	CIO-Platform	Standard Operating Procedures (SOPs)	System should have capability to define the following activity types:
				o Manual Activity - An activity that is done manually by the owner and provide details in the description field.
				O Automation Activity - An activity that initiates and tracks a work flow and select a predefined flow order from the list.
				O If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
				O Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.
				o SOP Activity - An activity that launches another standard operating procedure
CIO-GE 18.1	CIOP	CIO-Platform	Gateway Engine	System should normalize the data coming from different devices of same type and provide secure access to that data using data API(s)/appropriate connectors to application developers
CIO-GE 18.2	CIOP	CIO-Platform	Gateway Engine	Platform should include Device Management of Data Transformation and connectivity services from various sources in a secured manner

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-AE 19.1	CIOP	CIO-Platform	Analytics Engine	Platform shall also support artificial intelligence-based advanced intelligence to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset & infrastructure management and better city services.
CIO-AE 19.2	CIOP	CIO-Platform	Analytics Engine	System should be state of the art technology platform capable of storing, transforming and processing humongous volumes data both structured and unstructured like text, image, video files in a parallel processing mode. The stored datasets which may be diverse, complex and massive are to be retrieved and processed in tolerable time. The platform must be capable to store unstructured, semi-structured and structured data in a reliable, secure, and fault-resilient and must act as a scalable data store that can be organized and sorted for indexing and analysis
CIO-AE 19.3	CIOP	CIO-Platform	Analytics Engine	System should be flexible to integrate with other city and e-government software applications.
CIO-AE 19.4	CIOP	CIO-Platform	Analytics Engine	System should have capability to analyze data in motion to display the alerts in real-time and store the data in centralized database for future trend analysis.
CIO-AE 19.5	CIOP	CIO-Platform	Analytics Engine	System should use analytics ranging from descriptive analytics to advanced algorithms, including automated modeling, text analytics, decision management, and optimization.
CIO-AE 19.6	CIOP	CIO-Platform	Analytics Engine	System should be able to analyze the real-time data, weekly data, monthly data, and archival data also and generate the reports in the system.
CIO-AE 19.7	CIOP	CIO-Platform	Analytics Engine	System shall have the ability to develop various threat models consisting of algorithms of keywords, Boolean operators, and weighting and brought to the attention of the user via the GUI
CIO-AE 19.8	CIOP	CIO-Platform	Analytics Engine	System solution shall support analysis of content aggregated into charts and graphs
CIO-AE 19.9	CIOP	CIO-Platform	Analytics Engine	System should support advanced predictive analytics and Correlation.
CIO-AE 19.10	CIOP	CIO-Platform	Analytics Engine	System should be flexible to integrate and execute intelligence on various city utility, surveillance, eGov / ERP applications and other city applications in both structured and unstructured data sets.
CIO-AE 19.11	CIOP	CIO-Platform	Analytics Engine	The platform should be able to predict insights on data from various city infrastructure and applications.
CIO-AE 19.12	CIOP	CIO-Platform	Analytics Engine	The platform should have predictions with measurable accuracy of at least 95%
CIO-AE 19.13	CIOP	CIO-Platform	Analytics Engine	The platform should be able to predict and integrate with Smart City solutions helping in driving operational policies creation.
CIO-AE 19.14	CIOP	CIO-Platform	Analytics Engine	System should provide platform with end user access ranging from ETL, integration of data from structured & unstructured data sources, intelligence with simulation and modelling and interactive dashboards with adhoc query, integration with spreadsheets, proactive alerting, Scorecards and so on.
CIO-AE 19.15	CIOP	CIO-Platform	Analytics Engine	System should provide capabilities to create KPIs to measure progress and performance over time and graphically communicate strategy & strategic dynamics using Strategy maps, Cause and Effect diagrams, and Custom views. Intuitive and dense visualizations must be available.
CIO-AE 19.16	CIOP	CIO-Platform	Analytics Engine	System should enable the operators to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system should carry the following tasks
				o Connect to a variety of data sources
				o Run intelligence on the result set
				o Visualize the results
				o Predict outcomes

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				o Prescribe options for DSS (decision support system)
CIO-AE 19.17	CIOP	CIO-Platform	Analytics Engine	System should support multiple standard data sources such as CSV, TSV, MS Excel, NoSQL, RDBMS, etc.
CIO-AE 19.18	CIOP	CIO-Platform	Analytics Engine	System should provide intelligence on data from selected data source(s).
CIO-AE 19.19	CIOP	CIO-Platform	Analytics Engine	System should provide capability to check with multiple predictive algorithms.
CIO-AE 19.20	CIOP	CIO-Platform	Analytics Engine	System should facilitate to visualize data on dashboard and ensure following features:
				o It should allow to change visual attributes of a graph in the visualization workspace / dashboard.
				O User should not be allowed to alter the graph/visualization definition.
				O User should be allowed to select and customize visualization components based on the needs.
CIO-AE 19.21	CIOP	CIO-Platform	Analytics Engine	System should have Built-in What-if Analytics feature of the platform
CIO-AE 19.22	CIOP	CIO-Platform	Analytics Engine	System should provide the capability to manage the emergencies and in-turn reducing risks, salvaging resources to minimize damages and recovering the assets that can speed up recovery.
CIO-AE 19.23	CIOP	CIO-Platform	Analytics Engine	System should take proactive decisions that help minimize risks and damages, the solution should provide BI and Simulation systems as part of the Decision Support System.
CIO-AE 19.24	CIOP	CIO-Platform	Analytics Engine	System should help simulate what if scenarios. It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/3D map. The solution should help build the list of assets, their properties, location and their interdependence through an easy to use Graphical User Interface.
CIO-AE 19.25	CIOP	CIO-Platform	Analytics Engine	Solution should highlight not only the primary asset impacted but also highlight the linked assets, which will be impacted.
CIO-AE 19.26	CIOP	CIO-Platform	Analytics Engine	Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships
CIO-RE 20.1	CIOP	CIO-Platform	Rule Engine & Optimization	System should have ability to respond to real-time data with intelligent & automated decisions
CIO-RE 20.2	CIOP	CIO-Platform	Rule Engine & Optimization	System should provide an environment for designing, developing, and deploying business rule applications and event applications.
CIO-RE 20.3	CIOP	CIO-Platform	Rule Engine & Optimization	System should be able to deal with change in operational systems, which has directly related to the decisions that operators are able to make.
CIO-RE 20.4	CIOP	CIO-Platform	Rule Engine & Optimization	System should have at-least two complementary decision management strategies: business rules and event rules.
CIO-RE 20.5	CIOP	CIO-Platform	Rule Engine & Optimization	System shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions
CIO-DEM 21.1	CIOP	CIO-Platform	Digital Evidence Management	System shall provide Digital Evidence Management for critical events and incidences with provision for long term tamper proof data preservation so as to make it admissible in the court of law.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DEM 21.2	CIOP	CIO-Platform	Digital Evidence Management	System should be able to package related evidence documents, video clips, and audio clips and create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters.
CIO-DEM 21.3	CIOP	CIO-Platform	Digital Evidence Management	System should be preserved in disk based storage systems that are tamper proof with hardware WORM and self-healing to ensure that integrity and quality of evidence is maintained as per requirements of the judiciary.
CIO-DEM 21.4	CIOP	CIO-Platform	Digital Evidence Management	System should ensure fault free functioning and data integrity.
CIO-MA 22.1	CIOP	CIO-Platform	Mobile Access	The platform should facilitate native mobile applications (Android, iOS) to visualize the status and control specific actions of the system that deployed across DSIR.
CIO-MA 22.2	CIOP	CIO-Platform	Mobile Access	The platform should provide Integrated Mobile Application for Android and iOS, for capturing real-time information from the field response team using Mobile Standard Operating Procedure.
CIO-MA 22.3	CIOP	CIO-Platform	Mobile Access	System should be able to acknowledge the incident and provide real time updates from the incident site.
CIO-MA 22.4	CIOP	CIO-Platform	Mobile Access	System should have provision of both App based as well Web based as the case may be for role based unrestricted access to central CIOP.
CIO-MA 22.5	CIOP	CIO-Platform	Mobile Access	The platform should provide Integrated Mobile Application for Android and iOS, for public services.
CIO-LOG 23.1	CIOP	CIO-Platform	Logger	System should provide the ability to collect and store data in order to provide reports for transactional and business events.
CIO-LOG 23.2	CIOP	CIO-Platform	Logger	System should track user activities on the system for reporting purposes.
CIO-LOG 23.3	CIOP	CIO-Platform	Logger	System should monitor all mission-critical infrastructure components – including applications, services, operating systems, network protocols, systems metrics, and network infrastructure.
CIO-LOG 23.4	CIOP	CIO-Platform	Logger	System should define and handle multiple data sources in order to generate graphs to be evaluated as performance result.
CIO-LOG 23.5	CIOP	CIO-Platform	Logger	System should manage ticket generation upon incident or service request
CIO-LOG 23.6	CIOP	CIO-Platform	Logger	System should store information about transactional data to monitor components interaction, activities and performances and application errors
CIO-LOG 23.7	CIOP	CIO-Platform	Logger	System should be able to store information about transactional data to monitor components interaction, activities and performances and application errors
CIO-CA 24.1	CIOP	CIO-Platform	Citizen Mobile App	The system shall have a separate mobile app for citizen who can raise a request through a mobile app and track the ticket.
CIO-CA 24.2	CIOP	CIO-Platform	Citizen Mobile App	System shall be easy to use. There shall be a single button to dial the SOS
CIO-CA 24.3	CIOP	CIO-Platform	Citizen Mobile App	System should have shortcut key to send alerts to Emergency Control Center without typing anything
CIO-CA 24.4	CIOP	CIO-Platform	Citizen Mobile App	The system shall allow the users to allow the camera access to record and send the details
CIO-CA 24.5	CIOP	CIO-Platform	Citizen Mobile App	System shall allow the citizen users to connect with the City Emergency Operations for assistance during emergency
CIO-CA 24.6	CIOP	CIO-Platform	Citizen Mobile App	The system should have Email and SMS gateway integration to update the citizens
CIO-CA 24.7	CIOP	CIO-Platform	Citizen Mobile App	System should have auto Push notification system enabled to update the citizens using mobile apps

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-CA 24.8	CIOP	CIO-Platform	Citizen Mobile App	System shall be available on latest versions of iOS, Android and be upgradable
CIO-CA 24.9	CIOP	CIO-Platform	Citizen Mobile App	System should be able to download the app from Application Store or link should be provided on official website of the Department to download the app from Application Store.
CIO-HD 25.1	CIOP	CIO-Platform	Helpdesk	The system must provide flexibility of logging, viewing, updating and closing incident manually via web interface.
CIO-HD 25.2	CIOP	CIO-Platform	Helpdesk	The system must support ITIL (Information Technology Infrastructure Library) processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes
CIO-HD 25.3	CIOP	CIO-Platform	Helpdesk	System must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools
CIO-HD 25.4	CIOP	CIO-Platform	Helpdesk	The system must be able to provide flexibility of incident assignment based on the workload, category, location etc.
CIO-HD 25.5	CIOP	CIO-Platform	Helpdesk	System must allow easy definition on multiple escalation levels and notification to different personnel via window GUI or console with no or minimum programming
CIO-HD 25.6	CIOP	CIO-Platform	Helpdesk	The system must support tracking of SLA (service level agreements) for call requests within the help desk through service types
CIO-HD 25.7	CIOP	CIO-Platform	Helpdesk	System could be integrated with CRM/ITIL tools. Incident request ticket shall be generated and mapped or assigned to an associated resource to resolver or support. Incident ticket lifecycle need to be completely managed and monitored
CIO-SI 26.1	CIOP	CIO-Platform	SCADA Integration	System should be integrated with CIOC
CIO-SI 26.2	CIOP	CIO-Platform	SCADA Integration	System should exchange data through JSON format
CIO-SI 26.3	CIOP	CIO-Platform	SCADA Integration	System should use ESB or IoT API Adapter for consuming the web services from SCADA application.
CIO-SIOT 27.1	CIOP	CIO-Platform	Social IOT Integration	System should provide integration of the Incident Management application with the social media.
CIO-SIOT 27.2	CIOP	CIO-Platform	Social IOT Integration	System should provide intelligence based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.
CIO-SIOT 27.3	CIOP	CIO-Platform	Social IOT Integration	System should extract messages and display it in an operational dashboard.
CIO-SIOT 27.4	CIOP	CIO-Platform	Social IOT Integration	System should be able to correlate the extracted message from the social media with existing other events and then should be able to initiate an SOP.
CIO-SIOT 27.5	CIOP	CIO-Platform	Social IOT Integration	System should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started.
CIO-SIOT 27.6	CIOP	CIO-Platform	Social IOT Integration	System should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.
CIO-APP 28.1	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	Platform should integrate with eGovernance and Utility ERP Solution in such a way that it can operate in modes as follows:
				o Emergency Mode
				o Disaster Mode
				o Business as Usual Mode
				o Degraded Operations Mode
				o Normal Mode

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				o The Business As-Usual Mode in CIOC is expected to help cities improve operation performance while interlinked to the ERP and other city applications.
CIO-APP 28.2	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	Platform needs to integrate with Accounts module of ERP in such a way that it delivers the following functionalities -
				o View the spending pattern across the budget heads with a facility to drill down. The view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly, quarterly and yearly views available
				o View area wise budget spent across the city on a city map. Accounts View the feeds received from ERP system on the city map.
CIO-APP 28.3	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	Platform should integration with Assets module of ERP in such a way that it delivers the following functionalities –
				o View geo tagged movable assets on the map based on their classification.
				O View non-civic infrastructure assets on the map based on their classification.
				O View civic infrastructure assets on the map based on their classification.
CIO-APP 28.4	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	Platform should be integrated with Citizen Centric services module of ERP in such a way that it delivers al the functionalities of ERP, eGov and other city applications.
CIO-APP 28.5	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	System should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly, quarterly and yearly views available.
CIO-APP 28.6	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	View turnaround times for issuance of certificate on the city map. The view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly, quarterly and yearly views available.
CIO-APP 28.7	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	View the aggregate transactions performed at a given civic center on the city map. The view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly, quarterly and yearly views available.
CIO-APP 28.8	CIOP	CIO-Platform	eGovernance and Utility ERP Integration	View the rating of civic centers based on collections, services offered and staff availability on the city map. The view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly, quarterly and yearly views available.
CIO-IF 29.1	CIOP-AM	CIO-Platform	Integration Framework	System should facilitate SOAP / REST based interfacing technique to leverage the real-time point-to-point synchronous integration mode with external or third-party systems.
CIO-IF 29.2	CIOP-AM	CIO-Platform	Integration Framework	System should facilitate Message based interfacing technique to leverage asynchronous integration mode.
CIO-IF 29.3	CIOP-AM	CIO-Platform	Integration Framework	Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer
CIO-IF 29.4	CIOP-AM	CIO-Platform	Integration Framework	System should facilitate to integrate data in batch mode, frequency and schedule of data exchange should be configurable.
CIO-IF 29.5	CIOP-AM	CIO-Platform	Integration Framework	System should have capabilities to receive input message in heterogeneous formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different clients as per formats applicable
CIO-IF 29.6	CIOP-AM	CIO-Platform	Integration Framework	Solution should support the following integration security standards
				Authentication
				Authorization

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				Encryption
				Secure Conversation
CIO-IF 29.7	CIOP-AM	CIO-Platform	Integration Framework	System should have the ability to integrate devices using their APIs into this platform. For example, if the City wants to deploy Smart Parking solution, this platform should have the ability and provision to write adaptors, which interface with the parking sensors or management software of the parking sensors to collect parking events, data, alerts, and notifications from the devices and their software managers
CIO-IF 29.8	CIOP	CIO-Platform	Integration Framework	System should allow integration of business process in ERP workflows like property tax collection, etc.
CIO-IF 29.9	CIOP	CIO-Platform	Integration Framework	The platform should have the capability to retrieve data directly from any urban systems like ERP, eGovernance, SCADA, IOT by following standard security systems and API mechanism
CIO-IF 29.10	CIOP	CIO-Platform	Integration Framework	The platform should also have the access to read data directly from a set of databases (HBase, MongoDB, Oracle, Cassandra, MySQL, etc.)
CIO-IF 29.11	CIOP	CIO-Platform	Integration Framework	The platform should also have access to read/write data from application database through API services
CIO-IF 29.12	CIOP	CIO-Platform	Integration Framework	System should be able to read all types of data including flat CSV files, Excel files, Text files, etc.
CIO-IF 29.13	CIOP	CIO-Platform	Integration Framework	System should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols
CIO-IF 29.14	CIOP	CIO-Platform	Integration Framework	The platform should support real-time data aggregation for event-detection and this should be configurable via SOP's, API services
CIO-IR 30.1	CIOP	CIO-Platform	Integration Requirement	Platform would combine various data feeds from all city systems and further process information out of these data feeds to provide actionable insights, alert and notifications in near real time. Web based Dashboard can provide city management capabilities and can provide holistic view of the DSIR Operations and services.
CIO-IR 30.2	CIOP	CIO-Platform	Integration Requirement	System should facilitate Integration approach for individual subsystems to be done using data ingestion service of CIOP
CIO-IR 30.3	CIOP	CIO-Platform	Integration Requirement	System should enable REST API based service Integration: Event/data can be pushed from the subsystem using REST Services exposed by CIOP
CIO-IR 30.4	CIOP	CIO-Platform	Integration Requirement	System could share data in flat file csv format, which can be consumed by CIOP for further actions.
CIO-IR 30.5	CIOP	CIO-Platform	Integration Requirement	System should facilitate JDBC based integration for systems if relational tables are accessible.
CIO-IR 30.6	CIOP	CIO-Platform	Integration Requirement	System should support MQ Based integration if subsystem is capable MQ based integration
CIO-IR 30.7	CIOP	CIO-Platform	Integration Requirement	System should facilitate to develop integration adaptors in cases where controlling of subsystem is needed or data massaging is needed
CIO-IR 30.8	CIOP	CIO-Platform	Integration Requirement	System should support MQTT Based integration if subsystem is capable MQTT based integration
CIO-IR 30.9	CIOP	CIO-Platform	Integration Requirement	CIOP should act as a common operation platform and based on the integration with the subsystem, if the subsystem provides capabilities to be managed externally via REST / Web services. CIOP can be configured to manage the components integrated with CIOP.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-IR 30.10	CIO-P	CIO-Platform	Integration Requirement	CIO-P should provide near real time data of various assets / Subsystem for near real-time monitoring at the CIOC. Assets can be selected by point and click. Near real time information of the asset is displayed, and along with this standard report (24 * 7) reports will be displayed.
CIO-IR 30.11	CIO-P	CIO-Platform	Integration Requirement	Platform should leverage the information provided by different devices/ platforms & various Departments and providing a comprehensive response mechanism for the day-to-day challenges across DSIR. The proposed CIO-P shall be a fully integrated portal-based solution that can provide seamless incident – response management, collaboration and geo-spatial display.
CIO-IR 30.12	CIO-P	CIO-Platform	Integration Requirement	Platform should provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Thus, the CIO-P provides a Common Operating Procedure of various events in real-time on a unified platform with the means to make collaborative and consultative decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.
CIO-IR 30.13	CIO-P	CIO-Platform	Integration Requirement	Platform should be envisioned to provide a high processing power and adequate data storage with a high-performance information highway to provide process information in real time and serving decision support system. The CIO-P should also provide portability to meet changing City scenario.
CIO-IR 30.14	CIO-P	CIO-Platform	Integration Requirement	Platform should have a functionality to provision data storage and processing power of the platform adequately to meet the system design and functionality to be achieved.
CIO-IR 30.15	CIO-P	CIO-Platform	Integration Requirement	Platform should be capable of seamless integration (API based) with various government and emergency services like disaster and emergency services, utility services etc., the proposed solution should support recording of external mobile video feeds, data communication.
CIO-IR 30.16	CIO-P	CIO-Platform	Integration Requirement	The Platform shall support event logs including operator's onscreen activities, voice & video events, etc. for further analysis, training and similar activities.
CIO-IR 30.17	CIO-P	CIO-Platform	Integration Requirement	System should provide real-time analysis of individual events and also a measure of the incidents for each of the silos integrated on the platform, which intended to help the decision makers.
CIO-IR 30.18	CIO-P	CIO-Platform	Integration Requirement	Platform should support & have the ability for adding more/new layers of solutions seamlessly with minimal effort as and when required. On platform the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions. The system shall provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users.
CIO-IR 30.19	CIO-P	CIO-Platform	Integration Requirement	Platform would have provisions for monitoring and control of all the Smart City Applications
CIO-IR 30.20	CIO-P	CIO-Platform	Integration Requirement	System should facilitate to receive inputs or feeds from different components of Smart City Solutions for CIOC video wall for monitoring, tracking and decision support purpose on real time basis supported with GIS technology. Further, operators shall be working on their respective monitors for assessing the inputs and triggering actions at ground level.
CIO-KPI 31.1	CIO-P	CIO-Platform	Key Performance Indicator	Platform would have integrated view of all the smart initiatives undertaken by DMICDC with focus to serve as a decision support engine for city administrator in day-to-day operations during exigency situation
CIO-KPI 31.2	CIO-P	CIO-Platform	Key Performance Indicator	Platform should leverage on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. CIO-P shall be a fully integrated, web-based platform that provides seamless incident – response management, collaboration and geo-spatial display.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-KPI 31.3	CIOP	CIO-Platform	Key Performance Indicator	Platform should facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The smart city operations center shall be accessible by operators and concerned authorized entities with necessary authentication credentials.
CIO-KPI 31.4	CIOP	CIO-Platform	Key Performance Indicator	Platform should provide 24*7 City Surveillance System for effective management of the city
CIO-KPI 31.5	CIOP	CIO-Platform	Key Performance Indicator	Platform should leverage state of the art technology to effectively manage city operations
CIO-KPI 31.6	CIOP	CIO-Platform	Key Performance Indicator	Platform would be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Sewerage/ Drainage system, Disaster Mgmt. System, etc.
CIO-EAI 32.1	CIOP	CIO-Platform	Enterprise Application Integration	Platform should support integration of all supportive COTS/other applications that is being used in Silos through API services
CIO-EAI 32.2	CIOP	CIO-Platform	Enterprise Application Integration	Platform should integrate all SCADA related applications.
CIO-EAI 32.3	CIOP	CIO-Platform	Enterprise Application Integration	Platform should integrate necessary 3rd party applications which is planned to use for city services to provide better services for CIOC operations.
CIO-EAI 32.4	CIOP	CIO-Platform	Enterprise Application Integration	Platform should process data from enterprise applications that being used for City services.
CIO-FI 33.1	CIOP	CIO-Platform	Integration of Future IT initiatives	Platform should be scalable and modular in structure and shall be able to integrate other future IT initiatives for DSIR.
CIO-TP 34.1	CIOP	CIO-Platform	Integration and testing phase	Platform should be integrated with data feeds of the various Smart City systems envisaged under DSIR.
CIO-DB 35.1	CIOP	CIO-Platform	Database	MSI should propose their preferred database for SQL/NO-SQL requirement as per solution requirement
CIO-ESB 36.1	CIOP	CIO-Platform	Message Bus	MSI can propose integrated ESB functionalities with command center application or can use common ESB bus for standardized integration.
CIO-IOC-37.1	BI/Analytics	Business Intelligence & Analytics	City Integrated Operation Centre	It shall make use of cross-system data analytics from historian and real-time information received from independent systems through smart city platform to aid in the operations and management of city services.
CIO-IOC-37.2	BI/Analytics	Business Intelligence & Analytics	City Integrated Operation Centre	The system shall have ability to synthesize, analyze and integrate data from all City systems and should provide analytical insights to city integrated operation center for running real time sensors and to decision makers for policy making and optimizing decisions.
CIO-IOC-37.3	BI/Analytics	Business Intelligence & Analytics	City Integrated Operation Centre	The Analytics system shall be capable of carrying out business intelligence as well as real time analytics for city systems where it shall develop insight into possible future conditions or events. Analytics shall measure the efficacy of services delivered and also help operators and city personnel to test scenarios.
CIO-CS-38.1	BI/Analytics	Business Intelligence & Analytics	Citizen services	System to have the capability to analyze traffic movement assessment using data received from sources such as GIS data, traffic data as well as from other sources.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-CS-38.2	BI/Analytics	Business Intelligence & Analytics	Citizen services	System to have a capability to analyze traffic pattern detection, which can aid in modifying or adjusting the pre-configured traffic signaling process with continuous change in patterns as per the traffic congestions observed in areas and align the signaling accordingly.
CIO-CS-38.3	BI/Analytics	Business Intelligence & Analytics	Citizen services	System to have the facility to forecast traffic density by location and time of day and predict traffic control man power required at various signals and locations/junctions within the city.
CIO-CS-38.4	BI/Analytics	Business Intelligence & Analytics	Citizen services	System to have the facility for segmentation and profiling of repeat traffic offenders by integrating with echallan as well as traffic system of police to enhance the traffic management by using predictive analytics techniques.
CIO-CS-38.5	BI/Analytics	Business Intelligence & Analytics	Citizen services	System to have a capability to estimate the possible bottlenecks/issues/challenges across the city from a security stand point by analyzing the real-time data streaming from video surveillance system and carry out required analytics for forecasting the same using various techniques. (AI or any other)
CIO-CS-38.6	BI/Analytics	Business Intelligence & Analytics	Citizen services	System to have a facility for real time streaming analytics on tweets and social media events, blogs, grievances and discussion portal with data quality and content categorization
CIO-PS-39.1	BI/Analytics	Surveillance	Public Security	System to have a facility to; - Enable the law enforcement to identify the area of security concerns - Forecast the man power required for surveillance in high risk area - Identify hidden areas of security concerns - Profile each area based on the type of predominant crime
CIO-PS-39.2	BI/Analytics	Surveillance	Public Security	System to have a facility to dynamically through real time surveillance data sense the citizen environment and mitigate government service disruptions through social media and other citizen data. The same should also integrate/interact with access system to provide enhance analytics on personnel behavior as well as predict its future action plan as per his behavior
CIO-SM-40.1	BI/Analytics	Business Intelligence & Analytics	Social Media	System to have a facility to; - Constantly monitoring and perform scouting on social media (Facebook/twitter, etc. handle of DICDL) for suggestions/feedback/solutions - Capture and manage grievances and feedback to improve efficiency and the turnaround time of citizen grievances - Policy Intervention Planning as well as keep a tab on top issues/ problems - Identify Topic and Identify sentiment –Positive/Negative/Neutral (sentimental analysis)
CIO-SOL-41.1	BI/Analytics	Business Intelligence & Analytics	Solution	System to facilitate with provisioning data analytics lab environment to quickly establish analytics use cases across various components of smart city involving but not limited to statistical analysis, data mining, predictive modelling/analytics, machine learning, time-series forecasting, text analytics, content categorization, etc.
CIO-WM-42.1	BI/Analytics	Water Management	Water Quality Analytics	System to have facility for; - Real time monitoring and streaming analytics based event generation on turbidity, pH & chlorine levels at Reservoir / WTP plants, flow rate and pressure monitoring, as well as any other requirements of DICDL. - Real time monitoring of chlorine level at reservoirs, storage tanks, etc. - Timely trigger to depute resources/personnel on how much local chlorine boosting to be done in case of chlorine decay during distribution (preventive actions) - Real time monitoring of cleaning up of reservoirs and alert in case of failure in cleaning - Analysis of correlation between multiple water quality parameters as well as carrying out any preventive actions if the case may be.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				- Understand trends of water quality across the reservoir and analyze the effectiveness of corrective actions. - Analyze the root cause of certain water quality changes and suggest corrective actions. - Analyze the root cause of water drain/flow at various levels using multiple analytics techniques to avoid wastage of water and preventive actions before the breakdown. - Predictive models for expected water quality degradation - Statistical models for water quality and cost of quality treatment to optimize raw material cost
CIO-WM-42.2	BI/Analytics	Water Management	Water Availability Forecasting & Planning	System to have facility for; - Real time monitoring of inflow, outflow & water level at reservoirs, WTP's and Intermediate chainage of the pipeline as well as other locations within the city as the case may be. - Real time monitoring of schedule adherence and duration adherence of water distribution - Area-wise / Meter wise Hierarchical forecasting for short / medium / long-term demand and supply planning, generate alerts for demand variations on actual and actual vs forecast. - Timely trigger to depute personnel in case of deviations/abnormalities, etc. - Measuring flow variations in various branches - Deploying rules for provisioning of water to industrial/residential locations at different time intervals as well as different cost as desired by DICDL in time to time basis.
CIO-WM-42.3	BI/Analytics	Water Management	Energy Efficiency Analytics	System to have facility for; - Real Time Condition Monitoring of Water / Waste Water Pump - Intelligent algorithms using data mining techniques that will predict and detect faults such as vibration, cavitation, functional loss such as pressure loss or flow loss etc. - Integration of variable speed drive with connected/integrated technology (IoT, API's, etc.) using intelligent sensors, SCADA systems, PLC's and streaming analytics capabilities for adjustment of set points. - Reliability modelling taking into consideration pump and its component historical failure with heat map across the number of pumps to capture the risk
CIO-WM-42.4	BI/Analytics	Water Management	Waste water treatment analytics	System to have facility for; - Real time monitoring of streaming analytics based event generation on various quality parameters of Waste water treatment plants. - Timely trigger to depute required personnel on how much raw material to be added which would facilitate the control of process output in acceptable levels. - Real time generation of alarms and SMS notifications in case of exceptions - Predictive modelling including Cluster Analysis for correlation between multiple levels of water quality parameters across the stages and the target output water quality measurement - Understand trends of water quality across the reservoir and analyze the effectiveness of corrective actions. - Analyze the root cause of certain water quality changes and suggest corrective actions. - Analyze and identify problems like sedimentation, clogging of individual pumps and load fluctuations, etc.
CIO-EM-43.1	BI/Analytics	Energy Management	Solution	System to have a facility to provision proven intelligence system for planning and asset maintenance for Power Grid which.
CIO-EM-43.2	BI/Analytics	Energy Management	Power outage	System to have facility where; - Depending on the data shared from power grid it can generate various reports related to outage, document its recovery in real-time and isolate

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
			Management	locations of physical damage. (if any) - Gathering data from power generation/transmission as well as from consumer utilization and help in analysis of demand and supply along with the capacity of the power grid. Can also assist with various other analysis on the power distribution and demand supply characteristics. - Analysis of the peak/non-hours of usage and changing rates of the power supply as per the decision/directions given by DICDL which should be communicated to power generation and supply agencies using integrated/connected systems. (variable rate power supply at different time duration as well as type of requirement).
CIO-EM-43.3	BI/Analytics	Energy Management	Prevention of Technical and commercial losses	System to have facility for; - Loss analysis for different groups and categories of consumers - Accounting and auditing at Feeder level, Distribution Transformer level and DCU level. - Given the voltage and energy information for already deployed or planned deployment of smart meters, the software solution should be able to identify the meters who are liable for stealing energy
CIO-EM-43.4	BI/Analytics	Energy Management	Energy performance forecasting	System to have facility for collection of data from utilities on regular time interval to help the analyst in understanding the pattern of energy usage as well as other requirement that may arise as per the real time and legacy data shared by DICDL. The seasonality pattern observed from the legacy data should be able to help in looking for when and in which region the demand will be high or low.

3.1.5. Basic surveillance solution

The surveillance system is design to cover public area like, public roads, schools, hospital not only for post analysis but getting proactive alerts to Command center using advance video analytics. The surveillance system is design to cover public area like, public roads, schools, hospital not only for post analysis but getting proactive alerts to Command center using advance video analytics.

GENERAL REQUIREMENTS

- The system design should allow seam less interface with central VMS system and other relevant system for analytics and monitoring.
- All components to be connected to the network via access switches through at least Ethernet connection unless stated otherwise or components selected by the MSI require a higher bandwidth.
- H.264 or better encoding format to be used for recording all cameras and dual stream feature shall be available in all cameras.
- The system to be designed to provide next to real time video footage, still images which shall be used as evidence in case of any event for forensic analysis.
- Resolution, lenses, aperture and shutter speed settings, sensor, scanning technique and encoding to be selected for clear representation of the captured scene on still images.
- The system should support multi-cast streaming video to allow concurrent users to view the same video stream
- Server based architecture to be considered for design and implementation of Surveillance system at DSIR
- Surveillance system should be scalable for future enhancements with addition of different types of cameras and carrying out video analytics on them.
- The cameras should comply with open platform surveillance system, without limitations to image quality or functionality.

- Server based surveillance architecture should support seam less integration with third party cameras and Video analytics software applications

Broad Requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-AS 1.0	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Redundancy	It must ensure predictability of infrastructure in different operating scenarios. The technology and solution of the components shall be selected with high MTBF and Low MTTR.
CIO-AS 1.1	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Availability	It must ensure higher uptime by providing sufficient redundancies (Inbuilt) so that maintenance can be carried out without impacting running system. It measures the security resilience of Data Centre/Server room.
CIO-AS 1.2	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Resilience	Resiliency is the ability of a server, network, storage system, or an entire data center, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.
CIO-AS 1.3	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Modularity	It must ensure use as needed and achieve lower PUE's in lower load requirement in the commencement of DC/server room operations and also helps in modular addition of capacities.
CIO-AS 1.4	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Scalability	As requirement of field equipment's grow, it must ensure smooth and regular horizontal and vertical upgrade of any application hardware as requirements grows.
CIO-AS 1.5	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Scalability	The solution must involve four major components including Cameras, VMS (Video management software), Video analytics and the Video transmission network.
CIO-AS 1.6	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Scalability	The system must allow seam less interface with server based surveillance solution at Various Buildings, central VMS system and other relevant system for analytics and monitoring.
CIO-AS 1.7	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Scalability	The system design and integration provided a next to real time video footage, still images which shall be used as evidence in case of any event for forensic analysis.
CIO-AS 1.8	CCTV & Security Surveillance systems	CIO- Attributes of Surveillance	Scalability	VMS must support seam less integration with third party cameras, Video analytics software applications and other required applications/systems.
CIO- SD- 1.0	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The MSI must offer complete solution for high-definition video encoding, recording, and display, designed as an end-to-end system for the demands of professional IP video security.
CIO- SD- 1.1	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	System must be Scalable to accept an unlimited number of HD and megapixel cameras, the system must be intelligent, yet easy-to-use approach to video security that provides greater control, enhanced operational flexibility, improved management, and expanded recording, archiving, and integration capabilities compared to anything else available.
CIO- SD- 1.2	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system must be designed for reliability through fault-tolerant, distributed architecture, and multiple levels of redundancy.
CIO- SD- 1.3	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The VMS must provide an open interface that facilitates the creation and deployment of user interface plug-ins including mapping, video information overlays, access control, and license plate recognition.
CIO- SD- 1.4	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	Video capabilities
CIO- SD- 1.5	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	1. Support recording of MJPEG, MPEG-4 and H.264 IP video streams

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.6	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	2. Support megapixel video cameras up to 28 Megapixel resolution
CIO- SD- 1.7	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	3. Support for ONVIF S and G profiles
CIO- SD- 1.8	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	Analytic capabilities integral to VMS
CIO- SD- 1.9	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	1. Motion - Detection of objects that move within, enter, or exit a scene and triggering an event
CIO- SD- 1.10	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	2. Alarm – Detection of physical alarms from cameras within the system, triggering an event
CIO- SD- 1.11	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	3. Analytic – Detection of analytic events from cameras
CIO- SD- 1.12	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system must be built upon open, industry standards and facilitates integration with IT infrastructures and other digital and analog systems. Towards this, the system provides an API/SDK that is capable of being used at a level consistent with a full-featured gateway. The gateway provides a RS-232 ASCII interface, Ethernet interface, and the ability to create custom plug-ins to the system user interface.
CIO- SD- 1.13	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system must support for IP cameras from multiple manufacturers
CIO- SD- 1.14	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system does not limit resolution, frame rate, or number of standard-resolution or megapixel cameras that can be recorded, viewed, and managed on the system.
CIO- SD- 1.15	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	Multiple users must be able to simultaneously view the same camera view or sequence. The system must use multi-cast streaming video to allow multiple users to view the same video stream, though not necessarily synchronized with each other, without affecting the bandwidth of the network.
CIO- SD- 1.16	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system must support sequences running on any network monitor. Alarms or user intervention are capable of interrupting a running sequence
CIO- SD- 1.17	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system must allow for programming of alarms and associated incoming alarms with related parts of the system. Alarms and other triggers can be grouped into system events. System events must be configured using Boolean logic that requires multiple entities to be true before a system event is triggered.
CIO- SD- 1.18	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	Individual, group, or all alarms must be disabled by special sequences, which can be initiated by the operator or automatically by time/day/date.
CIO- SD- 1.19	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system logs all alarms and events must be in the system manager database.
CIO- SD- 1.20	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system provides for virtual matrix functionality, leveraging the IP network to switch any camera to any monitor as well as transmit alarms and other system messages to any console on the network.
CIO- SD- 1.21	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system utilizes a system manager to provide user and database management.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.22	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system manager software must support database failover when using two servers by maintaining a continuously synchronized duplicate of the main database at all times.
CIO- SD- 1.23	CCTV & Security Surveillance systems	Surveillance	SYSTEM DESCRIPTION	The system must provide multi-level diagnostics of each component in all critical areas. These diagnostics must be reported to a diagnostic console for processing. The diagnostic data must be capable of being scripted into actionable events within the system. In addition, standard SNMP messages must be capable of being mined by network diagnostic systems such as Open View and others for diagnostic traps and operational data.
CIO- SD- 1.24	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	The following functional capabilities are considered essential for the CCTV System described in this specification:
CIO- SD- 1.25	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	Camera Monitoring
CIO- SD- 1.26	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	Camera Controlling
CIO- SD- 1.27	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	Have an extremely high degree of reliability.
CIO- SD- 1.28	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	Intuitive operation
CIO- SD- 1.29	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	Flexibility for future development.
CIO- SD- 1.30	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	Reliable recording.
CIO- SD- 1.31	CCTV & Security Surveillance systems	Surveillance	SYSTEM CAPABILITIES	High Quality Image Storage
CIO- SD- 1.32	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system should be-based for easy setup and maintenance.
CIO- SD- 1.33	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must support browser-based / GUI / Management Software based administration interface which provides management capabilities, locally and remote, without an installed desktop
CIO- SD- 1.34	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must support the ability of modular plug-ins.
CIO- SD- 1.35	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must be designed for reliability through fault-tolerant, distributed architecture, and multiple levels of redundancy.
CIO- SD- 1.36	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must provide predictable scalability and modular design.
CIO- SD- 1.37	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must support up to 6 monitors per workstation, each driven by independent CPUs, displaying up to 16HD streams per monitor.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.38	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system workstations must be capable to utilize a 3D mouse and programmable keyboard accessories, and keyboard shortcuts for common operations, to maximize operator control.
CIO- SD- 1.39	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system needs to provide an open interface that facilitates the creation and deployment of User Interface plug-ins including mapping, video information overlays, Access control, and license plate recognition.
CIO- SD- 1.40	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must support recording of MJPEG, MPEG-4 and H.264 IP streams.
CIO- SD- 1.41	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must support Megapixel video streams up to 28 Megapixel.
CIO- SD- 1.42	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system is to have a fully open architecture with support for both IP-specific camera as well as cameras with ONVIF S.
CIO- SD- 1.43	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must be capable to Aggregate independent VMS deployments across networks and manage all video through a single system while preserving local operation.
CIO- SD- 1.44	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system will be able to be viewed, managed, and played back through a single user interface
CIO- SD- 1.45	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must run on standard commercial off-the-shelf processors and hardware with predictable performance characterized by benchmark information on manufacturer supplied specifications.
CIO- SD- 1.46	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system will support Analytics at no additional licensing cost.
CIO- SD- 1.47	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	The IP video management system must indicate system performance and operation status utilizing a variety of reports including csv and pdf formats.
CIO- SD- 1.48	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client software must create and assign tags, organizing system resources as administrators or operators decide.
CIO- SD- 1.49	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client software must provide the capability of running a client application in addition to the video management system.
CIO- SD- 1.50	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client software, at minimum, to include advanced search capabilities for camera and recordings.
CIO- SD- 1.51	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client software will utilize an Investigation mode which enables operators to synchronize video playback and export investigative playlists covering scenes of interest in forward or reverse at speeds up to 128 times normal playback.
CIO- SD- 1.52	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	A client computer with system compatible software must be the user interface for viewing one or more systems. Live and recorded video and current event video must be displayed on any client computer using a proper login and password. The client computer must be able to connect to an unlimited number of recorders simultaneously to display live and recorded video.
CIO- SD- 1.53	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client Software must not require a license and be available to be installed on as many clients as required by the user.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.54	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client Software access will be User Account Controlled such that an operator must enter their credentials and will only have functionality prescribed to by the set of Roles assigned to their user account by their administrator. User Roles must limit the ability to access live or recorded video as well as the ability to export video and other standard client operations.
CIO- SD- 1.55	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client Software to allow multiple monitor support for up to 6 displays per client workstation, providing virtual matrix functionality with the use of enhanced decoders.
CIO- SD- 1.56	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client Software must allow video streams to be selectable from a system tree on an individual camera, individual system, client defined local groups, or from pre-defined recorder based groups.
CIO- SD- 1.57	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client cells, at minimum, have the ability to include system management, live, and search options. Tabs can be displayed simultaneously on the client.
CIO- SD- 1.58	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Systems cells will, at minimum, display connection status, system names, and custom categories. This tab at minimum will additionally allow: a. Mapping plug-ins b. Card Access plug-ins c. Web Browser plug-ins d. Live video e. Recorded video f. Mission control console g. eConnect plug-ins h. ANPR plug-ins i. Synchronized video live and recorded (investigations) j. Screen layout select 1, 4, 9, 16 etc. k. Digital Zoom l. User selectable in-video PTZ control m. Quick review from 30 sec, 1 min, 30 min and 1 hour (through keyboard hot buttons) n. Virtual matrix capabilities o. Display recorded video with full VCR controls with an active overlay, (play, fast forward and reverse, and frame by frame). p. Playback available on a time lime format for ease of use
CIO- SD- 1.59	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Video export to any system-accessible media including locally to HDD, CD/DVD, Flash USB device or to network storage.
CIO- SD- 1.60	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Video authentication of exported video via check sum verification.
CIO- SD- 1.61	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Client, at minimum, must support simultaneous playback for up to (9) 1080P and above resolution cameras all synchronized with each other. Also, have the capability to playback non-synchronized cameras at one time in different cells.
CIO- SD- 1.62	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Modular Window Based Client: the client must be comprised of 1 main control panel, which can be hidden, working in unison with a series of windows, each providing a tab-based experience.
CIO- SD- 1.63	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Savable Tabs: any layout of video can be saved as TAB to be later recalled by on operator.
CIO- SD- 1.64	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Dockable Mission Control: the main control panel can be hidden, free-floating or dynamically docked to any open VMS client Window.
CIO- SD- 1.65	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Mission Control Sort: the device list in mission control must be sorted by device name or device ID.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.66	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Mission Control Filter: the device list in mission control can be filtered by the following terms: a. Simple text based filter (matching the device name or device ID) b. Tag based filtering (shows devices matching the intersection of all assigned tags) c. Status based Filtering: show devices with a particular status: 1. Online 2. Offline 3. Recording 4. Not recording 5. On screen 6. not on screen
CIO- SD- 1.67	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Saved Investigations: operators are able to save a current investigation, preserving the associated device list and any created clips for later recall. Saved investigations can be shared with other operator's similar tabs.
CIO- SD- 1.68	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Remote Workspace Push: an operator with appropriate permissions can choose to have a saved workspace sent to one or more operators' clients, causing their system to launch the saved workspace.
CIO- SD- 1.69	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Remote Tab Push: an operator with appropriate permissions can choose to send a saved tab one or more operators' clients, causing their system to launch the saved tab.
CIO- SD- 1.70	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Thumbnail on time bar: when hovering over the time bar, an operator will see a thumbnail representing the contents of the video stream at that point in time.
CIO- SD- 1.71	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Information popup: when hovering over a device, an operator will see a popup that shows the following: a. Device state b. Device name c. device ID d. thumbnail e. associated tags f. IP Address
CIO- SD- 1.72	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Snapshot: an operator will be able to create a quick JPG image of the current frame of video in a cell.
CIO- SD- 1.73	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Digital Zoom: the operator will be able to digitally zoom in on a video stream on live or playback.
CIO- SD- 1.74	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Optical Zoom and Pan Tilt Control: operators will be able to use the mouse, 3D mouse joystick to send commands to cameras that support PTZ mechanism, thereby controlling where the camera is pointing.
CIO- SD- 1.75	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Preset Trigger: operators will be able to trigger a preset action on cameras that are storing presets.
CIO- SD- 1.76	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Drag to Swap: an operator will be able to select the video in one cell, drag that video over another cell and have the system swap the streams.
CIO- SD- 1.77	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Dynamic call-up by ID: operators will be able to start typing a camera ID while having a cell selected to immediately see an input box. Hitting enter will load the associated camera to the cell.
CIO- SD- 1.78	CCTV & Security Surveillance systems	Surveillance	IP VIDEO MANAGEMENT SYSTEM	Last Workspace Recall: the operator will be presented with the last workspace they had opened when they logged back into the system.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.79	CCTV & Security Surveillance systems	Surveillance	Live View and Playback	A list of video and audio sources which users are authorized to access must be displayed.
CIO- SD- 1.80	CCTV & Security Surveillance systems	Surveillance	Live View and Playback	Each video source must indicate a list of current viewers to a user with appropriate permissions.
CIO- SD- 1.81	CCTV & Security Surveillance systems	Surveillance	Live View and Playback	The client computer must be able to connect to an unlimited number of recorders simultaneously to display live and recorded video.
CIO- SD- 1.82	CCTV & Security Surveillance systems	Surveillance	Live View and Playback	The client must allow video streams to be selectable from a system tree on an individual camera, individual system, client defined local groups, or from pre-defined recorder based groups.
CIO- SD- 1.83	CCTV & Security Surveillance systems	Surveillance	Live View and Playback	The client must playback audio associated with video sources for users with the correct permissions.
CIO- SD- 1.84	CCTV & Security Surveillance systems	Surveillance	Live View and Playback	Users must be able to seamlessly switch between live and recorded video on the fly.
CIO- SD- 1.85	CCTV & Security Surveillance systems	Surveillance	Live View	For live view, cells 1/4 the size of the tab or larger will use the primary stream from a video source, and cells smaller than 1/4 the size the tab must use the secondary video stream.
CIO- SD- 1.86	CCTV & Security Surveillance systems	Surveillance	Pan Tilt Zoom (PTZ)	Digital Zoom - An operator must be able to digitally zoom in a video stream in live or playback mode.
CIO- SD- 1.87	CCTV & Security Surveillance systems	Surveillance	Pan Tilt Zoom (PTZ)	Optical Zoom and Pan Tilt Control: Operators must be able to use a mouse or joystick to control PTZ cameras.
CIO- SD- 1.88	CCTV & Security Surveillance systems	Surveillance	Playback	The Client application must enable simultaneous playback for up to (9) synchronized cameras.
CIO- SD- 1.89	CCTV & Security Surveillance systems	Surveillance	Playback	The Client application must have the capability to playback non-synchronized cameras at one time in different cells.
CIO- SD- 1.90	CCTV & Security Surveillance systems	Surveillance	Playback	For viewing recorded video, cells 1/4 the size of the tab or larger must display full-frame rate video, and cells smaller than 1/4 the size of the tab must playback only I-Frames to conserve bandwidth and processing power.
CIO- SD- 1.91	CCTV & Security Surveillance systems	Surveillance	Playback	When hovering over a recorded video time bar, an operator must see a thumbnail representing the contents of the video stream at that point in time.
CIO- SD- 1.92	CCTV & Security Surveillance systems	Surveillance	Playback	Available playback control functions:
CIO- SD- 1.93	CCTV & Security Surveillance systems	Surveillance	Playback	1) date-time selection
CIO- SD- 1.94	CCTV & Security Surveillance systems	Surveillance	Playback	2) synchronized playback of selected cells within a tab
CIO- SD- 1.95	CCTV & Security	Surveillance	Playback	3) play video at normal speed

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
	Surveillance systems			
CIO- SD- 1.96	CCTV & Security Surveillance systems	Surveillance	Playback	4) pause video and advance one frame
CIO- SD- 1.97	CCTV & Security Surveillance systems	Surveillance	Playback	5) pause video and rewind one frame
CIO- SD- 1.98	CCTV & Security Surveillance systems	Surveillance	Playback	6) Fast forward video with speed 8X and above up to 128x
CIO- SD- 1.99	CCTV & Security Surveillance systems	Surveillance	Playback	7) Rewind video with speed 8X and above up to 128x
CIO- SD- 1.100	CCTV & Security Surveillance systems	Surveillance	Playback	8) rewinds video 30 seconds and initiates playback
CIO- SD- 1.101	CCTV & Security Surveillance systems	Surveillance	Playback	9) forward video to live playback
CIO- SD- 1.102	CCTV & Security Surveillance systems	Surveillance	Playback	10) take snapshot of the current frame
CIO- SD- 1.103	CCTV & Security Surveillance systems	Surveillance	Playback	Hovering over a video playback cell with a mouse must display the playback control menu.
CIO- SD- 1.104	CCTV & Security Surveillance systems	Surveillance	Playback	The user must be able to configure a rotating sequence of cameras, allowing the application to cycle through cameras relevant to the operator without intervention.
CIO- SD- 1.105	CCTV & Security Surveillance systems	Surveillance	Playback	The user must be able to configure a sequence of cameras that appear on alarm, allowing the application to cycle cameras when an event or alarm relevant to the user occurs.
CIO- SD- 1.106	CCTV & Security Surveillance systems	Surveillance	Investigations	An investigation mode must be available to provide a 2 x 2 layout with synchronized playback controls, allowing users to fully investigate a scene from multiple angles.
CIO- SD- 1.107	CCTV & Security Surveillance systems	Surveillance	Investigations	The investigation mode must open in a new tab.
CIO- SD- 1.108	CCTV & Security Surveillance systems	Surveillance	Investigations	The investigation mode must enable operators to synchronize video playback and export investigative playlists covering scenes of interest in forward or reverse at speeds from 8 times and above up to 128 times normal playback
CIO- SD- 1.109	CCTV & Security Surveillance systems	Surveillance	Investigations	Users must be able to create playlists from multiple video clips encompassing selected scenes from an investigation.
CIO- SD- 1.110	CCTV & Security Surveillance systems	Surveillance	Investigations	Operators must be able to save a current investigation, preserving the associated device list and any created clips for later recall.
CIO- SD- 1.111	CCTV & Security Surveillance systems	Surveillance	Investigations	Saved investigations must be capable of being shared with other operators' similar tabs.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.112	CCTV & Security Surveillance systems	Surveillance	Investigations	Operators must be able to export individual video clips or entire playlists to the Core application, storing clips relevant to their investigation independent of the system's network video storage for evidentiary safe-keeping and quick access.
CIO- SD- 1.113	CCTV & Security Surveillance systems	Surveillance	Export	An operator must be able to create and export a JPG snapshot image of the current frame of video in a cell.
CIO- SD- 1.114	CCTV & Security Surveillance systems	Surveillance	Export	The Client application must enable video export to any system-accessible media including locally to HDD, CD/DVD, and Flash USB device or to network storage.
CIO- SD- 1.115	CCTV & Security Surveillance systems	Surveillance	Export	Exported video must be subject to check sum verification.
CIO- SD- 1.116	CCTV & Security Surveillance systems	Surveillance	Display	The Client application must have both built in video decoding and the ability control separate hardware video decoders, providing virtual matrix functionality.
CIO- SD- 1.117	CCTV & Security Surveillance systems	Surveillance	Display	The Client application must allow multiple monitor support for up to 6 displays per client workstation, with the use of hardware video decoders.
CIO- SD- 1.118	CCTV & Security Surveillance systems	Surveillance	Display	The Client application must allow the user to configure remote or "shared" displays, providing monitor wall functionality.
CIO- SD- 1.119	CCTV & Security Surveillance systems	Surveillance	Display	The Client application must allow up to 4 1080p, 30 IPs streams (or 120 IPs total) per monitor.
CIO- SD- 1.120	CCTV & Security Surveillance systems	Surveillance	Events	The Client application must an operator to respond to events.
CIO- SD- 1.121	CCTV & Security Surveillance systems	Surveillance	Events	Certain events must be configurable for acknowledgement. a. Acknowledgement options: 1) snooze 2) in process 3) acknowledged b. Authorized operators must have the ability to derive additional information about an event from the core application. c Plug-ins – The Client application must support modular plug-ins for enhanced functionality.
CIO- SD- 1.122	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to maintain database of cameras and recording devices, and provide a convenient Web interface.
CIO- SD- 1.123	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to define administrators level user accounts, which will have the ability to set new roles and subset and permissions, determining the system functions, and devices users can access.
CIO- SD- 1.124	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to allow the ability to assign resources to recording pools through the Admin portal.
CIO- SD- 1.125	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to store videos that operators elect to export from network storage devices for safe keeping.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.126	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to be deployed as an independent database server working with an independent video server to route video traffic to appropriate users as requested.
CIO- SD- 1.127	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to be deployed as a cluster, providing fault tolerance, scalability and load balancing.
CIO- SD- 1.128	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Database Server	Ability to be deployed as a virtual machine.
CIO- SD- 1.129	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Gateway server	The video server must connect the user with the appropriate device i.e.: camera, encoder, decoder as necessary.
CIO- SD- 1.130	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Gateway server	Will be added to modularly, to expand the system's capabilities, or build redundancies within the system to maximize video availability.
CIO- SD- 1.131	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Gateway server	Ability to be deployed on an independent server utilizing the server resources for all its tasks.
CIO- SD- 1.132	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Gateway server	Ability to be deployed on the same server as the database service.
CIO- SD- 1.133	CCTV & Security Surveillance systems	Surveillance	Video Management Server – Gateway server	Ability to be deployed as a virtual machine.
CIO- SD- 1.134	CCTV & Security Surveillance systems	Surveillance	Operator Station	Client Software must be deployable on Standard Windows based machines.
CIO- SD- 1.135	CCTV & Security Surveillance systems	Surveillance	Operator Station	Operator workspace can optionally be extended up to 6 monitors or beyond with use of Enhanced Decoders.
CIO- SD- 1.136	CCTV & Security Surveillance systems	Surveillance	Operator Station	Allows the creation of Operator workspaces, which must define the layout of control panels, windows, and pre-populated camera channels and other content.
CIO- SD- 1.137	CCTV & Security Surveillance systems	Surveillance	Operator Station	Allow users to configure and recall complete workspaces, enabling operators to quickly log in and get the information they need.
CIO- SD- 1.138	CCTV & Security Surveillance systems	Surveillance	Operator Station	Client software must be controlled using a standard mouse and keyboard.
CIO- SD- 1.139	CCTV & Security Surveillance systems	Surveillance	Operator Station	Client software operation must be enhanced utilizing the 3D mouse, or G710 Keyboard.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.140	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Patented six-degrees-of-freedom (6DoF) sensor – Intuitively and precisely navigate digital models or camera positions in 3D space.
CIO- SD- 1.141	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Advanced ergonomic design – The full-size, soft-coated hand rest positions the hand comfortably, and 15 large, soft-touch, function keys allow quick access to frequently used commands.
CIO- SD- 1.142	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Quick View Keys – Fingertip access to 12 views makes it easier to switch cameras.
CIO- SD- 1.143	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Intelligent Function Keys – Easy access to 4 application commands for an optimized workflow.
CIO- SD- 1.144	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	On-Screen Display – Provides a visual reminder of function key assignments on your computer screen.
CIO- SD- 1.145	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	3D Space Mouse Modifiers – Fingertip access to Ctrl, Shift, Alt and Esc keys saves time by reducing the need to move your hand between mouse and 3D Space Mouse.
CIO- SD- 1.146	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Virtual NumPad – Allows direct numerical input into your application using your standard mouse rather than the 3D Space Mouse.
CIO- SD- 1.147	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	The 3D Space Mouse must be part of an integrated system and must be configured so any number can be added to the system. When combined with user interfaces (UIs), network storage managers (NSM's), encoders, IP cameras, and video consoles, the 3D Space Mouse forms an integral part of a complete network-based video control system.
CIO- SD- 1.148	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	The 3D Space Mouse will meet or exceed the following design and performance specifications.
CIO- SD- 1.149	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	The mechanical keys deliver responsiveness and tactile feedback superior to rubber-domed keys. With an actuation force and distance of 45 g and 2 mm, respectively, the keys are optimized for rapid command entry. The keys have been tested for durability to a 50 million cycle life.
CIO- SD- 1.150	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Whisper-quiet key. Quiet, non-clicking key switches, and a built-in dampening ring underneath each keycap significantly reduce the distracting noise coming from your key presses without sacrificing responsiveness.
CIO- SD- 1.151	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Adjustable dual-zone backlighting, illuminated to locate keys—even in low light. The entire keyboard is backlit in white LED light and adjustable to one of four brightness levels, plus "Off". For better visibility of the WASD and arrow keys, their brightness can be adjusted independently from the rest of the keyboard.
CIO- SD- 1.152	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	26-key rollover Multi-key input on the VMS means complex moves can be executed exactly every time. With 26-key rollover, press almost any number of keys plus modifier keys (Control, Alt, Shift) in any order and get exactly what you intended.
CIO- SD- 1.153	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	110 anti-ghosting keys technology on contact. All 110 keys of the VMS are calibrated to prevent anti-ghosting. During the heat of battle, you need to simultaneously run, strafe, select a weapon and open a door. Press and hold multiple keys simultaneously without fear of missing or unexpected key presses.
CIO- SD- 1.154	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	USB pass-through to easily connect your mouse or other USB device via the keyboard Hi-Speed USB pass-through for your computer's USB port.
CIO- SD- 1.155	CCTV & Security Surveillance systems	Surveillance	Keyboard with Joystick	Durable tilt legs stand up under keyboard. The durable tilt legs provide stability and comfort even in your most intense gaming sessions.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- SD- 1.156	CCTV & Security Surveillance systems	Surveillance	ENHANCED VIDEO DECODER	The HD network video decoder is to be fully VMS compatible.
CIO- SD- 1.157	CCTV & Security Surveillance systems	Surveillance	ENHANCED VIDEO DECODER	The HD video decoder needs to support any digital video stream on the network and allow for the decoding of up to 16 simultaneous streams from any video encoder or recorder. It must also allow for simultaneous and independent viewing of both live and recorded video.
CIO- SD- 1.158	CCTV & Security Surveillance systems	Surveillance	ENHANCED VIDEO DECODER	The HD video decoder must decode H.264 in High, Main, or Base profiles, and MPEG-4 encoded video streams.
CIO- SD- 1.159	CCTV & Security Surveillance systems	Surveillance	ENHANCED VIDEO DECODER	The HD video decoder capability to decode up to sixteen 4CIF resolution, 30 images per second (IPs) MPEG-4 encoded video streams simultaneously, or up to twelve H.264 Baseline, 4CIF resolution, 30 IPs video streams simultaneously, or up to four 1080p streams encoded in H.264 Baseline profile. Additional streams must be decoded using the network bandwidth consumption and CPU processing requirements by automatically subscribing to a lower resolution, lower bit-rate stream from a given camera depending on current load and screen configuration.
CIO- SD- 1.160	CCTV & Security Surveillance systems	Surveillance	ENHANCED VIDEO DECODER	The HD video decoder will drive one high-resolution monitor through HDMI connections for displaying the video footage.
CIO- SD- 1.161	CCTV & Security Surveillance systems	Surveillance	ENHANCED VIDEO DECODER	Diagnostics to be systemized with other system components. Any faults must be reported to users that have subscribed to diagnostic alarms regardless of where the user is located. In addition, the HD video decoder must also support SNMP messages and traps and be compatible with SNMP versions 1 and 2.
CIO- SD- 1.162	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The storage management application server must incorporate both server functions and storage elements into a purpose-built chassis.
CIO- SD- 1.163	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The storage management application server must not require removal from its rack installation when hard disk drives or power supplies must be replaced.
CIO- SD- 1.164	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The storage management application must record video and audio streams from IP cameras and video encoders on the network.
CIO- SD- 1.165	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The storage management application server must support extension through network storage, allowing the server to preserve and extend the life of video by moving it to an external, network storage location.
CIO- SD- 1.166	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The storage management application server must support failover, allowing a storage management application server to act as a hot standby for any number of other, active storage management application servers.
CIO- SD- 1.167	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The storage management application must have the following further functions and characteristics: a. Employ the Windows Server 2012 or above operating system b. Use RAID 6 parity across the storage drives to protect recorded data against a hard disk drive failure c. Use enterprise-level hard disk drives specifically rated for operation in RAID systems d. Employ the following redundancy features i. redundant, hot swappable power supply modules ii. Designed for online service and maintenance and cannot be removed from the rack when hard disk drives or power supplies must be replaced. e. Guaranteed recording throughput: 450 Mbps and up to 300 total cameras per storage device under normal and error (RAID rebuild) conditions f. Guaranteed downloading throughput: 175 Mbps per storage device under normal and error (RAID rebuild) conditions. g. The storage server must natively support panoramic cameras any combination of cameras from third-party manufacturers supporting ONVIF Profile S. h. Support continuous, scheduled, alarm/event (including analytic), and motion

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				i. Pre- and -post alarm periods must be configurable i. Support bookmarking of video content j. Support recording of secondary video streams
CIO- SD- 1.168	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	Support privacy tools that allow administrators to establish maximum retention times for video
CIO- SD- 1.169	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	Ability to report all diagnostic events, including software status diagnostics to a centralized user interface
CIO- SD- 1.170	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	Fully manageable from a remote workstation, including the ability to configure settings and update firmware and software
CIO- SD- 1.171	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	Capable of interfacing with a UPS using a USB connector
CIO- SD- 1.172	CCTV & Security Surveillance systems	Surveillance	Video Storage Manager	The server based surveillance system must receive status and control signals from the UPS when it is in backup mode, informing the operator about the amount of charge remaining and triggering a controlled shutdown when the charge becomes zero. The network storage manager is to be capable of interfacing with the Smart-UPS [®] using a USB connector. The server based surveillance system must receive status and control signals from the uninterruptible power supply (UPS) when it is in backup mode. This function must inform the operator about the amount of charge remaining and trigger a controlled shutdown when the charge becomes zero. The storage must be sized appropriately to accommodate the following requirements. - Type: Continuous, 24 hours/day - Scene type: Complex crowded with high motion - Resolution: 1920 X1080 Resolution - Frame rate: 25 Frames Per Seconds - Real Time Recording: 30 days. - Image Quality : Best
CIO- Camera- 1.0	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	High Definition PTZ must deliver crystal-clear, live streaming images with resolution up to 1920X1080p.
CIO- Camera- 1.1	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	It must offer four times the resolution of standard definition domes, and must be an ideal solution to view details such as faces, license plates, or other specific features.
CIO- Camera- 1.2	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	HD PTZ must support High-Profile H.264 compression, a vast improvement in quality over MPEG-4 and 20 times more efficient than M-JPEG.
CIO- Camera- 1.3	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	The HD PTZ dome system must be featured with open architecture connectivity for third-party software recording solutions allowing integration into virtually any IP-based HD system. HD PTZ must be ease of installation and ease of maintenance.
CIO- Camera- 1.4	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	Window blanking feature in the camera must enables a user to configure up to eight, four-sided, user-defined privacy areas.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-Camera-1.5	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	The camera must have video analytic built in with the camera and not limited to abandoned object, camera sabotage, directional motion, loitering detection, object counting, object removal & stopped vehicles.
CIO-Camera-1.6	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 1: Outdoor PTZ High Definition Camera Dome.	The outdoor fixed HD dome system must meet or exceed the design and performance specifications mentioned in RFP
CIO-Camera-1.7	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	The network camera must offer dual video streams with up to 3-megapixel resolution (2048 x 1536) in progressive scan format.
CIO-Camera-1.8	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	The network camera must provide extended Wide Dynamic Range (WDR), low-light performance, and anti-bloom technology.
CIO-Camera-1.9	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	The network camera must use a true WDR sensor that takes multiple exposures at the pixel level and has a rating for WDR of 120 dB or higher.
CIO-Camera-1.10	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	The camera must also be vandal with IK10 certified and tamper resistant.
CIO-Camera-1.11	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	Camera must support up to 128 GB Edge Storage with SD Card
CIO-Camera-1.12	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	The network camera must provide a removable, local storage medium (Micro SD) for scheduled and event-based recording of images.
CIO-Camera-1.13	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night Bullet Camera	The network camera must provide an accessory port for hardware expansion and two-way audio and additional alarm inputs.
CIO-Camera-1.14	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 2: Outdoor 3 Megapixel IP Day/Night	The Outdoor Bullet Camera must meet or exceed the following design and performance specifications

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
			Bullet Camera	
CIO-Camera-1.15	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must offer dual video streams with up to 2-megapixel resolution (1920 X 1080) in progressive scan format.
CIO-Camera-1.16	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	An alarm input and relay output must be built in for integration with hard-wired external sensors.
CIO-Camera-1.17	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must provide a removable, local storage medium (Micro SD) for scheduled and event-based recording of images.
CIO-Camera-1.18	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The cameras must support minimum 25 FPS @ full resolution and Up to maximum of 30 Frames per Second (fps)
CIO-Camera-1.19	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The camera must also be vandal with IK10 certified and tamper resistant.
CIO-Camera-1.20	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must be capable of firmware upgrades through a network using a software-based device utility.
CIO-Camera-1.21	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must provide an accessory port for hardware expansion and two-way audio.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-Camera-1.22	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The cameras must support Motorized zoom for easy remote set up
CIO-Camera-1.23	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must offer auto back focus (ABF) functionality through a push button on the camera. ABF parameters must also be configurable through a standard Web browser interface.
CIO-Camera-1.24	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must offer a video output port providing an NTSC/PAL analog video output signal for adjusting field of view and focus at the camera.
CIO-Camera-1.25	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must provide advanced low-light capabilities with sensitivity down to 0.03 lux.
CIO-Camera-1.26	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	Up to 30 images per second at 1920 X 1080
CIO-Camera-1.27	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The network camera must have a removable IR cut filter mechanism for increased sensitivity in low-light installations. IR cut filter removal must be configurable through a Web browser.
CIO-Camera-1.28	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP Day/Night Dome Camera vandal proof	The camera must have Auto-Exposure, Backlight compensation, contrast enhancement.
CIO-Camera-1.29	CCTV & Security Surveillance systems	Analytics & Camera Features	Type 5: Indoor 2 Megapixel IP	The network camera must have a window blanking feature to conceal user-defined privacy areas that cannot be viewed by an operator. The network camera must support up to four blanked windows. A blanked area must appear on the screen as a solid gray window.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
			Day/Night Dome Camera vandal proof	

The CCTV cameras and related equipment's must be connected in a secured way so that the malicious attacks such as DDoS, etc. from source end cannot take place. This should also include binding of camera, MAC address on to upstream switch and other measures as required.

CAMERA SUPPORT EQUIPMENT

- Camera housing and/or fixations not in any way to diminish or obscure the camera view or performance.
- Transparent housing parts to be scratch and impact resistant.
- Lower bubble of dome housings to be tinted to obscure camera position from detection.
- Cameras in high-abuse locations to be installed in domes with a watertight surface mounting, impact-resistant polycarbonate dome, and heavy-gage, 6061 T6 aluminum body.
- Outdoor cameras to be mounted in exterior enclosures that provide a minimum IP66 rating and include integral sun shield, cooling devices and heater to maintain interior temperature within operating range of camera. MSI to verify if environmental protection is sufficient considering local conditions and install the cameras accordingly.
- Interior flush mounted housings to be rated for use in an air plenum space.
- Mounting brackets to be powder coated cast aluminum, painted welded steel or reinforced composite construction. Unreinforced polymer not to be allowed.
- Mounting and housing finish being coordinated with the relevant parties.
- **Ceiling mounts type:**
 - Camera to be installed in dome style housing semi-flush mounts in suspended ceiling.
 - The camera housing to be secured to a load-bearing ceiling.
 - Cabling to be fed through dedicated flexible conduits, secured to construction ceiling.
 - Where indicated on architectural reflected ceiling plans, camera-mounting location to be in line with installed lighting units. Mounting geometry and finish to match the encasement of the lighting units.
- **Wall mount type:**
 - Camera to be installed in dome style housing semi-flush mounts in wall or column cladding.
 - The camera housing to be secured to the load-bearing wall or column.
 - Cabling to be fed through dedicated flexible conduits, secured to construction wall or column.
- **Surface mount type:**
 - Camera housing to be mount without housing or cabling penetrating the wall, column or ceiling.
 - Cabling to be fed through mounting brackets and in dedicated flexible conduits.
 - Suspended cameras to be rigidly mount to avoid image distortions due to vibrations.
- **Pole/Mast mounts type:**
 - Camera housing to be mount on Pole/mast.

- Cabling to be fed in dedicated conduits internally through pole or mast.

3.1.6. Hosting: On premise and Cloud

The hosting requirements of the project shall be met via a hybrid architecture that includes:

- On-premises; and
- On-Cloud.

Overall, the objective of this architecture is to optimize the number of on-site servers without compromising the overall performance of the system. DICDL shall provide the hosting infrastructure i.e. compute infrastructure at GSDC Gandhinagar for hosting all applications and services. All the software, OS, DB licenses required for successful hosting and running of the system for the contract duration is in MSI Scope . The following indicative systems (but not limited to) envisaged to be hosted on-cloud:

- ERP
- Industry specific solutions for Utilities
- eGovernance
- City Portal
- Social Media
- Website
- Citizen service mobile platform/applications

For the above mentioned system, MSI shall propose respective system architecture of hybrid model to cater to the requirements of DICDL. Also, any additional servers required for local processing and storage as per the respective solution should be considered by MSI as part of their technical proposal/bid. Apart from the above-mentioned systems, all other systems are expected to be hosted on-site are (but not limited to);

- Surveillance solution
- City Integrated Operation Platform
- Enterprise Management System (EMS) catering to Network Management for Server room and field devices
- Service desk solution
- IBMS
- Security solutions for Field devices and ABCD server room
- Any other solution that MSI feels necessary to be implemented at DSIR

MSI is required to provide an overall solution meeting the below mentioned minimum requirements for various applications. It is expected that all applications for on-cloud hosting shall support cloud ready architecture.

Application	High Availability/ Clustering at DC	Single Sign On	Backup	DR (minimum production capacity)	RTO	RPO	Expected response time in seconds
ERP	Yes	Yes	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	3

Industry specific solutions for Utilities	Yes	Yes	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	3
eGovernance	Yes	Yes	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	3
City Integrated Operations Platform	Yes	Yes	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	2
Portal	Yes	Yes	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	2
Website	Yes	Yes	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	2
Kiosk Software	No	No	Yes	No	60 Minutes	15 Minutes	2
Citizen service mobile platform/applications	No	No	Yes	Yes (Minimum 50%)	60 Minutes	15 Minutes	3

3.1.6.1. Hosting on GSDC Cloud at Gandhinagar

- For hosting of all applications, an overall hybrid architecture of on-site infrastructure and infrastructure provided by the cloud service provider shall be considered.
- All solutions provided by the MSI shall be High Availability (clustered/Load Balanced) configuration and shall be highly available. The server infrastructure provided by DICDL through the cloud service provider GSDC shall be of high availability (typically 99.74%).
- MSI to ensure that all applications are designed to support high availability requirement of the infrastructure.
- All application level redundancy, scalability, reliability, etc. requirements shall be under the scope of the MSI.
- As part of the Bid, MSI shall define the expected storage, server requirements for all stages of the contract for the applications that will be hosted on-cloud.
- MSI shall recommend system architecture for all the applications for both on-premises and cloud hosting.
- MSI shall specify/confirm RTO (Recovery time objective), RPO (Recovery point objective), Clustering/high-availability, Single sign on, proposed application uptime, proposed Application response time for all applications, and their respective storage requirements over the implementation and O & M period.
- MSI shall only be responsible for the application level performance, uptime, and not that of the availability of the hardware infrastructure being provided by the cloud service provider. However, the MSI shall be fully responsible to work hand-in-hand with the cloud service provider and ensure that an overall highly available solution is provided for the project.
- EMS (Enterprise Monitoring System) /NMS will be provided for the servers and application hosted in SDC
- Operating system and database licenses has to be provided by MSI as per solution
- All virtualization will be provided on Hyper-V (Microsoft) at GSDC, if any another virtualization solution is required as per the proposed solution of MSI then in that case MSI has to provide complete

solution including hardware, software and licenses as per the requirement.

- Connectivity between ABCD server room and GSDC will be provided by DICDL
- MSI needs to deploy under the supervision of GSDC team the proposed solution as described above post all relevant data regarding licensing , sizing and throughput has been provided to GSDC team by MSI reviewed and approved by GSDC.
- Gujarat State Data Center (GSDC) will provide computing infrastructure (computer power and storage) on x86 platform (virtualization/cloud environment) with server operating system platform Windows Server/Linux –RHEL (Red Hat Enterprise Linux operating system). SDC will provide the entire required infrastructure such as servers and internet connectivity etc. Bidder has to make arrangement of active-active clustered on cloud.
- MSI is required to quote, supply, install and maintain the required OS, Database and other software licenses. Considering the 7 years of growth if more compute infrastructure and storage will be required than it will be provided by the employer. However, during project life for user count staying same if hardware sizing needs enhancement due to performance issues then we will not pay extra for any licenses.
- The MSI shall interact with GSDC team to understand the GSDC's pre-requisites for deployment of application and develop the application in such a way that it is acceptable to GSDC/DICDL and complies with the standards prescribed for the State Data Centre.
- MSI is responsible for database/application configuration/end-to-end hosting of application at State Data Center (SDC). MSI will also be responsible for daily server monitoring and all other services required to perform during the O&M period w.r.t to his scope of work only.
- DICDL shall provide the necessary administrative support for hosting at GSDC. However, the necessary support, installation, update, upgrade and security will be the responsibility of MSI.
- MSI has to provide proposed bill of material in the following format along with the technical bid.
- Bill of Material for **Hardware**

Sr. No.	*Description	vCPU	RAM	HDD Space	Quantity	Remarks, if any

*Description: required DB servers, app servers, reporting servers or any other server (for production, testing development etc.), equipment required for running the application at DC; 1 physical core = 2 vCPU

- Bill of Material for **Software**

Sr. No.	Product Description	Unit of Measurement	Licenses quantity for DC	Remarks, if any

*Description: Required all the readymade software including OS and Database, App, Web, BI etc. for DC.

Following are the cybersecurity components that will be provided by GSDC Gandhinagar through shared services. MSI must provide the quantity of licenses for software solutions and throughput for hardware appliances to GSDC.

- Firewall Analyzer –reports will be provided as an when requested
- Secure Sockets Layer (SSL)
- Perimeter and Internal Firewall
- Intrusion Prevention System (IPS)
- Web Application Firewall (WAF)
- Antivirus and Anti-Malware

- Host Intrusion Prevention System (HIPS)
- Email Security
- Security information and event management (SIEM)
- DNS Security

3.1.6.2. Hosting on ABCD Server room

For all hosting on-site, the MSI shall consider them in their proposal and provide the required infrastructure as part of the project. The server specifications for the hosting infrastructure on-site can be found under section for minimum hardware specifications covered as part of the IT Infrastructure. As part of the Bid submission, the MSI shall provide detailed hosting requirements in terms of servers and storage that will be required for hosting the respective applications and services on-cloud and hardware-sizing requirement for the architecture designed from their end. In addition, MSI shall also provide details on the bandwidth requirement of the connectivity link required between Dholera (DSIR) and the respective CSP facility. The bandwidth requirements needs to be shared by MSI and the same will be provided by DICDL.

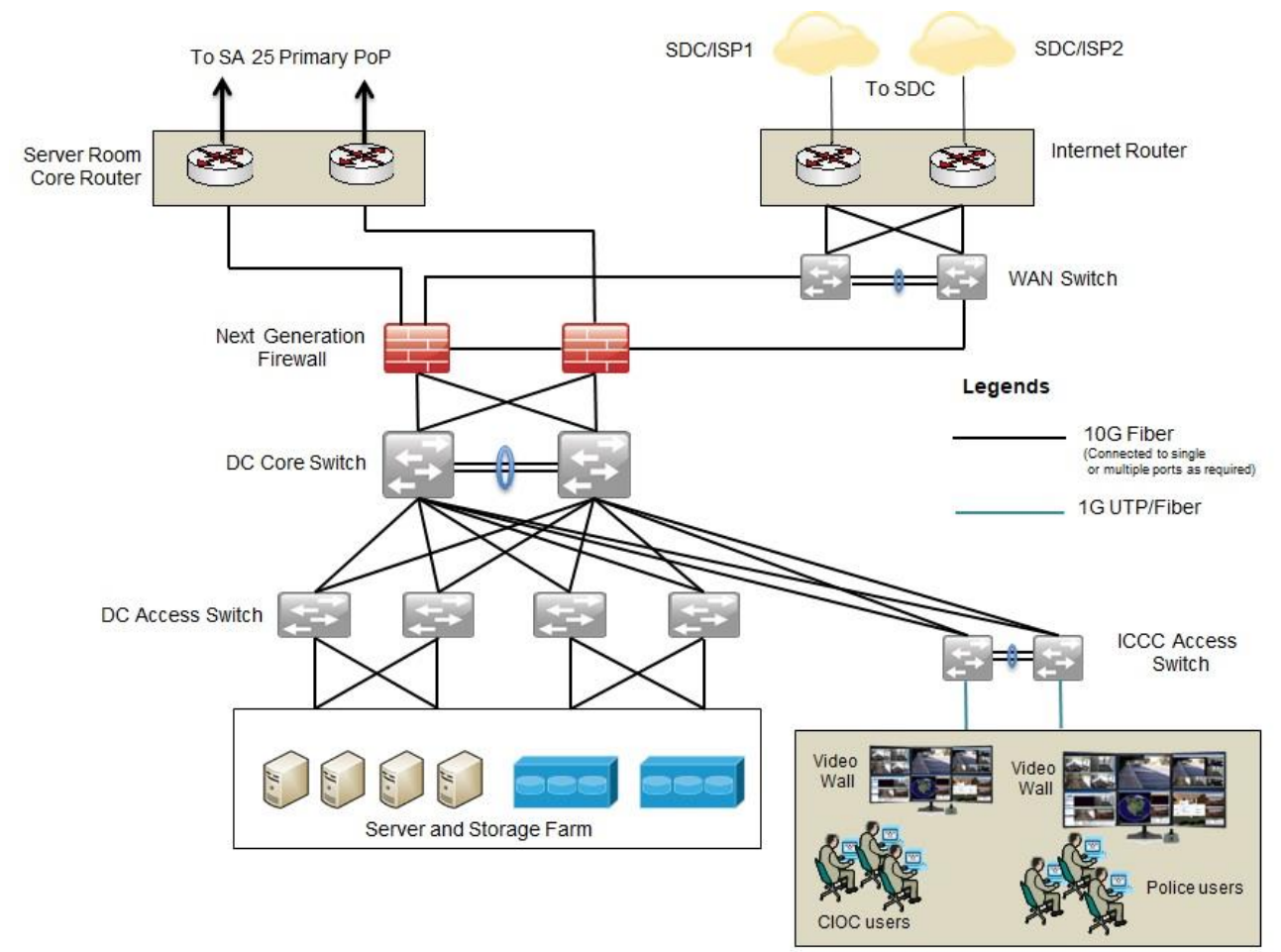


Figure – 24 Logical Diagram Server Room (SPV Building)

Functional, technical and non-functional requirements

Domain	Requirement ID	Short Description
SR	FR-SR-1.1	MSI shall be responsible to carry out any detailed survey prior to submission of bid for the complete solution components required to finalize infrastructure requirement, network bandwidth requirement, implementation, operational & administrative challenges etc.
SR	FR-SR-1.2	MSI shall suggest the sizing of the required hardware necessary for meeting the required performance of the system as per the SLA's defined in the RFP document for various components/domains.
SR	FR-SR-1.3	The MSI is responsible for sizing the proposed hardware for all the modules of ICT in future and performance requirements of the solution
SR	FR-SR-1.4	The MSI shall ensure that the LAN / WAN, servers, storage and backup are sized adequately with built in redundancy into the architecture
SR	FR-SR-1.5	The MSI must size and propose Highly Available Common Database software & Supporting infra for all Applications.
SR	FR-SR-1.6	DICDL team should have secured and seamless access to its data, applications, services and storage.
SR	FR-SR-1.7	The ICT infra shall be capable of integrating with other components as and when needed
SR	FR-SR-1.8	MSI should provide a dashboard view for monitoring all DC & DRC activities inclusive of hardware, application, data, bandwidth, backup and storage.
SR	FR-SR-1.9	The MSI should provide rack-view monitoring for power consumption & capacity.

Common servers for IT considering work packages

The ICT initiative for DSIR is to build a smart, socially and technologically attractive, sustainable excellent city which will be one of the engines for economic growth of the region.

ICT infrastructure is expected to add to the sustainable development / economic growth for Dholera inhabitants and create excellent quality of life, along with a platform for efficient operations and administration for city's infrastructure.

Dholera SIR is expected to be a city that would use Information and Communications Technology (ICT) as an underlying enabler pervasively, to integrate multiple essential disciplines of city such as eGovernance, safety and security, industrial growth, utilities, economy, etc.

The proposed ICT infrastructure should be highly reliable, agile and Scalable enough to expand ICT services without affecting running operations. The proposed ICT solution should be highly resilient by way of High Availability and robust data protection.

Server Room physical infrastructure

A data center is a facility that centralizes an IT operations and equipment, as well as where it stores, manages, and disseminates its data. Data centers house a network's most critical systems and are vital to the continuity of daily operations. Consequentially, the security and reliability of data centers and their information is a top priority for organizations. A dedicated and high-performance network infrastructure is crucial for the implementation of the Smart City concept is required to be considered.

Before making choices on the design of any Data center network, all the major parameters that may have an impact on it must be considered. The most obvious among them at this stage of the pre-analysis, are the city-wide size, as well as the backbone role of the network.

The Back-bone Network, CIOC and Data center/Server room should integrate different technologies which are open, interoperable and work as one converged ICT infrastructure and provide scalability, performance, flexibility, adaptability, ease of management, control, provisioning and high availability get the information at the right time to take the right decision. This back-bone also needs to have a Data Centre/Server room which is highly scalable, high performance, simple, virtualized, high availability, which can host applications like Surveillance, traffic management, Various SCADA systems, e-governance, ERP, and various IOT systems including parking, smart energy, Smart Sensors etc. which interact together to manage as one single system including data analytics and finally security.

Objective is to create an ICT infrastructure with a unified and resilient network to ensure convenient and ubiquitous delivery of reliable, speedy, affordable services and information to citizens thereby facilitating rapid and inclusive growth in the country with participation from various stakeholders in the ecosystem.

The objective is to create on demand, configurable, resilient, scalable, and interoperable and IPv6 compliant infrastructure with ubiquitous and affordable access to integrated infrastructure for delivery of public services for overall socio-economic development and digitally inclusive national economy. It would make available infrastructure with facility of plug and play for various stakeholders in the ecosystem like Smart City, ministries/departments, state Governments, local Governments, private sector, NGOs, NKN, Smart city, Digital India.

State of the art technology must be used to achieve the objectives for efficient and effective functioning of the infrastructure. Technical requirements should not only address current challenges but also take into an account futuristic requirements. This would necessitate the system to consider three key factors in any technology:

- The current state of the technology.
- The backward compatibility and
- The transition plan

Networking security considering work packages

Server Room should have first level of security. This provides optimization of the server room network, as unwanted traffic does not hog the bandwidth unnecessarily and affect the real-time applications. The server room network needs to have first level of security, so that any protocol attacks, anomalies, malicious traffic can be monitored and right action can be taken, so that the network is not affected. If, this is not monitored and stopped, the network may have issues like slowness, applications not working properly, long delay's etc. By enabling first level of security, these issues can be monitored and right action can be taken. This also helps in analyzing the security threats that are affecting the server room network and proper measures can be taken by enabling additional security mechanisms to the network. To start with SFW, DPI and Intrusion prevention is looked at and in future additional security mechanisms at the application level is also planned.

Next Generation Firewall

Next-generation firewall classifies all traffic, including encrypted traffic, based on application, application function, user and content. We can create comprehensive, precise security policies, resulting in safe enablement of applications. This lets only authorized users run sanctioned applications, greatly reducing the surface area of cyber-attacks across the organization. Next-generation firewall can provide Protection from known and unknown threats. Next-generation firewall limits unauthorized data transfer, detects, and blocks a wide range of threats. Next-generation firewall Identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment, and automatically disseminates updated protections globally in near-real time.

3.1.7. Network Operations Center

As part of this RFP, it is proposed that a Network Operations Center (hereinafter referred to as “NOC”) shall be established for monitoring the network infrastructure laid as part of City Network Backbone across all locations as proposed in this RFP.

The minimum requirements/ specifications for the NOC area are detailed in the following subsections. While it is mandatory for the MSI to meet these minimum requirements, if the MSI estimates that a particular requirement would need a higher category of equipment, the MSI shall provision for the same in the bid response. The MSI shall however provide basis for arriving at the solution being proposed as part of the bid response.

The NOC shall analyze network problems, perform troubleshooting, communicate with various DICDL officials / technicians/department officials and track problems through resolution. The key objective of the NOC is to ensure the health and availability of components. When necessary, NOC shall escalate problems to the appropriate stakeholders. MSI shall develop service catalogue for NOC and get a sign off on the same from DICDL / ICT Consultants/authorized entity.

The overall Scope of Work (SoW) for the MSI in regards to setting up of NOC includes the following:

- City Integrated Operation Centre area consists of the Network Operation Area, Server Room, Reception area, Conference room, etc.
- Design, supply, installation and setting up of the necessary basic Infrastructure for City Integrated Operation Centre area in terms of civil, interior, electrical and Air-Conditioning System, Fire Prevention, Detection and Suppression System, Lighting system, Power, multilayer Physical Security infrastructure like bio-metric based access-control system, CCTV/ surveillance systems etc.
- MSI shall take consultation and approval from DICDL/ICT Consultants/authorized entity, for the interior layout and material to be procured for the operations area.
- Primary responsibilities of NOC personnel shall include but not limited to:
 - Network Supervision and Monitoring
 - Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode
 - Configuration Management
 - Ensure proper configuration of network, systems and applications for the provision of reliable and high quality end-user services
 - Change Management, Network Extension
 - Ensure efficient day-to-day management of short-term network changes and optimization, including their implementation. This activity shall be synchronized with the maintenance scheduled activities
 - Performance Management
 - Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
 - Service and Network Provisioning
 - Define all necessary actions to be performed when a request for a new customer service is issued by customer care, and control the actions performed at NOC level or field level until completion
 - Scheduled Activities Planning
 - Provide regular plans for all scheduled activities, including preventive maintenance. Respect a schedule, and achievement of the plan. This is linked to the change management function which ensures overall synchronization of all network activities
 - IT and DB Management
 - Day-to-day management of all OSS systems, IT systems and databases (administration,

- backups)
- Security Management
 - Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
- Quality Management
 - Define quality management policies, ensure implementation and usage for competitive quality of service
- Workforce Management
 - Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
- Network Inventory Management
 - Ensure consistent management of network equipment, and accurate up-to-date documentation of it
- Spare Parts Management
 - Manage spare part handling and logistics to minimize repair/swap turnaround times for defective items, and keep low CAPEX for spare parts and consumables
- Asset Inventory Management
 - Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment
- Repair and Return
 - Receive and repair defective boards, return repaired or replacement boards.

Features of NOC

Major functions, which needs to be catered by NOC (but not limited to), are;

- Incident Management based on resource workload, incident Category etc.
- Tracking and reporting of all contractual SLAs in an automated way.
- Updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- The NOC shall escalate issues in a hierarchical manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation

3.1.8. Functional Requirement of Server room Non-IT Infrastructure Setup

As a part of Smart City initiative and order to carry out the administrative and development functions, the Administrative and Business Centre for Dholera (ABCD) complex is planned to support for 153 sq. km of Dholera Special Investment Region (DSIR).

ABCD complex was designed along with the overall master plan of the area covering 9 HA of land. – ABCD complex will house the offices of the proposed Node/ City level department offices, Exhibition Cum Auditorium Centre, Server room and City Integrated Operations Centre. However, looking at the development plan and timelines to construct the Data Centre building, DSIR planned to build Server room which can be scaled up to interim data center for full proof data center at a later point in time within City SPV building which shall meet the initial preliminary requirement of Data Centre Facility.

Server room shall be built to host Surveillance systems, EMS as well as other required system on premises considering the hybrid cloud model to support/integrate citizen applications and provide support to ICT infrastructure of DSIR. The Services belongs to server room and data center have been finalized based on the project requirements and International Best Practices for Data Centre.

The proposed Designs, Solutions, Specifications & BOQ along with draft drawings are enclosed in the tender document and are meant for reference and for purpose of bidding. MSI should be responsible for preparing

all the necessary shop drawings within the layouts enclosed and the BOQ in consultation with the DICDL/PMNC/ICT Consultant to arrive at the final scheme in line with the requirements of the DSIR.

The proposed server room will remain under comprehensive warranty for 5 Years considering the operation and maintenance phase from date of Go-Live of the Project.

To manage & maintain highest Uptime for server room applications (99.74%), MSI needs to design the same accordingly by planning the required parameters/components to achieve the said efficiency. This may include characteristics like Redundancy, Availability, Resilience, Modularity, Scalability, Serviceability and Manageability, etc.

Redundancy:

Ensures predictability of infrastructure in different operating scenarios. The technology and solution of the components shall be selected with high MTBF and Low MTTR.

Availability:

Ensures higher uptime by providing sufficient redundancies (inbuilt) so that maintenance can be carried out without impacting running system. It measures the security resilience of server room.

Resilience:

Resiliency is the ability of a server, network, storage system, or an entire data center, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.

Modularity:

Ensures use as needed and achieve lower PUE's in lower load requirement in the commencement of DC/server room operations and also helps in modular addition of capacities.

Scalability:

Ensure smooth and regular horizontal and vertical upgrade of server room/DC as requirements grows

Serviceability:

Serviceability refers to how easy it is to find a root cause for an incident or problem and solve the same. Ideal situation will be when issues will be tracked automatically and infrastructure in itself solves the issues.

Manageability:

Manageability refers to how easy, efficient, less time consuming, detailed and effective ways to manage the server room.

Design parameters

Server room is planned to have a minimum number of racks as per the Technical Solution designed by MSI considering the functional and technical requirements shared in the RFP as there would be only few applications to be deployed in server room considering the hybrid cloud model and connecting the server room to cloud service provider. Server room would have the racks where in depth hardware sizing should be carried out by the MSI and propose the number of servers and racks (network & server) accordingly. The server rack power density should be of 7KW and network rack of 5KW each considering the dual power consideration for high available mode.

MSI need to propose auxiliary systems/peripheral components required for installation and commissioning of server room viz. UPS, HVAC, etc. and should be catered in the cost proposed for the said component.

Every subsystem and system integrated into the server room site infrastructure must be consistently

deployed with the same site uptime objective of 99.74%.

The indicative/ conceptual server room Layout has been provided in the RFP, however based on the location identified by customer, selected MSI should prepare the floor plan in concurrence to the final requirement documented for the project.

MSI needs to cater to the hardware as well as physical security of server room keeping in mind various parameters mention as below;

The minimum specifications of hardware/software, which should be considered by MSI while proposing the solution as well as hardware is all, follows for various components;

Server Room Layout

Data Security and Infrastructure uptime is most critical and foremost requirement of Data Centre and physical security plays key role. Hence, it is important to understand the critical level of individual areas supporting Data Centre Operations. Complete Data Centre building is bifurcated in to four zones are as follows:

Zone A: This caters the Server hall area where Compute, Storage & Networking equipment are hosted. Server hall called as critical facility and proposed with three level authentication which involves frisking at reception, Mantrap Access & Bio-metric based access to Server Hall.

Zone B: Comprises of NOC & Helpdesk Area (Network Admin Team and L1 support Team) and BMS rooms. As these team are managing IT Infra access to these areas are limited by means of frisking, escorting and smart card based authentication.

Zone C: Comprises of Electrical, UPS/ Battery, Fire suppression rooms, Telecom Rooms etc. As these areas required third party access for maintenance, escort shall be made mandatory till the activity completed.

Zone D: This comprises of building & campus Entry & Exit points and shall be catered through perimeter surveillance, Physical security checks, baggage scanner etc.

MSI shall consider the above mention standard conditions and criteria while designing and at the time of installation, commissioning and O&M phase of server room at a location specified by DICDL in ABCD building.

Defects Liability Period (DLP):

The scope includes a comprehensive onsite free DLP of 60 months from the Go-Live date of the project. Preventive maintenance of equipment's under the scope of contract (proposed server room) like LT Electrical, UPS, HVAC and IBMS etc. for all the products during warranty will be within the scope and needs to be undertaken by the successful MSI. DLP should also include Subscription/AMC for any licensed product offered.

During operations and maintenance phase, Consumables like Fuel Filter, Engine Oil & Fuel shall be procured by successful MSI with prior approval and agreed rate with DICDL and get reimbursed from DICDL. MSI to co-ordinate with respective vendor for arrangement of below mentioned consumables items.

Below items are considered as consumables during Operations and maintenance phase.

1. High Speed Diesel
2. Consumables like air filters, engine oil, lube oil, coolant, gaskets, petroleum jelly, distilled water, battery (Post DLP), coolant and consumables during routine checks, etc. DG set & UPS Batteries (Post DLP)
3. Cables, MCB, MCCB, ACB Breakers & Energy meters

4. Fusible items like bulb, tubes, fuses, starter, chokes, LED drivers etc.
5. Fire Suppression Gas (In case release due to operation team fault or improper maintenance of fire alarm and detection system, MSI to replace the Fire suppression agent specified in the RFP at no cost to customer. The same also needs to be refueled/replaced in case of any minor/major incident)
6. UPS Capacitors and fans (MSI to replace the UPS Capacitor Bank before end of UPS warranty of 60 Months).

DICDL will not accept any offer of used or refurbished products or equipment. The successful MSI shall warrant that all the products and equipment offered will be fresh from stock and / or factory. Successful MSI shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all equipment, accessories etc. covered in the RFP. Successful MSI must warrant all equipment, accessories, spare parts etc. against any manufacturing defects during the DLP period. During the DLP period Successful MSI shall repair / replace at the installed site, at no charge to DSIR, all defective components that are brought to the MSI's notice.

Integrated Building Management System (IBMS)

Successful MSI need to design & implement, commission complete IBMS package in Server room and Command & Control Center, should include below systems and should be open protocol based to integrate with our systems like DCIM etc.

1. Access Control System
2. Addressable fire alarm and suppression system
3. CCTV
4. HVAC
5. VESDA
6. Water leak detection System
7. Rodent & Repellant System
8. Building Management System

Successful MSI need to provide the Operations & Maintenance services at DSIR Centers on 24 x 7 x 365 Basis to Operate, provide support and manage various Packages & utilities of Data Centers. The successful MSI to ensure the Preventive Maintenance of the product is carried out in timely manner. Regular reporting on Key Point Indicators (KPIs), recording of various parameters as per operating guidelines will be Successful MSI's responsibility.

The server room going live is one of the major milestones for any organization. However, there is a lot of effort that goes into operating and maintaining the server room. Adequate care should be taken to ensure that the design can take care of providing high availability and strict service levels while at the same time keeping the operating costs low.

Technical Annexures

The MSI shall refer to the following annexures for details:

A. Annexure: Floor Plans & SLD

- 5.1.1: Server Room Floor Plan
- 5.1.2: Server room Main Single Line diagram

B. Building Drawings

- 5.1.3: City DICDL Building 1st Floor ICT Room Layout

- 5.1.4: City DICDL Building 2nd – 8th Floor ICT Rooms Layout
- 5.1.5: City DICDL Building ICT Shaft Schematic
- 5.1.6: BEC Building Ground Floor ICT Rooms Layout
- 5.1.7: BEC Building 1st Floor ICT Rooms Layout

Functional and technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
SR-PHY-1	SR	Non-IT Infrastructure	UPS System	Data Centre Modular UPS System: IGBT Based, Transformer less, True Online, 0.9 input p.f., Total THD < 3%, Overall efficiency > 95%, UPS system with 3 Phase Input & 3 Phase Output and backup time of 30 mins on full load along with Individual Cell level Battery Monitoring System inclusive of interconnecting cables, panels, monitoring station and all accessories complete in all respect as required.
SR-PHY-2	SR	Non-IT Infrastructure	UPS System	Auxiliary UPS System for BMS, staging and another auxiliary load: IGBT Based, Transformer less, True Online, 0.9 input p.f., Total THD < 3%, Overall efficiency > 94%, UPS System with 3 Phase Input & 3 Phase Output and backup time of 30 mins on full load
SR-PHY-3	SR	Non-IT Infrastructure	Precision Air Condition System for Data Centre	Precision Air Conditioning system with following details: - EC Fan, Digital Scroll/Inverter Scroll Compressor - Net Sensible Cooling min: 35 KW, Cold Aisle Temp: 23 Deg C/50% RH & Return Air Temp: 35°C & 35 % RH. - Ambient Temp for condenser: 45 Deg C - Dual Power Supply Alternate heater and humidifier - Built in Automatic Transfer Switch Unit -Unity Communication Card (able to support both Modbus/SNMP)
SR-PHY-4	SR	Non-IT Infrastructure	Rack Power Distribution	Rack Power Distribution System - Rack iPDU's (32A) for 7KW Rated Racks
SR-PHY-5	SR	Non-IT Infrastructure	Rack Containment	Cold Aisle Containment as per drawing between Core N/W Rack Room with retractable sliding door at both sides. - Suitable for phase 1 rack and as per the layout. POD doors should have provision for fixing card reader, electromagnet and magnetic contact (from any access control vendor)
SR-PHY-6	SR	Non-IT Infrastructure	Civil and Interior Work	Civil and interior work within Data Centre building. Scope includes Partition walls, Flooring & Ceiling work, painting works
SR-PHY-7	SR	Non-IT Infrastructure	Electrical Work	Electrical HT & LT Data Centre Power Distribution system : - Main LT Panel - Cabling and distribution system - Earthing and Grounding etc. as per detailed SLD
SR-PHY-8	SR	Non-IT Infrastructure	Physical Security System	Integrated building Management System includes Fire alarm and detection system, Fire suppression system, Rodent repellent System, Access control system, Water Leak Detection system, Public address system, CCTV

Requir ement ID	Domain	Business Topic / Application / Module Name	Sub- Module / Functionali ty	Short Description
				surveillance System

Indicative Floor Plan:

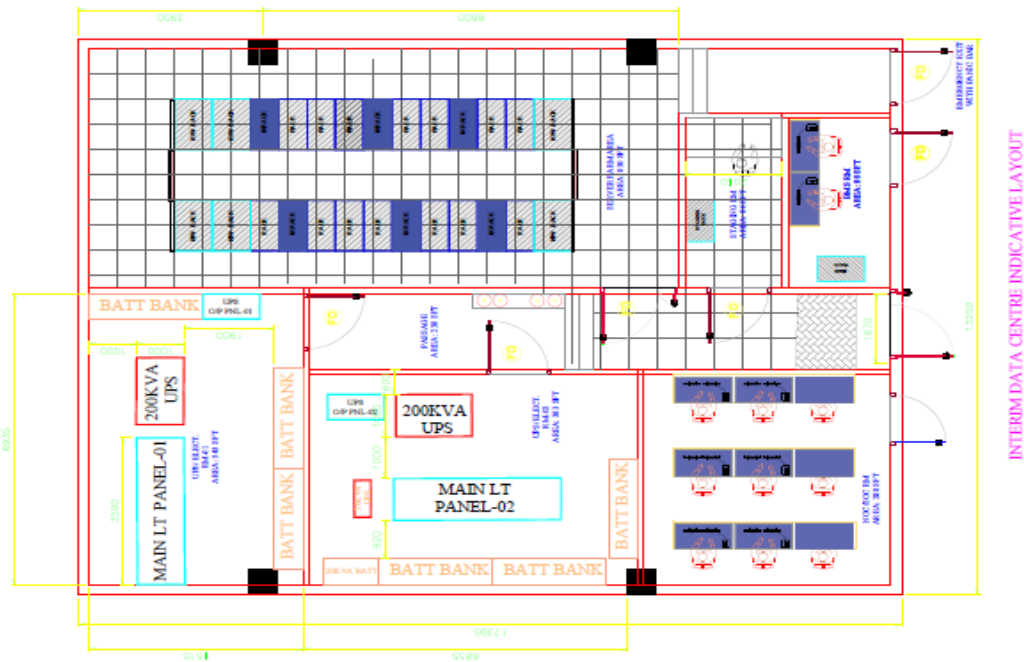


Figure-25 Indicative/Conceptual Floor Plan (Server Room)

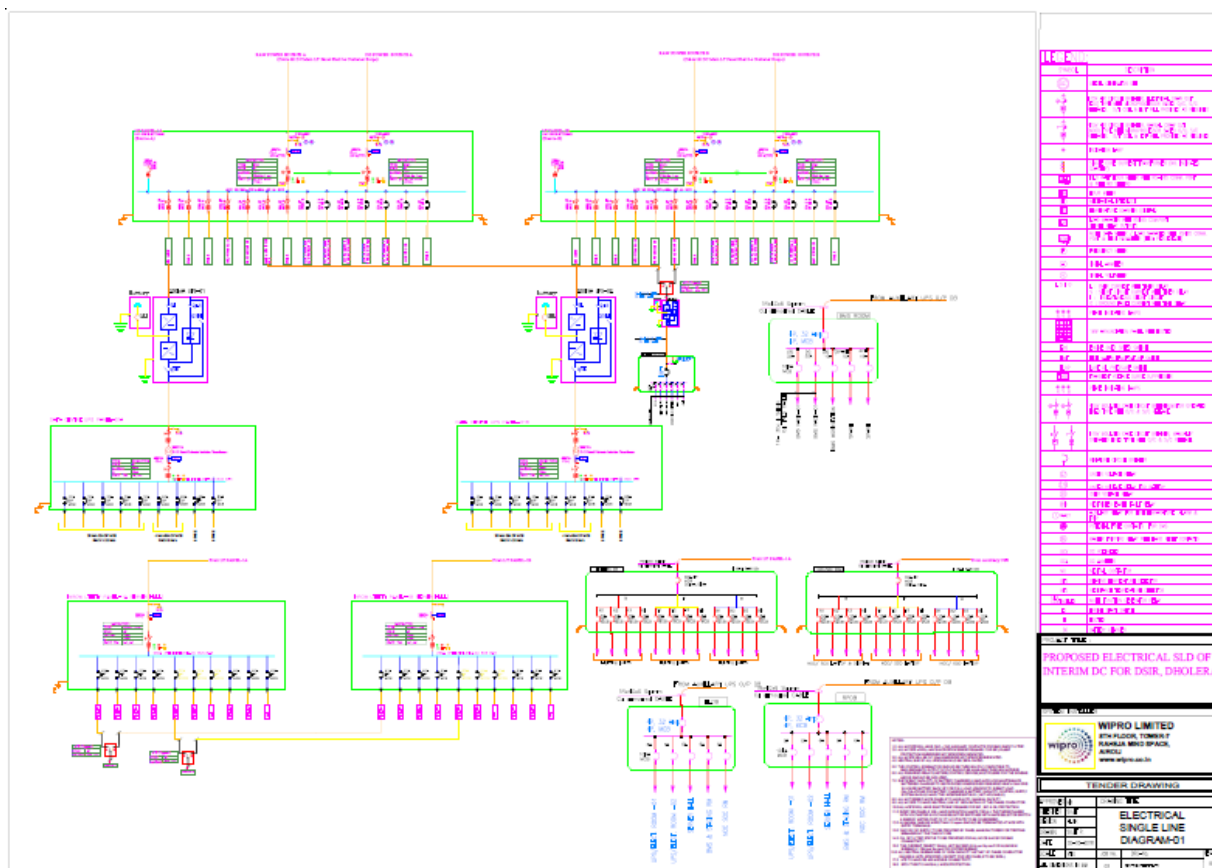


Figure-26 Electrical Single Line Diagram

3.1.9. Information Security

Scope of Work and Solution Design

The goal of DSIR is to ensure best-in-class, state-of-the-art and sustainable ICT technologies and solutions are adopted, deployed and enabled in DSIR in line with the world class smart cities. After analyzing evolving threat landscape using an attack surface analysis and potential risks to DSIR's regular management, we see some of the major security challenges as Cyber Attack surface, Bandwidth consumption due to interconnected thousands of sensors, or actuators, would communicate to a single/multiple server(s). MSI should propose a limited/partial Cyber security solution keeping in mind securing threats coming from the external cyber world to DSIR internal network as well as stopping any threats originates from internal networks. The proposed solution should consider layers of security to protect all DSIR infrastructure, web, application & mission critical servers

The high-level scope of security solution is as below

- Server Room security - server/storage/backup security, end point security, IDS/IPS etc. End device security, including physical security of all end devices such as display boards, kiosks etc.
- Citywide N/W security – With increasing internet penetration, there is going to be increase in risk of data misuse. Solutions like intrusion prevention system could minimize the risk of hacking.

The details of solution components and high-level description is as given below:

Infrastructure Security

Infrastructure or DC Security solution should consists of next-generation (NG) IDS/IPS, NGFW, Antivirus for Servers and end-points, etc. Details are as below;

- **Data Center NG Firewalls** – It consists of fully integrated, threat-focused NGFW and delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint
- **Data Center NGIPS** – It provides protection against traditional and sophisticated types of attacks
- **Host security** – The solution covers anti-virus solution, Host Intrusion Prevention System. This is installed on Servers & workstation to detect and prevent malicious activity being triggered at servers & systems
- **End point security** – The solution is about detecting and blocking malware by continuously analyzing for malware, and getting retrospective alerts. The dedicated advanced endpoint protection solution to stop APT threats and should not be subset of Antivirus or HIPS or traditional end point solution. The solution works on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint. It works as an independent module without relying on other endpoint and network systems for any of its functionality. It will be capable of working along with all leading endpoint AV vendors without needing to replace them. It utilizes layered and defense in depth approach, wherein the solution cannot be of the same make as endpoint AV. It supports detecting of all malware types, both known and unknown. The movement of all known and unknown malware would be tracked and reported across the endpoints. It should be able to support continuous and root cause analysis to help in triaging of security incidents.
- **AV Solution** - Endpoint AV Protection is required to stop advanced threats with next generation technologies that apply advanced machine learning, file reputation analysis, and real-time behavioral monitoring.

Network Security

Internal network solution should have following components

- **Network Access Control** – The Solution provides a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture, profiling and guest management services on a single platform. The Solution should include all required licenses to perform above mentioned capabilities for 100 endpoints from day one and scalable to 500 in future and it should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise. The Solution supports the endpoint checks for compliance for all windows endpoints such as check process, registry, file & application, check operating system/service packs/hotfixes ,check for Antivirus installation/Version/ Antivirus Definition Date, check for Antispyware installation/Version/ Antispyware Definition Date and check for windows update running &

configuration

The solution should have 802.1X port-based authentication enabled on all IT/OT devices to prevent unauthorized devices from gaining access to the network. The 802.1X must be enabled on the device port and the device must have a RADIUS configuration and be connected to the secure access control server. The EAP support must be enabled on the RADIUS server. The AAA is configured on the port for all network-related service requests. The authentication method list is enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. The IEEE 802.1X port-based authentication feature is available only on integrated switching routers that support switch ports. Or else we would need to have a separate solution that allows for simple deployment of 802.1X authentication, without compromising on security across the enterprise. The solution includes RADIUS/DIAMETER server and user repository servers and delivers 802.1X authentication as a zero-touch solution.

- **Trusted Wi-Fi internet security** - This solution securely encrypts all data transmitted over both wired and wireless Internet connections. It utilizes industry-standard 128-bit encryption. It creates a Virtual Private Network to hide all personal web-surfing information
- **Next-Gen Network Firewall** - To defend and increase threat visibility with advanced protection. The Next-Gen Firewall protects DSIR network against known and advanced threats. It includes
 - Enterprise-class firewall, Network Address Translation (NAT) within solutions
 - NGIPS: threat prevention and full contextual awareness of users, infrastructure, applications, and context to detect multi-vector threats and automate defense response. It passively and automatically recognizes evolving network landscape by analyzing network traffic and detecting what is on network.
 - On-box SSL decryption and re-encryption: Solution decrypts network traffic to detect attacks, applications, and malware. It also enables re-encryption after inspection where required.
 - Threat Containment: It has capability to identify a compromised endpoint and alerts NAC. In turn, Network Access Control (NAC) should be able to quarantine the affected endpoint.

Functional requirement for Network access control:

- Proposed solution should include two appliances to be configured in Active/Standby
- Proposed solution should integrate with Firewall so that they learn identity information from access devices
- Should support enforcing security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention
- Should support improve network access control capabilities to identify, mitigate/quarantine and rapidly contain threats
- Should utilize standard RADIUS protocol for authentication, authorization, and accounting (AAA).
- Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Transport Layer Security (TLS).
- Should provide a wide range of access control mechanisms, including downloadable access control lists (ACLs), VLAN assignments, URL redirect
- Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, IoT and tablets.

- It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.
- The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.
- Should support capability to verify endpoint posture assessment for PCs connecting to the network. Should be a persistent client-based agent to validate that an endpoint is conforming to a smart city's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispymware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications.
- Allows administrators to take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.
- Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.
- Solution should support the following endpoint checks for compliance for windows endpoints:
 - Check process, registry, file & application
 - Check operating system/service packs/hotfixes
 - Check for Antivirus installation/Version/ Antivirus Definition Date
 - Check for Antispymware installation/Version/ Antispymware Definition Date
 - Check for windows update running & configuration
- Proposed solution should support TACACS+ / RADIUS to simplify device administration and enhance security through flexible, granular control of access to network devices. TACACS+ / RADIUS device administration should support:
 - Role-based access control
 - Flow-based user experience
 - Per Command level authorization with detailed logs for auditing
- Proposed solution should support capability to customize TACACS+ / RADIUS Services by specifying customer TACACS+ / RADIUS port number
- Proposed solution should support capability to create different network device groups so that administrator can create:
 - Different policy sets for IOS/OS or wireless controller OS
 - Different for firewall
 - Differentiate base on location of device
- Proposed solution should be able to create TACACS+ / RADIUS profile like Monitor, Privilege level, default etc. to control the initial login session of device administrator.
- Proposed solution should be able to create TACACS+ / RADIUS authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive
- Proposed solution must support TACACS+ / RADIUS in IPv6 network
- Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.
- Should support Identity source sequences that defines the order in which the solution will look for user credentials in the different databases. Solution should support internal Users, Internal Endpoints, Active Directory, RADIUS Token Servers, Certificate Authentication Profiles
- Should support troubleshooting & Monitoring Tools

Functional requirements for End Point Security

- Endpoint software must be easy to deploy and support (not limited to) deployment through 3rd party systems management tools
- Root cause analysis on a suspected machines should include the following capability:
 - Sequential and chronological trace of events with details including host, username, IP, client application involved
- Software footprint should be small and must support interactive and/or silent install.
- Proposed endpoint software should support malware tracking and provide visualization at the network level: systems and users affected, patient zero, and method/point of entry.
- Proposed system must support continuous and persistent monitoring of files to detect polymorphic and time bound malware whenever they start turning bad and shall not be only an on-demand scan mechanism
- Remediation at endpoints for incident response should include (and not limited to):
 - Track and capture files on suspected machine with option for lookups on suspected devices
 - Block of files / process / services that are showing malicious behaviors
 - Dropper detection and blocking of downloads via URL / sites
 - Submit suspected malicious files for further analysis
- The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user
- The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)
- The proposed solution shall provide details to enable forensic analysis of incidents
- The solution shall be capable of working in Windows, Mac & Linux operating systems
- The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints
- The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition
- Proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing to administrator
- Proposed solution should be able to do a threat hunting across all endpoints and quarantine the specific malicious file
- Proposed endpoint solution should run as is and not require any system changes at OS level like enabling Volume Shadow copy Service, disabling admin access or any other user level change
- Solution must support Exploit Prevention detection engine to block exploits and memory attacks that target certain processes.
- Solution must support System Process Protection adds protection for memory attacks against Windows system processes.
- Solution must support Adding Process Exclusion type to support System Process Protection in AMP for Endpoints Windows Connectors.
- Solution must support Adding Policy settings to enable Exploit Prevention and System Process Protection in AMP for Endpoints Windows Connectors.
- Exploit protection - for protecting certain popular applications like MS Word, Excel, PowerPoint, Internet Explorer, Firefox, Chrome, Adobe Reader and others from attacks loading malwares that directly into the memory of these processes.

Creation and maintaining the Information Security Training Program

- Develop IT Security and Compliance Training program for DICDL team
- Develop IT Security training calendar and post training evaluation mechanism

- Conduct trainings for DICDL control owners and control operational stakeholders over the IT Control framework
- Conduct the IT Regulatory and Security trainings for DICDL resources
- Conducting control walkthrough and “Point in Time” test to ensure that DICDL resources have understood the control requirement and evidence which needs to be submitted.
- Development of periodic control testing calendar based on control criticality and define reporting templates

Information Security Requirements

The Information Security solution should be proposed keeping in mind securing threats coming from the external cyber world to DSIR internal network as well as stopping any threats originating from internal networks. Multiple layers of security should be considered to protect all infrastructure and mission critical servers. The aim is to reduce the attack surface as much as possible and to make the surface that is visible as robust and resilient as possible.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
INF-ARC 1.0	Information Security	Architecture & Design	Security of privacy and data	Security and privacy of data within the DSIR program will be foundational keeping in view of the sensitivity of data and critical nature of the infrastructure envisioned to be built for DSIR Smart City operations. Security and privacy of data should be fundamental in design of the system without sacrificing utility of the system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one
INF-UIM 2.0	Information Security	User Identity Management	Levels of Authentication	Based on the security requirements the following levels of authentication should be evaluated: • For applications handling sensitive data, it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data • For applications handling highly sensitive data, it is recommended that two factor authentication mechanisms should be considered. The first line of defense is the password conforming to the password complexity rules'. Along with the password, next user has to provide a one-time password, which varies for each session. One-time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and many other attacks. A counter-

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				synchronized One-Time Password (OTP) solution could be used for this purpose.
INF-UIM 2.1	Information Security	User Identity Management	Authorization	Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list: • Establish groups of users based on similar functions and similar access privilege. • Identify the owner of each group • Establish the degree of access to be provided to each group • The Solution must support federation.
INF-UIM 2.2	Information Security	User Identity Management	User Identity Management	The solution should have capabilities of Credential Management, Self Service registration, Profile Management, Workflow management, Provisioning Policies, Role Management, Delegated Administration Application Integration and Identity Reconciliation, The solution should support the following: • The concept of management of identity creation, identifier assignment, attribute profiles, identity reconciliation, and authenticators. • The management of collections of identities that represent groups and roles. Identities can be assigned to groups and roles based on identity attributes, business rules, or on an ad-hoc basis. • The process of determining if an individual should have access to a system or function. Includes role-based authorization. (RBAC). • Create, read, update, and delete identities in the Solution by providing a provisioning API (ex: update password, change user name, and check PIN code). • Encryption of passwords
INF-AUD 3.0	Information Security	Audit Trail & log	Audit Trail & log	Audit trails or audit logs should be maintained. Log information is critical in identifying and tracking threats and compromises to the environment. There are a number of devices and software that should be logged which include firewalls, authentication servers, database servers, routers, DHCP servers, etc. It is essential to decide what activities and events should be logged. The events, which ideally should be captured, include • Create, read, update and delete of confidential information; • User authentication and authorization activities in the system, granting, modification or revoking of user access rights;

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				• Network or service configuration changes; • Application process start up, shutdown or restart, abort, failure or abnormal terminations, failure of network services; • Detection of suspicious activities such as from Intrusion Detection and Prevention system, antivirus, anti-spyware systems etc.
INF-STC 7.0	Information Security	Compliance to Standards & Certifications	Compliance to Standards & Certifications	• Information Security ISO 27001 • Government of India IT security guidelines including provisions of: - The Information Technology Act, 2000” and amendments thereof especially Information technology amendment Act 2008 primarily concentrates on the compensation for negligence in implementing and maintaining ‘reasonable security practices and procedures’ in relation to ‘sensitive personal data or information’ (“SPDI”), Section 72-A of the IT Act mandates punishment for disclosure of ‘personal information’ in breach of lawful contract or without the information provider’s consent - Guidelines and advisories for information security published by Cert-In/MeitY (Ministry of Electronics & information Technology, Government of India) issued until the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

3.1.10. Enterprise and Network Management System

Scope of Work and Solution Design

In addition to hardware and software requirements as prescribed in this RFP, MSI is required to design size, supply, implement and maintain an Enterprise Management System (EMS) during the total project duration. The EMS should be able to support the proposed hardware and software components deployed over the tenure of the Contract.

1. EMS should be capable of providing early warning signals to the Helpdesk Agents on the performance issues, and future infrastructure capacity augmentation. The EMS should also support single pane / dashboard with visibility across multiple areas of applications for project monitoring and control.
2. MSI shall design, supply, install, customize, test, implement, rollout and maintain the EMS application and hardware hosted in ABCD Building and field equipment’s. The services hosted in DICDL provided on Cloud would be monitored through shared services provided by the CSP.
3. MSI should ensure the EMS solution supports the proposed hardware and software components

deployed over the tenure of the Contract.

4. MSI shall document the solution architecture related artifacts to cover areas like Application architecture, system architecture, component models, Data architecture, security architecture, infrastructure architecture, etc. The documentation to be reviewed and approved by the relevant authorities.
5. MSI shall document detailed solution design related artifact to cover areas like Functional specification, configuration, technical specification, etc. These documents need to be reviewed and approved by the relevant authorities.
6. MSI should engage the OEM solution to review the final solution design and assess it as per the best practices of the OEM.
7. Requirements that cannot be delivered as standard out of the box functionality or with configuration needs to be agreed with the design authority. If it is envisaged by design, authority a prototype or proof of concept shall be facilitated by MSI.
8. MSI shall be responsible to supply and install all required hardware/ software/ tools to meet the RFP requirement without any deviation. Any additional hardware or software necessary to meet the technical, functional and performance requirement of the project but not mentioned specifically in RFP shall be factored and supplied by MSI as part of this RFP.
9. MSI shall define the development and configuration standards. MSI shall be responsible to configure, build, enhance and customize the applications to ensure it meets the requirements without any deviations.
10. MSI shall define in agreement with the relevant authorities the exit criteria for each type of testing. MSI shall perform all the necessary testing like Unit testing, System Integration testing, load and performance testing. MSI shall assist in user acceptance testing. MSI shall develop the test strategy and test scenarios to cover all the process variants and requirements. MSI shall use industry standard tools required for testing. MSI shall ensure that the minimum exit criteria (as agreed by the relevant authority) is met to conclude the completion of the testing. MSI shall manage and monitor all the stages of testing. MSI shall document all the artifacts required for testing phase like, testing strategy, test plans, test scenarios, test cases, test results/reports with evidences, test cycles, etc. These documents shall be reviewed and approved by the relevant authorities for further processing.
11. MSI shall impart relevant training and guidance to the CIOC team as well as officials from DICDL and other respective designated authorities shared by DICDL to better understand the business and technical reports generated by the solution.
12. MSI shall maintain the detailed configuration of all the ICT components in the CMDB of EMS system.
13. MSI shall be held responsible for data collection, transition, data cleansing for all the data to be migrated to Production environment. MSI shall be responsible for the reconciliation of the data. MSI shall provide the necessary templates for data collection to DICDL. MSI should ensure that data in the production is accurate at go live and does not contain any erroneous data from test/UAT environment that can lead to unreliable/erroneous SLAs/KPIs.
14. MSI shall undertake the Business Change Management. MSI shall manage and anchor the BCM activities like collaboration hub, road shows, change champions grooming, communications etc.

15. MSI shall assist and anchor the ongoing benefit realization for DICDL.
16. MSI shall provide the Operations and Maintenance Services for a period of 5 years from the date of Go-Live. The MSI shall be responsible for following but not limited to:
 - Responsible for identification, diagnosis and resolution of problem areas and maintaining the defined SLA levels.
 - Provision of skilled and experienced manpower resources to administer and manage solution.
 - Provision and management of the service management tool to manage the tickets.
 - Periodic health checks of the systems and applications to ensure the system performance.
 - Users and authorization management
 - Periodic system patching and upgrade as recommended by the application vendor.
 - Management and maintenance of integrated environments like Development environment, Testing environment, Production environment and Training environment if applicable (ITSM tool).
 - Provide all necessary manpower resources onsite to manage and resolve any issues/incidents and carry out required changes, optimizations and modification
 - Management and maintenance of configuration, development and data on these environments.
17. MSI shall arrange for environments and tools for testing and for training as envisaged.
18. Production environment should never be used for testing and training purpose. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected MSI.
19. MSI shall be responsible for provisioning/facilitating all tools/environment required for testing and sufficient training shall be given to officials from DICDL and their designated authorities.
20. MSI shall provide a well-prepared build documentation / user manual for users, also a clear plan for user training, education & hands training on installed solution.
21. MSI shall be responsible to deliver all documents approaches for entire solution with proper training and knowledge transfer.
22. MSI shall adhere to the agreed SLA for deployment, operate, and maintain.

It is crucial for the CIOC to monitor the ICT implementations at DSIR in order to be productive and avoid serious threats from network failures and server downtime. A best of breed IT Enterprise & Network monitoring solution can provide the needed visibility and control over all the ICT hardware & software assets at DSIR. It will help the CIOC optimize network reliability-

23. It has proposed that a Network Operations Center (NOC) shall be established for monitoring the network infrastructure laid as part of City Network Backbone across all locations as proposed in this RFP. The NOC shall analyze network problems, perform troubleshooting, communicate with various officials / technicians and track problems until resolution. The key objective of the NOC is to ensure the health and availability of components and the Enterprise and Network Management System (EMS) proposed herewith will enable to the NOC to achieve these goals. The EMS solution proposed will allow the NOC to monitor the complete network 24/7 and help keep the network and systems functioning in a stable operation mode.

24. MSI is required to design size, supply, implement, customize and maintain the Enterprise Management System (EMS) solution and its underlying hardware to fulfill the requirements of this RFP and help the NOC in affectively monitoring the DSIR environment. The EMS shall be able to support the proposed hardware and software components deployed over the tenure of the Contract and provide for the regular monitoring, management and reporting of the ICT infrastructure and its project assets installed in the respective operations center as well as at field locations.
25. The proposed EMS solution should encompass, but not be limited to, the following functions:
- Configuration Management
 - Fault Management
 - Incident, Problem and Change Management
 - Asset Management
 - SLA Management & Monitoring
 - Performance Management
 - Event Management
 - Server, Storage and other Infrastructure Management
 - Monitor network components of the LAN & WAN
 - Network Link Monitoring
 - Application Performance Monitoring
 - Other modules as required by DICDL to meet the requirements of the RFP

EMS system shall facilitate with regular monitoring, management and reporting of the ICT infrastructure of the project assets installed in the respective operations centre as well as field locations. The activities performed by the MSI shall be under the supervision of DICDL and DICDL nominated agencies. EMS system shall have the following features including but not limited to and as well act as authoritative source for the same:

Following functionalities are desired by use of such EMS tools:

- Availability Monitoring, Management and Reporting
- Performance Monitoring, Management and Reporting
- Helpdesk Monitoring, Management and Reporting
- Traffic Analysis
- Asset Management
- Incident Management and RCA reporting.
- Change and Configuration management.

Functional requirements

Require ment ID	Domain	Business Topic / Application / Module Name	Sub- Module / Function ality	Short Description
EMS-FR 1.0	EMS	EMS	Generic / Function al	The EMS shall support single pane / dashboard for the purposes of the NOC with real time monitoring & visibility across multiple areas of DSIR environment for monitoring. The EMS solution shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
EMS-FR 1.1	EMS	EMS	Generic / Functional	The EMS shall be capable of providing early warning signals to the NOC on the performance issues, and future infrastructure capacity augmentation. The alarms should contain meaningful message text, instruction text, operator / automatic actions / linked graphs, duplicate message suppression.
EMS-FR 1.2	EMS	EMS	Generic / Functional	The EMS solution shall help the NOC to quickly triage the root cause for a network problem or service availability and provide actionable information to the respective teams for a quick resolution to the problem before end users get impacted.
EMS-FR 1.3	EMS	EMS	Generic / Functional	The alerting mechanism should be configurable to suppress events at the agent or managed node level itself and be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.
EMS-FR 1.4	EMS	EMS	Generic / Functional	The EMS solution shall offer service driven operations management of the IT environment to manage distributed heterogeneous systems from a single management station. The solution shall provide comprehensive and end-to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure.
EMS-FR 1.5	EMS	EMS	Generic / Functional	The EMS solution will also let the DMICDC team monitor and request reports for SLA requirements as agreed upon for various services both on availability & performance.
EMS-FR 1.6	EMS	EMS	Generic / Functional	The EMS solution should be able to monitor and provide availability reports for ICT assets both within and outside the datacenter. The EMS solution will allow the CIOC to associate an ICT asset with a consuming service so that it can be appointed a business value and its impact and utilization in the environment can be understood by the business.
EMS-FR 1.7	EMS	EMS	Generic / Functional	The EMS solution will provide comprehensive server monitoring capabilities to understand the processes & services running on a machine and resource utilization impact's performance such as a Database service, web server, application server etc.
EMS-FR 1.8	EMS	EMS	Generic / Functional	The EMS solution shall provide an insight into how various DSIR applications and services are performing both from the perspective of the end user and the infrastructure itself. The solution and its various integrations will allow the service & application owners to be proactively informed of any issues which can potentially impact the consumer and fix them beforehand.
EMS-FR 1.9	EMS	EMS	Generic / Functional	The EMS solution should include asset management capabilities to monitor the lifecycle for all ICT assets, both hardware and software, in the DSIR environment. It shall also allow the DICDL team to generate detailed reports for effective management such as reports on asset utilization, end of service, maintenance lifecycle etc.
EMS-FR 1.10	EMS	EMS	Generic / Functional	The solution should provide seamless integration between discovery, monitoring and service desk tools which will help in automated ticket logging in service desk for all the critical events captured/occurring in centralized monitoring console and to keep an updated CMDB. It shall also provide flexibility of logging,

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				viewing, updating and closing incident manually via web interface.
EMS-FR 1.11	EMS	EMS	Generic / Functional	The proposed helpdesk system shall support ITIL processes like request management, incident, problem management, knowledge, SLM, configuration management and change order management with out-of-the-box templates for various ITIL service support processes. The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
EMS-FR 1.12	EMS	EMS	Generic / Functional	The EMS solution shall be able to accurately measure the KPIs / SLAs agreed upon by DMICDC and report them on pre-communicated intervals to the key stakeholders for analysis. The SLA & KPI details should be obtained directly from application & platform owners and agreed upon by DMIC team as well. For continued improvement, these SLAs/KPIs might need to be updated from time to time to reflect the maturity of DMIC environment after agreement with DMICDC team.
EMS-FR 1.13	EMS	EMS	Generic / Functional	The EMS solution tools must be open to integration not only among themselves but also with other technologies being utilized at DSIR such as the Single pane view dashboard for the NOC & other SLA & Reporting technologies being utilized by different applications at DSIR. EMS solution will capture valuable data which will prove useful to other solutions such as the GIS solution for example to populate device data on visualization screens. Similarly, data integration will also have to be considered with the ERP HR modules to get approval flows and access levels of various resources for an ITSM request catalogue.
EMS-FR 1.14	EMS	EMS	Generic / Functional	To ensure EMS doesn't introduce any unsolicited security loopholes and concerns into DSIR, only SNMP v3 compliant devices must be integrated with the EMS systems and the MSI should ensure that non-standard ports and non-standard community strings are always used where possible.
EMS-FR 1.15	EMS	EMS	Generic / Functional	All EMS tools and applications must utilize all ports and all communications must be secured via SSL.

EMS solutions should adhere to the following standards but not limited to;

- Proposed EMS/NMS solution must be an industry standard, enterprise grade solution recognized by various organizations/leading analysts
- Probable OEM technical support group should be available on 24x7 basis.

Note: Vendor must perform a final infrastructure survey at the time of implementation and ensure the solution adequately supports the latest DSIR environment metrics without any additional cost to the DICDL

3.2. City Applications Work Package

All the city applications needs to be implemented based on the design and engineering provided in the functional requirements as well as other places in the RFP document.

The requirements to be implemented will not be limited to the following and MSI will be obligated to include all the additional requirements to be provided to MSI time-to-time without any repercussions to client.

3.2.1. ERP suite of Applications

ERP/ Shared services

The ERP system will be the backbone for DICDL that will enable efficient and integrated operations, maintenance and financial management. This system will closely integrate with other systems and be the main system used by DICDL to support and manage all the back office and controlling functions. It is envisaged that the ERP system will integrate and automate the internal business functions and provide a standardized best practice process framework to enable people centered, responsive, well governed functions.

It is envisaged that most of the key functionalities will be available in standard software and shall be configured to meet the business requirements in key functions of the DICDL. The ERP suite of applications will be the internationally leading standard ERP system with a proven track record and a road map in a similar domain. The ERP system should provide the SOA based integration framework for integrating various applications and systems with ability for process orchestration and exception management. The ERP suite of application should have appealing, intuitive and easy to use user interface.

ERP Solution: Proposed ERP System should be open-source with enterprise support for 5 years from the date of Go-Live. “Open-Source ERP” means software for which the source code is made freely available and may be redistributed and modified. Bespoke or owned developed solution will not be considered and accepted.

Main system components for ERP suite of applications are:

1. Dholera corporate website (Internet and intranet)
2. Customer facing systems (CRM): Multi-channel center for citizens/call center to record and manage the citizens interactions and case management to manage customers service requests / complaints.
3. Back office system: to effectively manage back office functions like Finance and Accounts, Cost controlling, Purchasing, Budgeting, contract management, Sales Management, Asset Management, IS Utilities, Asset Maintenance, Projects Management, Inventory management, HR and Payroll.
4. ERP suite of applications should provide the framework for integrating various applications
5. Governance, Risk and Compliance: to cover financial compliance, Access control, process control, Environment compliance, Trade management etc.
6. Master Data Management: Mastering data in single system, Data synchronization across various systems and exception management.

The related business requirements are as below:

1. DICDL envisage an ERP system to automate and digitize various business functions and process.
2. ERP suite of applications will be a holistic integrated solution to meet the DICDL requirements.
3. ERP suite of applications shall provide an integrated solution to enhance transparency, accessibility and efficiency of DICDL functions.
4. Shall streamline, standardize information digitization and access.
5. Shall facilitate information reuse across various departments and processes.
6. Shall have continued compliance with Government framework, policies, legal regulations and standards.

7. Shall provide a modular and customizable solution to meet DICDL requirements.
8. Shall be scalable to accommodate future growth and support hardware & software additions and upgrades.
9. The ERP solution shall be used and proven, fully integrated but modular Commercially off the Shelf - Enterprise Resource Planning (COTS - ERP)/ Open Source Product, covering all the key modules required as mentioned in the RFP.
10. The software application should be readily deployable with or without configuration to suit the customer's specific process requirements and does not involve developing the application from scratch. COTS/Open Source ERP software shall be implementable or deployable and maintainable by any other competent agency other than the manufacturer or agency, which has developed the COTS/Open Source ERP software. Proposed COTS/Open Source ERP software solution shall also be available with complete transparency including operation manuals, help documents and source code.
11. ERP suite of applications is an enterprise wide integrated application
12. ERP suite of applications comes with the Source Code for any enhancements and Customization
13. ERP suite of applications supports localization features for India taxes and provides the legal changes for these taxes as a support package from time to time
14. ERP suite of applications is completely scalable and supports large enterprise implementation
15. ERP suite of applications supports all security features required for enterprise application
16. ERP suite of applications Provides solution manager/equivalent suite, which integrated tool for monitoring of the implementation, administration and operation of the software.

Functional and Technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-FI 1	ERP	ERP-Finance	Organization Structure	System should allow to define the Financial organization structure as follows, but not limited to: - DICDL Company - Multiple company codes assigned to the DICDL company each having a separate legal entity. - Functional area assigned to company code - Credit control area assigned to company code - Multiple plants assigned to company code - Profit centers and profit center hierarchy - Business segments etc.
ERP-FI 2	ERP	ERP-Finance	General settings	Functionality to define other global settings like but not limited to: the fiscal years, posting periods, fiscal calendar, various posting keys, accounting document types, document number ranges etc.
ERP-FI 3	ERP	ERP-Finance	General Ledger accounting	Functionality to define the chart of accounts at group or entity level, account groups, retained earning accounts, hierarchical account structure etc. Should support multi-currency to support Imports and should have National Accounting Standards (IND-AS) compliant ledger and maintain accounts as per Indian Statutory requirements.
ERP-FI 4	ERP	ERP-Finance	General Ledger accounting	Functionality to open and close financial periods, postings should only be allowed in the open periods, provision of additional adjustment periods to the normal 12 periods for posting transactions in current previous or next financial year.
ERP-FI 5	ERP	ERP-Finance	General Ledger accounting	Functionality to park, change and post journal entries with complete audit and traceability by authorized DICDL users. Should generate unique document number for every financial posting document and allow for multiple line items per document. Functionality to drill down into the transaction details and original documents, which resulted in accounting document posting. Ability to create and maintain recurring journal entries.
ERP-FI 6	ERP	ERP-Finance	General Ledger accounting	Functionality for Automatic and manual clearing of GL account postings and should provide the flexibility for users to define the rules for automatic clearing. System should also allow resetting cleared accounting items.
ERP-FI 7	ERP	ERP-Finance	General Ledger accounting	System should have facility to easily maintain complex validations and substitution rules at various levels like document type, company code, profit center etc.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-FI 8	ERP	ERP-Finance	General Ledger accounting	Month-End closing: System should do the month end functions like but not limited to: - Perform foreign currency valuation, if applicable - Clear open items - Clear G/L Accounts - Open and close posting periods - Post Tax payables - Verify data flow - Display financial statement - Run Financial statement (Ledger comparison) - Process trial balance - Process mass data input - Manage the Assets not settled - internal order settlement - A/c clearing - GR-IR, GL, Customer , Vendor - Close Materials management period and Open Materials Management next period - depreciation run - Lock periods - Create AR/AP evaluation - Export GR/IR - Post Cap Cred/Debt GR/IR - Analyze GR/IR clearing - Open new forecasting period - reverse mass accruals update - carry forward commitment update - lock plan version for forecasting - Carry forward GL balances update - Carry forward AR/ AP Balances - Regroup AR/ AP balance by age - Post AR/ AP balance Regrouping
ERP-FI 9	ERP	ERP-Finance	General Ledger accounting	Year-end closing: Open Posting Periods: System should do the year end functions like but not limited to: - Regroup Receivables / Payables - Trial Balance - Generate Financial statements - Post Tax Payables
ERP-FI 10	ERP	ERP-Finance	General Ledger accounting	Financial Consolidation: System should do the consolidations like but not limited to: - Inter business elimination of Receivables - Inter business elimination of Payables - Inter business elimination of Revenues - consolidation of investments - Translation of statements - Sub-consolidation - Final consolidation - Regrouping of GL balances
ERP-FI 11	ERP	ERP-Finance	General Ledger accounting	Functionality to maintain multiple plan financial statements at business unit level and /or corporate group level to be uploaded from various formats like workbook, csv file etc. by authorized users. System should allow distributing / allocating planned data to other functions or organizational units. System should allow for top-down and bottom-up planning.
ERP-FI 12	ERP	ERP-Finance	General Ledger accounting	System should allow for recording financial transactions for multiple legal business entities and should be able to generate statutory financial reports / statements like but not limited to: - Profit and loss - Trial Balance - Balance sheet - Cash flow report - Year end schedules for audit - reconciliation report etc.
ERP-FI 13	ERP	ERP-Finance	General Ledger accounting	System should be flexible to define multiple adhoc and pre-defined reports required for monitoring and control purposes.
ERP-FI 14	ERP	ERP-Finance	General Ledger accounting	System should be able to generate cash management forecast and reconciliation statement for bank transactions.

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-FI 15	ERP	ERP-Finance	General Ledger accounting	Functionality to process incoming and outgoing payments and transfers of funds via various mediums like net banking, credit cards or any other payment mechanism. System should be able to process cheque and cash payments with automated handling of outstation cheque.
ERP-FI 16	ERP	ERP-Finance	General Ledger accounting	Functionality to mass upload GL entries via excel, csv etc. file formats by authorized users.
ERP-FI 17	ERP	ERP-Finance	General Ledger accounting	Functionality for Write-offs and write-ons with appropriate multi-level approval process.
ERP-FI 18	ERP	ERP-Finance	Asset Management	Asset master: System should have provision to manage various asset related processes like but not limited to maintain multiple asset classes and should allow for running different processes for different asset classes. System should allow authorized users to create, maintain, view, block or delete asset. System should be able to create sub numbers for assets, and provide complete change audit of the assets. System should have a provision of 360° View on Asset (Asset Explorer) and asset classes per chart of depreciation. System should have provision to transfer asset from one class to other.
ERP-FI 19	ERP	ERP-Finance	Asset Management	Asset acquisition: System should have provision to acquiring asset without order, acquisition with automatic offsetting entry, settlement of Orders to AuC (Asset under construction), settlement of AuC to Fixed Asset, Credit Memo creation in current and previous fiscal year.
ERP-FI 20	ERP	ERP-Finance	Asset Management	Asset retirement: System should have provision to sale asset including invoicing, asset sale through auction, and retirement of asset due to scrapping. System should generate relevant accounting documents as a result. System should have provision for asset write-off. Functionality to partially or completely retire asset, reinstate retired asset
ERP-FI 21	ERP	ERP-Finance	Asset Management	Asset valuation: Functionality to Transfer asset and Manual Value Correction by authorized users. System should have provision to reverse and delete asset document. Functionality for Intra-Company asset transfer. Functionality for capitalization and post-asset capitalization processes. Functionality to reevaluate asset, record and amortize revaluation reserve based on accounting standards.
ERP-FI 22	ERP	ERP-Finance	Asset Management	Asset transfer: Functionality for partial or complete asset transfer between: - Divisions / departments / cost centers / company codes - Location / Custodian / Projects etc.
ERP-FI 23	ERP	ERP-Finance	Asset Management	Physical verification: Functionality to - maintain a physical control of the asset via various asset attributes like serial no, location, cost center etc. -generate fixed asset verification sheet
ERP-FI 24	ERP	ERP-Finance	Asset Management	Asset Insurance: Functionality to track asset insurance details like sum insured, premium etc. Functionality to manage and account insurance claims.
ERP-FI 25	ERP	ERP-Finance	Asset Management	Month end closing: System should have provision to manage automated monthly depreciation run, recalculate asset value, and manage unplanned asset depreciation.
ERP-FI 26	ERP	ERP-Finance	Asset Management	Year-end closing: System should be able to generate Asset History sheet, Asset transaction list and depreciation reports.
ERP-FI 27	ERP	ERP-Finance	Asset Management	Functionality to automatically post controlling and accounting documents for every asset related transaction.
ERP-FI 28	ERP	ERP-Finance	Asset Management	Reports: Functionality to generate reports like but not limited to: - Fixed asset register - Period Depreciation report - Asset depreciation register with summary and details - unposted depreciation calculation report - various asset transactions like transfer, disposal, retirement, capitalization etc. - reconciliation report for GL and depreciation register
ERP-FI 29	ERP	ERP-Finance	Accounts Payable	Manage and maintain complete supplier master data: Functionality to create and maintain complete Supplier Master Data including details like but not limited to: Supplier VAT registration, address, Bank details, key contact persons and their contact details, procurement blocks etc. Functionality to maintain one time vendor record and related transactions for vendors who do not have long-term relationship with DICDL. Functionality to

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				classify Vendors and maintain them with different number ranges (example: Vendors, Employees etc.) Functionality to assign separate control accounts to Vendors in GL. Functionality to manage and view these masters only by authorized users.
ERP-FI 30	ERP	ERP-Finance	Accounts Payable	Invoice Creation: Functionality to create Invoice against a Purchase order, create Invoice without purchase order. Functionality to scan the incoming invoice and create incoming invoice document linked to the scanned invoice. Functionality for fast data entry of invoices. Functionality to automatically calculate TDS deduction for Vendor Payments, posting of input tax (GST) etc.
ERP-FI 31	ERP	ERP-Finance	Accounts Payable	Invoice Verification: Functionality for automated comparison of the Invoice against the Purchase order, Goods receipt and if applicable and variation is within allowed tolerance limits (% and/or absolute value) automated release of Invoice. Functionality to block the invoice if mismatch with GR and /or variance more than allowed tolerance and trigger the workflow for Quality Surveillance users to investigate and release/reject the Invoice. QS Users should be able to drill down into the related documents, master data and PO history to be able to investigate. Functionality for multi-level approval/ release of the invoice based on the invoice value.
ERP-FI 32	ERP	ERP-Finance	Accounts Payable	Invoice Payments: Functionality to: - Manage Payment Blocks - Schedule Payment Proposals - Revise Payment Proposal - Release Payment Proposal - Create Single Outgoing Payment - Post Outgoing Payment - Create Payment Medium - Generate payment advice via various mediums including electronic payment in the format acceptable by Banks - Automated clearing for invoices and payments - Reset Clearing for Invoices and Payments - Printing of Cheque - Automatic and Manual Payments Analysis - Open Payments Analysis - Bank Payment Approval - Payment acknowledgement printing
ERP-FI 33	ERP	ERP-Finance	Accounts Payable	Functionality to manage cheque numbers, cheque status and complete traceability of cheque processing, manual and automatic cheque printing
ERP-FI 34	ERP	ERP-Finance	Accounts Payable	Reports: Functionality to generate reports like but not limited to: - View Supplier Line Items - View Supplier Balance - Days Payable Outstanding - Overdue Payables - Future Payables - Cash Discount Forecast. - Cash Discount Utilization - Aging Analysis - Analytical Content for Accounts Payable - Payment forecast for different time horizon - Vendor account reconciliation - Overdue payments, open invoices, payments made in advance, blocked invoices etc.
ERP-FI 35	ERP	ERP-Finance	Accounts Payable	Functionality to re-value the open transactions and balances in foreign currencies in line with DICDL defined standards
ERP-FI 36	ERP	ERP-Finance	Accounts Payable	Functionality to manage and monitor: - Bank guarantees - Advance Payments to Vendors - allow advances to be adjusted partially or fully against the invoice - automatic vendor account postings and clearing - manage credit notes and payments against the credit notes - imports with Letter of Credit and Telegraphic Transfers
ERP-FI 37	ERP	ERP-Finance	Accounts Payable	Functionality to generate Supplier communications via various mediums like but not limited to: - Balance statements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				- Credit notes - Cheque and covering letter
ERP-FI 38	ERP	ERP-Finance	Accounts Payable	Functionality to manage travel management for employees and expense processing, payments related to expenses, etc.
ERP-FI 39	ERP	ERP-Finance	Account Receivables	Manage and maintain complete Customer master data: Functionality to create and maintain complete Customer Master Data including details like but not limited to: Customer VAT registration, address, Bank details, key contact persons and their contact details, Sales blocks etc. Functionality to maintain one time customer record and related transactions for customers who do not have long-term relationship with DICDL. Functionality to classify Customers and maintain them with different number ranges. Functionality to assign separate control accounts to Customers in GL. Functionality to manage and view these masters only by authorized users.
ERP-FI 40	ERP	ERP-Finance	Account Receivables	Invoice generation: Functionality to create Invoice against a Sales order or contract or debit note, create Invoice without sales order. Functionality to automatically calculate various tax components, posting of output tax (GST, sales tax, service tax, VAT or any other municipal levy), post invoice in accounting etc. Ability to provide discounts, rebate and other levy charges. Consider payment terms as defined for customer or group of customers.
ERP-FI 41	ERP	ERP-Finance	Account Receivables	Reports: Functionality to generate reports like but not limited to: - Overdue Receivables - Display Customer balances - View Customer Line Items - Days Payment Outstanding - Overdue Payments - Future Payments - Aging Analysis - Analytical Content for Accounts Receivables - Payment forecast for different time horizon - Customer account reconciliation - Overdue payments, open invoices, payments received in advance, blocked invoices etc.
ERP-FI 42	ERP	ERP-Finance	Account Receivables	Functionality to generate Customer communications via various mediums like but not limited to: - Customer Balance statements - Credit notes / Debit notes - Dunning (multiple levels with different format) - Payment receipts (automated / manual) - automatic reconciliation of sub ledger with the control account in GL - automatic interest calculation for overdue payments for a customer or group of customers as agreed
ERP-FI 43	ERP	ERP-Finance	Account Receivables	Receivables Clearing : Functionality for: -Revenue postings Via Bank statements -Reset Clearing of Invoices/Payments -Individual reversal of Invoices/documents -Manual Clearing of Open items
ERP-FI 44	ERP	ERP-Finance	Account Receivables	Revenue Recognition: Functionality to manage revenue recognition / accrual in line with the regulations for: - Payments received in advance - Payments received in arrears
ERP-FI 45	ERP	ERP-Finance	Account Receivables	Functionality to manage and monitor: - Bank guarantees provided by customers - Advance Payments received from Customers - allow advances to be adjusted partially or fully against the invoice - automatic customer account postings and clearing - manage debit notes and payments against the debit notes - automatic multiple level of dunning - multiple tax structures on various transactions - Compliance with GST procedures
ERP-FI 46	ERP	ERP-Finance	Account Receivables	Functionality for various challan preparation and filing of various tax returns according to Central as well as state governments legal requirements
ERP-FI 47	ERP	ERP-Finance	Integration	Functionality to integrate with various other DICDL applications for posting the FI/CO documents.

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP CM 1	ERP	Finance	Cashier Management	The ability to work off-line in the event of network failure.
ERP CM 2	ERP	Finance	Cashier Management	The ability to process point of sale transactions for utilities/non-utility account related commodities.
ERP CM 3	ERP	Finance	Cashier Management	The ability to process point of sale transactions for prepayments.
ERP CM 4	ERP	Finance	Cashier Management	The ability to track and distribute cash receipts to multiple general ledger accounts.
ERP CM 5	ERP	Finance	Cashier Management	The ability to configure GL account distribution for all types of transactions.
ERP CM 6	ERP	Finance	Cashier Management	The ability to capture and retain specific identifier for the source of payment.
ERP CM 7	ERP	Finance	Cashier Management	The ability for the user to search for an account while in the cashiering system using the customer name, address, phone number etc.
ERP CM 8	ERP	Finance	Cashier Management	The ability to enter a single account payment, which is composed of multiple tender types (e.g. credit card, cash, check, cashier's check, credit/debit (check) card, or money order).
ERP CM 9	ERP	Finance	Cashier Management	The ability to capture and retain payment check numbers in the system.
ERP CM 10	ERP	Finance	Cashier Management	The ability to print a daily summary of cash receipts by user defined classification codes and tender types.
ERP CM 11	ERP	Finance	Cashier Management	The ability for the user with proper security and audit trail to search, retrieve, and edit payment transactions before batch closing.
ERP CM 12	ERP	Finance	Cashier Management	The ability for the user to search and report payment transaction history using various criteria like cashier ID, receipt no, date, branch office etc.
ERP CM 13	ERP	Finance	Cashier Management	The ability to view alerts such as "Block check payment" indicator, preventing any check payments without a supervisor override.
ERP CM 14	ERP	Finance	Cashier Management	The ability to view alerts such as "Block credit / debit card payment" indicator, preventing any payments without a supervisor override.
ERP CM 15	ERP	Finance	Cashier Management	The ability to view collections alerts.
ERP CM 16	ERP	Finance	Cashier Management	The ability to support a check scanning device.
ERP CM 17	ERP	Finance	Cashier Management	The ability to support a validation printer.
ERP CM 18	ERP	Finance	Cashier Management	Payment Drawer Close-Out
ERP CM 19	ERP	Finance	Cashier Management	The ability to allow cashier to balance a payment batch on demand from any workstation regardless of where the payments were processed (secure location).
ERP CM 20	ERP	Finance	Cashier Management	The ability to allow authorized users to close out drawers on behalf of cashiers with appropriate permissions (security).
ERP CM 21	ERP	Finance	Cashier Management	The ability to allow authorized users to consolidate drawers and close out as a single batch.
ERP CM 22	ERP	Finance	Cashier Management	The ability to provide the means to produce a continuous audit trail of each transaction, including payment allocations, for each cashier's payment

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				batches. This printed audit trail must also be stored on electronic media for onscreen viewing and historical archiving.
ERP CM 23	ERP	Finance	Cashier Management	The ability to allow authorized users to assign/remove staff to / from cash drawer with audit trail.
ERP CM 24	ERP	Finance	Cashier Management	The ability to allow authorized users based on security and user role to perform payment corrections (e.g. reversal, void, charge back, etc.) after the close of business day while maintaining full audit details and data integrity.
ERP CM 25	ERP	Finance	Cashier Management	The ability to allow authorized users according to security and user role to perform deposit corrections (due to counterfeit bills, etc.) after the close of business day while maintaining full audit details and data integrity.
ERP CM 26	ERP	Finance	Cashier Management	The ability to combine individual payment batch deposit details into a single consolidated deposit, include a batch number and deposit ID number.
ERP CM 27	ERP	Finance	Cashier Management	The ability to ensure same payment batch doesn't get posted twice. A control process should be in place that a responsible staff should verify total payment received equal to total batched deposit amount and total payment applied to customer account for the day.
ERP CM 28	ERP	Finance	Cashier Management	The user (with proper security) has the ability, prior to the closing of the business day, to reverse any portion of a single payment that had been distributed to multiple line items or accounts in error and allow the user the opportunity to reapply that portion of the payment.
ERP CM 29	ERP	Finance	Cashier Management	The ability to allow a user, based on authorized security roles, manual override of payment priorities and apply payments to individual line items based on user assigned priorities.
ERP-SD 01	ERP	ERP-Sales	Organization Structure	Organization structure: System should allow to define the sales organization structure as follows, but not limited to: - Sales Organization - Distribution Channel - Division - Sales Office
ERP-SD 02	ERP	ERP-Sales	Master Data	Sales Master data: Functionality to manage and maintain time-sliced Sales master data like but not limited to: - Products / Services - Customers - Price lists - Discount and Rebate agreements - Pricing structure - Tax related data
ERP-SD 03	ERP	ERP-Sales	Quotation based sales	Functionality to generate Quote for various quote based services/products offered by the Corporation. It should be possible to create multiple line items which build the quote along with pricing and other data like validity duration. Functionality to print/email the quote in appropriate standardized format to customer. Functionality to track and follow-up with customer on quotes not converted to order before validity ends. Functionality to requote and re-determine the prices. Ability to manage a service charge for Quote preparation before the quote is generated, for certain service offerings. Functionality to capture customers' acceptance of the quote and conversion of the quote to a sales order. Functionality to deliver and record the delivery of goods / services and invoice the customer based on delivery or billing plan based on the service offering.
ERP-SD 04	ERP	ERP-Sales	Order based Sales	Functionality to generate Sales orders for various fixed price services/products offered by the Corporation. It should be possible to create multiple line items which build the order along with pricing and other data. Functionality to print/email the order in appropriate standardized format to customer. Functionality to deliver and record the delivery of goods / services and invoice the customer based on delivery or billing plan based on the service offering.
ERP-SD 05	ERP	ERP-Sales	Outbound Tax	For Quote / Order / Credit memo / Debit memo system should calculate the tax components in line with the set standards. System should be able to re-determine the tax on change of order value or tax rates based on the 'point-of-delivery' date. Functionality to manually trigger the re-calculation of taxes.
ERP-SD 06	ERP	ERP-Sales	Credit Notes	Functionality to generate Credit notes for various reasons. It should be possible to create multiple line items which build the credit note along with pricing and other data. Functionality to print/email the credit note in appropriate standardized format to customer. Functionality of multiple levels of approvals based on value and integrate with Accounts Payables.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-SD 07	ERP	ERP-Sales	Debit Notes	Functionality to generate Debit notes for various reasons. It should be possible to create multiple line items which build the debit note along with pricing and other data. Functionality to print/email the debit notes in appropriate standardized format to customer. Functionality to invoice the customer based on debit notes.
ERP-SD 08	ERP	ERP-Sales	Rebate agreements	Functionality to manage rebate agreements.
ERP-SD 09	ERP	ERP-Sales	Lease / rental contracts	Functionality to setup lease / rental contracts with multiple line items, contract validity and periodic billing plan. System should auto generate the periodic invoices based on Billing plan. The contracts should allow for billing in advance / arrears and handle the accounting in accordance with India GAAP.
ERP-SD 10	ERP	ERP-Sales	Invoicing	Functionality to invoice Customers based on Sales documents and send the Invoices to customer via various mediums like, email, hard copy etc.
ERP-HR 1	ERP	ERP-HR	Organization Structure	Organization structure: System should allow to define the hierarchical organization structure as follows, but not limited to: - Organization unit - Role - Position - Employee
ERP-HR 2	ERP	ERP-HR	Master Data	HR Master data: Functionality to manage and maintain time-sliced HR data for every internal and external employee like but not limited to: - Personal details - Organizational details - Categorization details - Payroll details - Family details - Leave entitlement - Communication data - Skills - Address - Planned working times and shifts - Bank details - contract elements - Travel privileges - Education -Dependents - Pensions etc.
ERP-HR 3	ERP	ERP-HR	HR Strategy	System should assist in defining the HR strategy which is heavily influenced by or coupled with the overall business strategy. There will be a reliance on other inputs, such as revenue forecasts, employee data, workforce analytics, benchmarking data, engagement surveys, PESTLE analysis (Political, Economic, Social, Technology, Legal, Environmental), in order to support the creation of a robust HR Strategy. Strategies will have a long-term focus, but will account for workforce planning that will usually be completed annually.
ERP-HR 4	ERP	ERP-HR	Workforce Strategy	System should assist in defining the workforce strategy to provide clear direction and method for achieving the goal of having the right number of people, with the right skills, in the right place at the right time. Tasks will usually stem from a Business or Functional level strategy, coupled with the HR Strategy and will highlight either a business need (ex. penetrating new area, increasing use of flexible staffing [part-time, contingent, contractor]) or a business risk (aging workforce, attrition/turnover of key employees).
ERP-HR 5	ERP	ERP-HR	Manage HR	Ability to monitor and update HR plans to measure the outcomes of HR activities and the contributions of HR to achieving the goals and objectives of the company's business strategy. It involves communicating/updating HR plans to stakeholders, determining the value added from the HR function, and reviewing and revising HR plans. System should assist in measuring, improving, controlling the performance of all HR services provided to the business. This can be a concentrated, centralized effort by HR management to improve areas as they see fit. A more effective approach will see each HR process area incorporating feedback and data collection as part of their daily work, in order to bolster the continuous improvement of the HR process area and, when issues/improvements are fed back centrally, for the HR function as a whole.
ERP-HR 6	ERP	ERP-HR	Competency framework	Functionality to create an organization competency framework for use throughout the business and HR process areas. A common framework needs to be used to increase usage and understanding of organization competencies

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				as a whole, with competencies added to reflect the different skills needed in different areas of the business. Usually a scale will also be used to signify the progression within a particular competency, as well as the attachment of competencies to jobs.
ERP-HR 7	ERP	ERP-HR	Manage Organizational Design	Functionality to design a new organization or part of an existing organization, which addresses business drivers for change. Following establishing the case for change, activities including defining the operating philosophy, organizational structure, outline roles, key activities and RACI models.
ERP-HR 8	ERP	ERP-HR	Manage Employee Requisitions	Functionality to create and develop employee requisitions process includes identifying gaps between current resourcing and org design, developing and opening job requisitions in line with defined organization design, preparing job descriptions, posting job requisitions, managing internal/external job posting Web sites, changing/updating requisitions, notifying hiring managers, and managing requisition dates.
ERP-HR 9	ERP	ERP-HR	Recruit/Source Candidates	Function to support the Recruit/source candidates' process, which involves selecting recruiting methods, performing recruiting activities, holding/participating in recruiting events, and managing recruitment vendors.
ERP-HR 10	ERP	ERP-HR	Screen and Select Candidates	System should support activities like interviewing, testing, evaluating candidates and then comparing candidates in order to select candidates, usually in order of preference. These will be considered against the capabilities and qualifications defined for the role.
ERP-HR 11	ERP	ERP-HR	Manage pre-placement verification	System should support the Management of pre-placement verification process which involves conducting background checks, performing pre-employment screenings, and recommending or not recommending a candidate.
ERP-HR 12	ERP	ERP-HR	Manage New Hire/Re-hire	Functionality to support and manage new hire/rehire process including drawing up and making a job offer, negotiating an offer, and hiring a candidate.
ERP-HR 13	ERP	ERP-HR	Manage Applicant Information	Functionality to manage applicant information which involves creating an applicant record; managing/tracking applicant data; and archiving and retaining records of non-hires. Once this record is complete, the information should transfer to the HR Core system and employee profile.
ERP-HR 14	ERP	ERP-HR	Manage Onboarding	Functionality to support Onboarding, which involves primarily a transfer of information and management of, or delivery of training - before, on and after the first day of employment.
ERP-HR 15	ERP	ERP-HR	Manage Orientation	Functionality to create, manage and maintain employee orientation programs, which should be aligned to the preceding onboarding activities and leading to the training and development of a new employee in their first year of employment. The process should include evaluation of the effectiveness of employee onboarding programs.
ERP-HR 16	ERP	ERP-HR	Manage Employee Performance	Functionality to manage and define performance objectives; reviewing, appraising, and managing employee performance; and evaluating and reviewing the performance management program. Output may include feed into payment of performance bonuses through the benefits and payroll processes.
ERP-HR 17	ERP	ERP-HR	Manage Employee Development	Functionality to support employee development process which includes creating short and long-term career goals, reviewing organizational career ladders, and identifying training and development opportunities.
ERP-HR 18	ERP	ERP-HR	Develop and Train	Functionality to support Develop and train employees process which includes aligning employee and organization development needs; developing competencies; conducting training needs analyses; and developing, conducting, and managing employee, management and contingent worker training programs.
ERP-HR 19	ERP	ERP-HR	Manage Employee Capabilities	Functionality to support the process of putting in place a set of capabilities, with descriptions and different levels, and linking these capabilities to either employees and / or positions within the organization. The assessment of employees own capabilities should take place under process area
ERP-HR 20	ERP	ERP-HR	Manage Talent and Succession	Functionality to select critical roles in the organization, and potential successors from within the organization (via the creation of talent pools and succession plans) or in some cases from external talent pools. Elected talents may take part in special training, mentor programs and career planning activities.
ERP-HR 21	ERP	ERP-HR	Manage Cases	Functionality to support the process which involves the management of grievance, disciplinary or other internal investigation cases according to set

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				company policy and legal guidelines or regulations. Typically, such cases include a high degree of administration and documentation.
ERP-HR 22	ERP	ERP-HR	Manage Employee Consultation Process	Functionality to support processes involved in consulting with employee representative groups, regarding proposed changes within the business. Consultation process can differ from Collective Agreements in that employee consultation can occur at any time in the year and about any topic great or small, and does not always have to result in agreement, rather than the regular, cyclical and usually constrained or specific nature of collective agreements which do have to result in agreement.
ERP-HR 23	ERP	ERP-HR	Manage Collective agreements	Functionality to Manage and record the negotiations between representatives of the employer and the employee, union representatives or workers council, to reach agreements on terms and conditions of employment. Agreements typically include determining compensation scales or rates, benefits, working hours, overtime, health & safety, training, and grievance mechanisms. Where costs are involved, this can involve taking away proposals and determining the likely cost before agreements are reached.
ERP-HR 24	ERP	ERP-HR	Manage Health and Safety	Functionality to support all processes regarding employee wellbeing and occupational health and safety. The health and safety processes residing within the HR process framework deal mainly in maintaining or increasing employee wellbeing, and reducing instances of occupational health problems via on-site or on-call occupational health professionals, insurance companies and employees.
ERP-HR 25	ERP	ERP-HR	Develop and Manage Reward, Recognition and Motivation	Functionality to support all processes involved with making sure that all employees are brought into the organization on the correct compensation package, and that this is reviewed according to a company policy and / or legal requirement. In addition to this, the organization will benchmark itself against competitors or similar organizations to ensure that its salaries are competitive. Finally, recognition policies should be reviewed along with reward structures, alongside benchmark information and internal metrics and engagement survey results, to ensure optimization against the HR and Reward strategy.
ERP-HR 26	ERP	ERP-HR	Develop and Manage Benefits	Functionality to support 'manage and administer benefits' process which includes delivering the employee benefits program, administering benefits enrollment, processing claims, and performing benefits reconciliation. (Benefits may be contractual or discretionary), payments to third party providing benefits.
ERP-HR 27	ERP	ERP-HR	Manage Retention	System to support all activities involved in making sure that steps are taken to decrease the likelihood of key employees, and their knowledge and skills, leaving the business. Conversely, it can also be necessary and healthy to encourage natural churn of employees out of the business, depending on key business drivers and specific knowledge and skills of the workforce.
ERP-HR 28	ERP	ERP-HR	Manage and Administer Payroll	Functionality to support payroll administration process which includes maintaining and administering the employee earnings and deduction information that is used to prepare payroll. Functionality to support various payroll components like but not limited to: • Basic salary • Dearness allowance • Housing • Card and conveyance • Long term reimbursements • Fringe benefits • Income tax • Tax on arrears • 3rd party deductions • Exemptions: like LTA, Medical reimbursements, Child education allowance, child hostel allowance, leave encashment, etc. • Professional tax • Provident Fund • Employee State Insurance • Labor welfare fund • Gratuity • Superannuation • Salary deductions like: day salary deduction etc.
ERP-HR 29	ERP	ERP-HR	Manage Promotion and	Functionality to support the process to manage promotion and demotion, which includes the administration and execution of employee promotion and

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
			Demotion Process	demotion. It also includes the processing of employee records and payroll and benefits transactions.
ERP-HR 30	ERP	ERP-HR	Manage Exit	Functionality to manage the separation process, which includes the administration and execution of employee separations. It includes the creation and generation of final payments, turnover reports, and vendor notification. This process also includes communications with former employees regarding benefits options
ERP-HR 31	ERP	ERP-HR	Manage Retirement	Functionality to Manage the retirement process, which includes management of the organization's retirement systems, tools, and processes. Once the retirement process is complete and if a decision to retire has been made, then the Manage Exit process deals with all the administrative activity surrounding a retiree leaving the business.
ERP-HR 32	ERP	ERP-HR	Manage Leave of Absence	System should manage leaves of absence process, which includes managing and administering the leave of absence policy for employees who are taking leaves in excess of their annual allowance.
ERP-HR 33	ERP	ERP-HR	Develop and Implement Employee Outplacement	Functionality to support the Develop and implement employee outplacement process, which involves creating, and providing career transition information and advice to employees whose roles have been eliminated.
ERP-HR 34	ERP	ERP-HR	Manage Reorganizations	Functionality to support all the processes involved with managing employee transfers into or outside the business, as well as reorganizations of business units and employees within the business.
ERP-HR 35	ERP	ERP-HR	Manage Workforce Reduction	Functionality to support the process which include an identification of areas of the business that require workforce reduction, before groups of employees are notified of potential risk of redundancy (termination of employment contracts). The process then focuses on procedures to identify which specific roles will be included/excluded in the future organization, and finally which employees will be selected for redundancy - whether voluntary or involuntary.
ERP-HR 36	ERP	ERP-HR	Manage Expatriates	Functionality to manage expatriates process which includes activities associated with both the expatriation and repatriation of employees within the organization.
ERP-HR 37	ERP	ERP-HR	Manage Employee Relocation Process	Functionality to manage employee relocation process which encompasses the execution of employee relocation using relocation systems, tools, and processes.
ERP-HR 38	ERP	ERP-HR	Manage Reporting Processes	Functionality to manage reporting process which consists of providing key HR data and reporting capabilities for the business to make use of. This should be a cohesive approach so that reports can be standardized and automated as much as possible to enable and encourage self-service reporting.
ERP-HR 39	ERP	ERP-HR	Manage Employee Query Process	Functionality to support manage employee enquiry process, which involves receiving, responding to, and recording information on employee inquiries. Efficiency of the process, system and use of data will be essential to ensuring a swift customer experience, with high levels of service and continuous improvement.
ERP-HR 40	ERP	ERP-HR	Manage and maintain employee data	Functionality to support the manage and maintain employee data process which includes making revisions to personal data such as changing beneficiary designations or employee status, as well as the effective capture and storage and sharing of data for use by the business and between business processes.
ERP-HR 41	ERP	ERP-HR	Develop and Manage Employee Metrics	Functionality to create measures to enable monitoring of employee KPIs such as time to hire, time to competence, employee turnover, engagement levels etc.. There will be close links, and often crossover with KPI measurements to improve the effectiveness of HR shared services and overall HR strategy.
ERP-HR 42	ERP	ERP-HR	Develop and Manage Time and Attendance Processes	Functionality to manage collecting, editing, approving, and entering data related to hours worked and paid time off.
ERP-HR 43	ERP	ERP-HR		Functionality to link closely to the data collected through employee engagement surveys, but likely to be more frequently tracked, based on

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
			Review Retention & Motivation Indicators	sentiment analysis, actual employee turnover data, productivity data and retention data (either gathered from managers or via predictive analytics systems).
ERP-HR 44	ERP	ERP-HR	Manage Employee Engagement	Functionality to manage the processes involved with creating and releasing employee engagement surveys, and then analysis of received data back to the business to support HR strategy, business unit action plans, learning and development planning etc..
ERP-HR 45	ERP	ERP-HR	Employee Self Service	Functionality to enable employees to carryout self-service functions like but not limited to: 1. Change certain self HR data 2. Timesheet entry 3. Apply expense claims 4. Apply for travel request 5. Manage Appraisals
ERP-HR 46	ERP	ERP-HR	Manager Self Service	Functionality to enable Managers to carryout self-service functions like but not limited to: 1. Approval of change certain HR data 2. Timesheet Approval 3. Expense claims Approval 4. Travel request Approval 5. Manage subordinates Appraisals
ERP-HR 47	ERP	ERP-HR	Starters/ Movers/ Leavers	Functionality to manage the process for Starters / Movers / Leavers via workflow and auto assignment of access to various systems based on the role assignment.
ERP-HR 48	ERP	ERP-HR	Integration	Integration with IBMS system to authenticate and allow access to a facility for all the DICDL complexes.
ERP-HR 49	ERP	ERP-HR	Integration	Integration with IBMS system to receive the 'IN' and 'OUT' times to populate the Timesheets.
ERP-PS 1	ERP	ERP-Project Systems	Plan, design and estimate Projects	Develop a dashboard to provide an overview of all or selected projects for senior management.
ERP-PS 2	ERP	ERP-Project Systems	Plan, design and estimate Projects	Application to prepare and maintain project or program plan which can be used and updated by multiple users simultaneously.
ERP-PS 3	ERP	ERP-Project Systems	Plan, design and estimate Projects	Ability to capture financial details of the projects executed in different categories.
ERP-PS 4	ERP	ERP-Project Systems	Plan, design and estimate Projects	Functionality to build a cost model for different types of projects or works based on the cost and expenses incurred on previous/ completed projects.
ERP-PS 5	ERP	ERP-Project Systems	Plan, design and estimate Projects	System to collect and compile information from various stakeholders for the analysis, feasibility assessment and continuous business justification or business case.
ERP-PS 6	ERP	ERP-Project Systems	Plan, design and estimate Projects	Functionality to prioritize investment for capital projects based on selected parameters and business outcome.
ERP-PS 7	ERP	ERP-Project Systems	Plan, design and estimate Projects	Functionality to monitor and manage progress of the projects.
ERP-PS 8	ERP	ERP-Project Systems	Plan, design and estimate Projects	Ability to document best practices and provide access for reference.
ERP-PS 9	ERP	ERP-Project Systems	Plan, design and estimate Projects	Functionality to communicate with stakeholders.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-PS 10	ERP	ERP-Project Systems	Plan, design and estimate Projects	Ability to manage health and safety of the staff and all stakeholders.
ERP-PS 11	ERP	ERP-Project Systems	Plan, design and estimate Projects	Functionality to manage project performance and risk. Ability to generate Earned Value (EV) based on progress of the projects. (Earned Value calculations require the following: - Planned Value (PV) = The budgeted amount through the current reporting period. Actual Cost (AC) = Actual costs to date. - Earned Value (EV) = Total project budget multiplied by the % complete of the project.)
ERP-PS 12	ERP	ERP-Project Systems	Approve Projects and programs	Ability to record or update project estimates, business case, project brief, project justification or cost benefit analysis report and a provision to upload other key documents which may be required for project or program approvals.
ERP-PS 13	ERP	ERP-Project Systems	Approve Projects and programs	Functionality to send a hyperlink to respective project documents or copy of the documents to relevant or designated managers/ officials for the approvals or review.
ERP-PS 14	ERP	ERP-Project Systems	Approve Projects and programs	Functionality to update and inform relevant or designated officials/ stakeholders, when the project/program is approved or rejected or progressed to next level for further approvals.
ERP-PS 15	ERP	ERP-Project Systems	Manage Project Performance	Functionality to track progress, resources and budget consumed for different durations and up to date.
ERP-PS 16	ERP	ERP-Project Systems	Manage Project Performance	Functionality to enter project data related to progress, KPIs, risks and resource utilization etc.
ERP-PS 17	ERP	ERP-Project Systems	Manage Project Performance	Ability to produce graphs and charts to present progress of the project graphically.
ERP-PS 18	ERP	ERP-Project Systems	Manage Project Performance	Dashboard which can be customized to monitor single and multiple projects with desired insights and KPIs.
ERP-PS 19	ERP	ERP-Project Systems	Manage Project Performance	Functionality to define, plan and monitor the Project based on hierarchical WBS structure. Functionality to define and plan dependencies, budgets and detailed network and activities for the WBS. Functionality to auto calculate the estimated cost based on planned resource and material/services assigned. Functionality to create various versions of cost estimates, with only one version active.
ERP-PS 20	ERP	ERP-Project Systems	Manage Project Performance	Functionality to roll up cost and revenue from lower level to higher level WBS.
ERP-PS 21	ERP	ERP-Project Systems	Manage Project Performance	Functionality to confirm time and material to WBS/network/activity. Actual cost to be calculated on the confirmation and goods/ service receipts.
ERP-PS 22	ERP	ERP-Project Systems	Manage Project Performance	Functionality to track scope of work for contracts, change of scope, claims and disputes and claim approvals.
ERP-PS 23	ERP	ERP-Project Systems	Manage Project Performance	Functionality to report on the stage and state of project, milestones, trend analysis, etc.
ERP-PS 24	ERP	ERP-Project Systems	Manage Project Performance	Functionality to provide comprehensive and flexible reporting system

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-PS 25	ERP	ERP-Project Systems	Integration	Integration may be required with other Project Portfolio Management applications.
ERP-PS 26	ERP	ERP-Project Systems	Manage Project Performance	Functionality for budget availability control for all project expenditures. Ability to break down initial budget to smaller packets for better cost controlling.
ERP-PS 27	ERP	ERP-Project Systems	Manage Project Performance	Functionality for back and forward scheduling considering the dependencies and constraints defined.
ERP-PS 28	ERP	ERP-Project Systems	Manage Project Performance	Functionality to enable precise planning, budgeting and monitoring of detailed activities costs of the project. Project accounting should fulfil below functions at various phases of the project: - Classify projects based on their types - Maintain Vendor details, schedule of rates - Calculate planned costs and revenues. - Technical and financial approval of project (via workflow) - Allocate budget based on planned costs - Integration with e-Tendering application - Awarding work to Vendor/s - Facility to track Project - Ability to upload / input measurement / progress of work - Monitor actual costs and its variance from planned cost - Facilitate local accounting standards - Calculate Work in Progress by asset class to enable recovery of capital taxation allowance - Cost and revenue settlement
ERP-IM 1	ERP/IM	Inventory Management	Organization structure	Functionality to define the required Organizational structure like but not limited to: - Company codes - Plants - Storage locations - Mobile storage locations
ERP-IM 2	ERP/IM	Inventory Management	Master data	Functionality to maintain Inventory related master data like but not limited to: - Material master (with information like serialized / non serialized, ABC category, FIFO/LIFO etc.) - Minimum inventory level - Procurement Lead times/ vendor - Purchasing unit - Batch data like batch no, expiry date - Vendor product codes - Bill of material - Standard value / Moving average value against material master
ERP-IM 3	ERP/SRM	Inventory Management	Configuration	Functionality to maintain conversion between units of measure
ERP-IM 4	ERP/IM	Inventory Management	Configuration	Functionality to configure Material Requirements planning parameters
ERP-IM 5	ERP/IM	Inventory Management	Configuration	Functionality to define material movement types/ transaction types and related account determination
ERP-IM 6	ERP/IM	Inventory Management	Configuration	Functionality to define stock types like unrestricted stock, Quality stock, reserved stock etc.
ERP-IM 7	ERP/IM	Inventory Management	Stores	Functionality to manage the stores functions like but not limited to: - Goods receipt - Goods transfer - Goods issue against requisitions, work orders, projects, consumption, replenishment of van stocks, user defined requisition types etc. - Generation of picking list - Printing of necessary documents in a predefined format - Quality inspection of goods receipt - Record inspection results and Rejection/Acceptance of Inspection lot - Bar code scanning and printing to tag stock or perform material movement - Material movement for items returned

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				- Cancellation of any of the material movements - Mass Upload material movement transaction from various file formats(xl/ csv/ txt etc.) - Scrap goods - dispatch goods against shipping notification - Track stock and value of inventory
ERP-IM 8	ERP/IM	Inventory Management	Van stocks	Functionality to manage Van stocks including functions like: - Goods receipts to Van stock - Goods issue from Van stock (issued against work order / projects / warehouse / other van stocks) - Replenish Van stock based on MRP considering the minimum stock levels - Consumption posting of goods from Van stock - Stock overview of Van stocks
ERP-IM 9	ERP/IM	Inventory Management	Material Movement	Functionality to update the value and quantity of stock based on the material transactions performed. Necessary controlling/ accounting documents needs to be posted by the system to relevant cost receivers / Accounts based on the movement type, system shall automatically determine the correct account / cost receiver. Functionality to manage the stock within the batch and serial no for serialized stock.
ERP-IM 10	ERP/IM	Inventory Management	Valuation	System shall allow valuation based on moving average value or standard price valuation based on the settings on the material master. System shall allow for split valuation for batch managed materials. Functionality to adjust standard price every year. Functionality for Month end processing for Inventory.
ERP-IM 11	ERP/IM	Inventory Management	Physical Inventory	Functionality to perform physical inventory count by providing functionality like but not limited to: - generation of count sheet - define cycle count frequency - approval for stock shortage/adjustment - identify stock shortage type (like shortage, damaged, non-usable etc.) - Post relevant costing/accounting documents
ERP-IM 12	ERP/IM	Inventory Management	Reporting	Functionality to generate various reports like but not limited to: - Stock overview report - Reorder point and forecast reports - Material transaction register - Damaged stock report - Material ageing report - Stock expiry report - physical Inventory variance report - Stock value and ABC analysis report - Nonmoving items report etc.
ERP-IM 13	ERP/IM	Inventory Management	Integration	Functionality to integrate with Analytics , BI/Data warehouse, mobile solution for field guys for inventory transaction, Procurement system, Finance and Controlling and other logistics modules like Asset Management, Projects Systems etc.
ERP-IM 14	ERP/IM	Inventory Management	Integration	Functionality to integrate with Weight-bridge and other related applications and perform Good Receipt based on the information received from these applications

Scope of Services for ERP, CRM, SRM, Asset Management and Utilities

- MSI shall document detailed requirements.
- MSI needs to document processes up to level 6 using a standard process documentation tool.
- All documents needs to be reviewed and approved by relevant authorities.
- MSI shall document the solution architecture related artifacts to cover areas like Application architecture, system architecture, component models, walk-through models, Data architecture, security architecture, infrastructure architecture, etc. These documents needs to be reviewed and approved by the relevant authorities.
- MSI shall document detailed solution design related artifact to cover areas like Functional specification, configuration, data model, technical specification, etc. These documents needs to be reviewed and approved by the relevant authorities.
- MSI shall be responsible to supply and install all required hardware/ software/ tools to meet the RFP requirement without any deviation. Any additional hardware or software necessary to meet the

technical, functional and performance requirement of the project but not mentioned in RFP shall be factored and supplied by MSI as part of this RFP without any additional cost to employer.

- MSI shall define the development and configuration standards. MSI shall be responsible to configure, build, enhance and customize the applications to ensure it meets the requirements without any deviations.
- MSI shall define in agreement with the relevant authorities the exit criteria for each type of testing. MSI shall perform all the necessary testing like Unit testing, System Integration testing, load and performance testing. MSI shall assist in user acceptance testing. MSI shall develop the test strategy and test scenarios to cover all the process variants and requirements. MSI shall use industry standard tools required for testing. MSI shall ensure that the minimum exit criteria (as agreed by the relevant authority) is met to conclude the completion of the testing. MSI shall manage and monitor all the stages of the testing. MSI shall document all the artifacts required for testing phase like, testing strategy, test plans, test scenarios, test results with evidences, test cycles, etc. These documents needs to be reviewed and approved by the relevant authorities.
- MSI shall manage the commissioning, deployment, roll out, intensive go-live support and transition of support to support team. All relevant documentation like Go-live plan, roll out plan, roll back plan, transition strategy, Service Management Transition document, Service support requirements etc. shall be provided by MSI. MSI shall ensure a smooth transition from deployment team to operate and maintain team.
- MSI shall be responsible for the training of trainers and end users and will provision for all the required documents and guides for training.
- MSI will be responsible for data collection, transition, data cleansing and data migration required for all the master and transaction data to be migrated to Production environment. MSI shall be responsible for the reconciliation of the data. MSI shall provide the necessary templates for data collection to DICDL. All relevant documentation like Data migration strategy, data cleansing and migration plan, Data Model, etc. shall be provided by MSI.
- MSI shall assist and anchor the ongoing benefit realization for DICDL.
- MSI shall provide the Operations and Maintenance Services for a period of 5 years from the date of Go-Live. It is continuous development process and no change request will be considered during the contract period.
- The MSI shall be responsible for following but not limited to:
 - Provide all necessary manpower resources onsite to manage and resolve any issues/incidents and carry out required changes, optimizations and modification
 - Responsible for identification, diagnosis and resolution of problem areas and maintaining the defined SLA levels.
 - Provision of skilled and experienced manpower resources to administer and manage solution.
 - Provision and management of the service management onsite tool to manage all the tickets in consolidated manner for all the city functions.
 - Interface shall be provided to capture the information from central management system (CMS) of Streetlights for automatically converting faults into tickets and upon resolution the necessary information to flow back about the needful having done. The MSI will have to study the central management system and work out the details for connecting CMS with CRM ticketing tool over SOA based ESB (Enterprise Service Bus would be part of ERP suite of applications).
 - Periodic health checks of the systems and applications to ensure the system performance.
 - Users and authorization management
 - Periodic system patching and upgrade as recommended by the application vendor.
 - Management and maintenance of integrated environments like Development environment, Testing environment, Production environment and Training environment.
 - Management and maintenance of configuration, development and data on these

environments.

○ Users and authorization management

- The MSI shall arrange for environments and tools for testing and for training as envisaged.
- Production environment should never be used for testing and training purpose. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected MSI.
- The MSI is responsible for all tools/environment required for testing and sufficient training shall be given.
- MSI shall provide a well-prepared build documentation / user manual for users, also a clear plan for user training, education & hands training on installed solution.
- MSI is also responsible to deliver all documents approaches for entire solution with proper training and knowledge transfer.
- MSI shall adhere to the agreed SLA for deployment and operate and maintain.

SRM

Procurement module should support functional services such as Supplier Portal, Strategic Sourcing, Self-Service Procurement, Supplier Qualification Management, Procurement Contracts Management, Purchasing, Analytics and Reporting (Management Information and Operational Analytics and Reporting).

Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-PR 1	ERP/SRM	Procurement	Organization structure	Functionality to define the required Organizational structure like but not limited to: - Company codes - Purchasing Organization - Purchasing Groups - Plants - Storage locations - Profit centers / cost centers etc.
ERP-PR 2	ERP/SRM	Procurement	Master data	Functionality to manage and maintain various master data entities required for Procurement like but not limited to: - Material Master including configurable material masters - kits - Service Master - Vendor Master - Bill of Material - Preferred Vendors, list prices and lead times - Product catalog - Purchase Agreements - Purchase info records - Inspection plans etc.
ERP-PR 3	ERP/SRM	Procurement	Configuration	Functionality to configure various Purchase order types, account assignment categories, Vendor evaluation criteria's, material types, tax procedures, pricing procedures etc.
ERP-PR 4	ERP/SRM	Procurement	Purchase Requisition	Functionality to raise Purchase requisition / shopping cart from other objects like Service order / work order / Projects / sales orders etc.
ERP-PR 5	ERP/SRM	Procurement	Purchase Requisition	Functionality for authorized DICDL users to raise a shopping cart request using a product catalog and appropriate account assignment for goods and services like but not limited to spares, office equipment and supplies, essential services and others as per DICDL needs.
ERP-PR 6	ERP/SRM	Procurement	Purchase Requisition	Functionality to monitor the status of the purchase requisitions raised. Functionality to attach various documents to the header and/or line items of the PR/PO/RfQ/RFP/Quotes/Proposals etc.

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-PR 7	ERP/SRM	Procurement	Purchase Requisition	Functionality to create purchase requisition and purchase orders for wholesale energy, water procurement and Gas.
ERP-PR 8	ERP/SRM	Procurement	Planning	Functionality to do Materials Requirement planning based on below criteria's:- - Consumption based planning (reorder point) - Requirement based planning - Forecast based planning
ERP-PR 9	ERP/SRM	Procurement	Receive and evaluate Quote	Functionality to create request for Quotation against the purchase requisitions, electronically send these requests to multiple suppliers, enter the quotes received with requisite details and attachments. Functionality to technically and functionally analyze and evaluate received quotations from various vendors based on criteria's like but not limited to: -Lowest price -Technical proposal -Delivery -Quality -Payment terms -Landed costs etc. - Functionality to convert/copy the whole or partial quotation/proposal based on the above evaluation.
ERP-PR 10	ERP/SRM	Procurement	Approval	Functionality to have workflow based multi-level PR approval procedure based on the value of the PR, PR raised by etc. based on the powers vested in signing authorities.
ERP-PR 11	ERP/SRM	Procurement	Purchase Orders	Functionality to convert PR to PO, using preferred vendors and source lists once PR is approved. Functionality to integrate with E-Procurement portal for managing the tender process. Once the tender has been awarded to a vendor, PO shall be created in ERP system. Functionality to consolidate multiple Purchase requisitions. Functionality to create multiple purchase orders for a single purchase requisition. Functionality to create purchase orders in different currencies.
ERP-PR 12	ERP/SRM	Procurement	Purchase Orders	Functionality to create long term contracts with validity time scale, limiting value and/or quantity. Functionality to have multiple releases against the long-term contracts.
ERP-PR 13	ERP/SRM	Procurement	Purchase Orders	Functionality to maintain prices, various taxes as per the tax rules, discounts, delivery instructions, other relevant attachments, delivery schedule, freight, insurance, penalty clause(% of value, daily rate or lump sum), carriage cost, transport costs etc. in the purchase orders / release orders at header / line item level.
ERP-PR 14	ERP/SRM	Procurement	Purchase Orders	Functionality to send the purchase order / release order / purchase requisition / amendments / shipment follow ups via various mediums like electronic, paper, Fax etc. Any reprints should clearly state that it's a copy.
ERP-PR 15	ERP/SRM	Procurement	Purchase Orders	Functionality to capture follow up dates, comments, follow up activities with comments for critical or delayed purchase orders.
ERP-PR 16	ERP/SRM	Procurement	Integration	Functionality to integrate with E-Procurement portal including e-bidding for tendering process and creation of Purchase order on allocation of the order to the Vendor.
ERP-PR 17	ERP/SRM	Procurement	Integration	Integration with Project Systems, Asset Management, production, utilities, sewage management system and other core DICDL functions for triggering of Procurement.
ERP-PR 18	ERP/SRM	Procurement	Goods and Service Receipt	Functionality to post goods and service receipts against the purchase orders. Functionality to perform and report mandatory quality inspection on incoming goods. Functionality to update inventory on goods receipt and quality clearance. Functionality to generate necessary document on goods receipts. Functionality to return the goods and update inventory in case if the quality inspection fails. Functionality to receive un-ordered or substitute goods based on appropriate business authorization.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-PR 19	ERP/SRM	Procurement	Goods and Service Receipt	Functionality to receive the serialized and batch managed products with relevant data attributes like serial numbers, batch details, expiry dates etc.
ERP-PR 20	ERP/SRM	Procurement	Goods and Service Receipt	Functionality to record receipt of service and labor in terms of hours against a purchase order/ service order / project or cost center.
ERP-PR 21	ERP/SRM	Procurement	Invoice Receipt	Functionality to create Invoice receipts in the system, validate the correctness of the invoice receipt. Functionality to scan the invoice receipt and automatically generate the IR in the system with the scanned document attached to the IR. Functionality to manually enter the IR.
ERP-PR 22	ERP/SRM	Procurement	Invoice Verification	Functionality to verify the content, taxes, prices against the PO. Functionality to have automated 3 way Invoice Verification performed before release of the payments, for any discrepancies above the set tolerances, a workflow needs to be triggered for multi-level approval procedure based on the value of the Invoice. Functionality to trigger an approval workflow for IR's above a certain values for multi-level approvals. Functionality to control the approval process as per governance standards. System shall block the invoices with appropriate blocking reasons if any discrepancies are identified. The invoice blocks should be removed only by authorized users after verification.
ERP-PR 23	ERP/SRM	Procurement	Finance and controlling	Functionality to integrate with Finance and Controlling modules to automatically post the accounting/ costing documents by automatically determining the accounts and purchase order line item account assignment when a relevant transaction is performed like but not limited to goods/services receipts, invoice verification, payment, etc.
ERP-PR 24	ERP/SRM	Procurement	Reporting	Functionality to generate various reports for Purchasing and contract management like but not limited to: - Purchase Requisition status - Quotes/ proposals received - Purchase order stages / statuses - Pending commitments against purchase orders - Consolidated discounts against the contracts - Quality inspection report - Vendor evaluation - GR/IR report - Blocked Invoice Receipts report - Payment report

Customer Relationship Management

Main function of CRM will be to serve as Citizen's Interaction Centre (CIC). Hence, all the necessary orientation in respect of configuration and customization will meet the objective of CIC besides other functions foreseen.

CRM system needs to keep customer's contact details up to date, track every interaction they have with DICDL, and manage their accounts. CRM system should mainly improve customer relationships, and in turn, customer lifetime value, help to serve customer faster and more efficiently and enable 'Ease of doing business' for DICDL. CRM system should enable multi-channel interactions with customers. CRM system should be able to track the history of all interactions with the customers: phone calls made, emails sent, meetings held, presentations delivered, enquiries and complaints received/resolved to enable every contact with customer always personal, relevant and up to date. CRM application should integrate with CMS application for managing, controlling and receiving information and status for the streetlight by way of ESB integration.

Functional and Technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CRM 1.0	CRM	CRM	Configuration	Functionality to configure various attributes like but not limited to: - Departments - multi level Interaction categorizations - Tasks codes with default SLA - Inbound and outbound channels - Defects / Impacts / type of work / Issues categories - Customer categorization - Scripts definition with questions, options and related question for each option - Standard outputs - Scripts for Email response Management (ERMS) - various tasks with SLA's for a type of request - Document / Attachment types - Activity types - Inbound / outbound email addresses - IR / case priorities
CRM 1.1	CRM	CRM	Configuration	Functionality to configure screens and menu based on user roles and profiles.
CRM 2.0	CRM	CRM	Master Data	Functionality to manage and maintain time-sliced Customer data for every citizen and organization like but not limited to: - Personal details - Organizational details - Categorization details - address details - Property details - citizen details like Aadhaar card no, pan no etc. - Communication data
CRM 2.1	CRM	CRM	Master Data	Functionality to manage and maintain time-sliced Property/plot data like but not limited to: - Address - owner - status - property categorization - Applicable tax - Map / plan - GIS TOID reference number
CRM 2.2	CRM	CRM	Master Data	Functionality to manage and maintain Asset data for all the ICT assets like but not limited to: - Asset details like categorization, serial no, location, make and model etc. - Reference no like GIS reference, asset registry no etc. - Asset status
CRM 2.3	CRM	CRM	Master Data	Functionality to manage and maintain Organization and call center agents data like but not limited to: - Agent name and ID - Department - Organization etc.
CRM 3.0	CRM	CRM	Interaction Center	Functionality to capture all the inbound and outbound interactions with customer via various channels like: - Telephone call - Email - Self-Service Portal - Mobile App - In-person visit - Letter - SMS etc.
CRM 3.1	CRM	CRM	Interaction Center	Functionality to capture various interaction details like but not limited to: - Customer details - Asset details - Property details - Hierarchical Categorization of Problem/complaint/application - Problem/complaints/application detailed description - Communication channel - Attachments - Internal and external notes

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				- Agents/ person responsible for the interaction - Department managing the request - SLA details - Date and time of customer interaction
CRM 3.2	CRM	CRM	Interaction Center	Functionality to automatically generate interaction record for inbound communication from customer like email or application via mobile app or website and auto assignment of department and person responsible to process the customer request.
CRM 3.3	CRM	CRM	Interaction Center	Functionality to automatically determine the tasks and SLA based on the categorization of the request and assign agent for respective tasks.
CRM 3.4	CRM	CRM	Interaction Center	Functionality to stop the SLA clock when awaiting on customer for further required details.
CRM 3.5	CRM	CRM	Interaction Center	Functionality to attach other documents like letters, plans, forms etc. to the interaction record
CRM 3.6	CRM	CRM	Interaction Center	Functionality to link various interactions together.
CRM 3.7	CRM	CRM	Interaction Center	Functionality to maintain various templates for letter / SMS / emails / Forms and auto-populate the data in these templates to generate standard outbound communication/interaction.
CRM 3.8	CRM	CRM	Interaction Center	Functionality to integrate with SMS/email gateway to send outbound communication and record the details of the outbound communication in CRM system
CRM 3.9	CRM	CRM	Interaction Center	Functionality to integrate with digital signature for every inbound and outbound communication.
CRM 3.10	CRM	CRM	Interaction Center	Functionality to create adhoc tasks with all the required details; link it to interaction record / case and assign it to a department or user along with SLA.
CRM 3.11	CRM	CRM	Customer identification	Functionality to identify customer based on various inputs like but not limited to: - Aadhaar card no / Pan card no - Address / First and last name - Citizen's smart card reference no - Functionality to authenticate the customer with set of questions.
CRM 3.12	CRM	CRM	Asset Identification	Functionality to identify Asset / Property based on various inputs like but not limited to: - Identification on GIS based on location details - Asset no - Property address / reference no - Type of asset and location
CRM 3.13	CRM	CRM	Customer information	Functionality to provide a view of all the customer transactions on a single screen relevant to the categorization of customer request like but not limited to: - Previous inbound and outbound interactions (closed and open) - Invoice and Payment history and related details - Related Property and its details - Any existing events in the vicinity of the address like repairs/ outages etc. - Utility meter and meter reading details - Other contracts/lease for the customer and its relevant details - Functionality to drill down further from this screen into the details of the transactions
CRM 3.14	CRM	CRM	Script	Functionality to configure the Scripts for call center agents. The script shall provide right questions to be asked and based on the options selected by customer dynamically propose the next question. The script should at the end create an interaction record and based on the request shall integrate with other relevant systems to create an application / work order/ sales order.
CRM 3.15	CRM	CRM	Case Management	Functionality to create a case and automatically capture the case attributes from the main interaction. Manage the case with person responsible / department etc. Assign various inbound/outbound interaction to the case.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CRM 3.16	CRM	CRM	Case Management	Functionality to create hierarchy of cases and link various cases
CRM 4.0	CRM	CRM	Integration	Functionality to integrate with eGov applications to create / update / view various eGov applications for the customer. CRM should be able to integrate and provide drill down functionality to view the updates, progress, status and SLA on the eGov applications.
CRM 4.1	CRM	CRM	Integration	Functionality to integrate with GIS application to be able to locate asset, use location services to locate property and view current planned and in-progress events with status and SLA in the vicinity which would impact the customer. Selected asset on GIS should be transferred to the Interaction record in CRM.
CRM 4.2	CRM	CRM	Integration	Functionality to integrate with ERP application to create / update / view customer related transactions like but not limited to: - Sales Orders, Quotations, Invoices, Debit and Credit notes - Contracts - Work orders for Asset Management - Customer ledger, Payments, Debts and open balances Functionality to drill down into the related transactions in ERP system.
CRM 4.3	CRM	CRM	Integration	Functionality to integrate with Utility systems to be able to create / update / view customer related transactions like but not limited to: - Utility account - Meter reads - Bills - Payments - Balances and account statements - Other utility related requests with status like transfer, Move-In, new connection, disconnection etc. - Consumption
CRM 4.4	CRM	CRM	Integration	Functionality to integrate with Master Data Management applications to: - Initiate data update to other system for master data entities or attributes mastered in CRM system - Update of Data in CRM system which are mastered in other systems.
CRM 4.5	CRM	CRM	Integration	Functionality to integrate with Workflow application to be able to: - Initiate workflow on certain configured events being triggered from CRM - Initiate/Update CRM transaction like interactions / tasks / alerts / case / outbound interaction etc. based on action taken for a work item task. - View CRM transaction details in the workflow application for investigation by the work item agent
CRM 4.6	CRM	CRM	Integration	Functionality to integrate with Smart Waste Management Application to be able to locate SWM asset, Schedule waste collection process, view waste collection schedule.
CRM 4.7	CRM	CRM	Integration	Functionality to integrate with Scheduling application to be able to locate relevant mobile assets, available slots for appointment booking, book customer appointment, details of the work orders, schedules for the work order etc.
CRM 4.8	CRM	CRM	Integration	Functionality to integrate with Payment Gateway application to be able to process customer payments via cards (Debit / credit / smart cards / Payment Wallets and various other payment methods) to: - Receive payments in a secured way considering data protection and PCI compliance - Make refunds - View payment status and history
CRM 4.9	CRM	CRM	Integration	Functionality to integrate with Emergency and Disaster Management application to be able to initiate / update / view E&DM requests for the customer.
CRM 4.10	CRM	CRM	Integration	Functionality to integrate with Document Management / Content Management application to be able to create / update / view any documents / attachments against customer interaction / case. Functionality to store the urn links to the related documents from the DMS/CMS.
CRM 4.11	CRM	CRM	Integration	Functionality to integrate with IVR application to be able to display the relevant customer screen on the call center agents display as soon as the call is taken by the agent.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CRM 4.12	CRM	CRM	Integration	Functionality to integrate with SMS and Email exchange gateways for inbound and outbound communications with attachments. Inbound Email and SMS shall be received by the CRM application and routed and processed by the ERMS (Email response Management system) component of CRM.
CRM 4.12	CRM	CRM	Integration	Functionality to integrate with Scanner. All the paper based interactions (applications/ complaints / requests) received needs to be scanned along with all the attached documents; the scanner shall integrate with CRM application to create a skeleton Interaction record with scanned documents as attachments. These interaction records shall be grouped by department and to be updated and processed via the back office function.
CRM 5.0	CRM	CRM	Reporting	Functionality to be able to generate real-time reports for customers like but not limited to: - Interactions - SLA monitoring of IR / tasks / alerts etc. by agents, departments, group, request types etc. - Complaints and resolution - IR statuses and historical changes / updates - Cases for SLA monitoring, status, completion etc. - Statistical reports on complaints, requests, applications and its closer per department, agent, type of request, compliance, period etc.
CRM 5.1	CRM	CRM	Reporting	Functionality to be able to generate real-time reports for agents like but not limited to: - Interactions - Worklist of IR / tasks / alerts/ cases etc. by priority and SLA lapse time. - Complaints and resolution - IR statuses and historical changes / updates - Cases for SLA monitoring, status, completion etc. - Statistical reports on complaints, requests, applications and its closer per department, agent, type of request, compliance, period etc.
CRM 5.2	CRM	CRM	Reporting	Functionality to be able to generate real-time reports for departments / groups like but not limited to: - Interactions - SLA monitoring of IR / tasks / alerts etc. by agents, departments, group, request types etc. - Complaints and resolution - IR statuses and historical changes / updates - Cases for SLA monitoring, status, completion etc. - Statistical reports on complaints, requests, applications and its closer per department, agent, type of request, compliance, period etc.
CRM 5.3	CRM	CRM	Reporting	Functionality to be able to generate management reports like but not limited to: - Compliance - Complaints and resolution - IR statistics - Cases for SLA monitoring, status, completion etc. - Statistical reports on complaints, requests, applications and its closer per department, agent, type of request, compliance, period etc. - Customer satisfaction - First time resolution etc.

Non-Functional requirements for ERP, SRM and CRM

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR 1.0	ERP, SRM and CRM	Non Functional requirement	Service Support	For all the critical applications in the portal service support is require. Any priority 1 incident should be resolved in 3 hours. Priority 2 incidents should be resolved in 5 hours. Priority 3 incidents should be resolved in 16 hours. Priority 4 incidents should be resolved in 40 hours. All the MIS requirements required shall be provided by the Service Support function once the new system is live. Daily health checks should be performed

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				and published on the above systems to ensure their availability and performance.
NFR 1.1	ERP, SRM and CRM	Non Functional requirement	Service Support	System housekeeping, maintenance resulting in system downtime or partial unavailability should be performed during the low usage window of the application in consideration.
NFR 1.2	ERP, SRM and CRM	Non Functional requirement	Operational Window	Where the systems are expected to employ batch/background processing, the batch/background processing should be scheduled and completed outside of the service window of the application to reduce the impact on the users
NFR 1.3	ERP, SRM and CRM	Non Functional requirement	Operational Window	For all the external interfaces, based on type of interface and the need, system should restrict receiving, sending or processing external data in a selected time window.
NFR 1.4	ERP, SRM and CRM	Non Functional requirement	Performance	All synchronous interfaces should have a response time of < 3 seconds
NFR 1.5	ERP, SRM and CRM	Non Functional requirement	Operational Window	Peak usage hours for the system are expected to be 09:00 – 18:00 Monday to Friday.
NFR 1.6	ERP, SRM and CRM	Non Functional requirement	Background processing	As this is an online system there is no batch window. The overnight interface file sent from Insight needs to be received and imported prior to the start of peak hours.
NFR 1.7	ERP, SRM and CRM	Non Functional requirement	System Security	All applications should provide • Physical Security • Access Security • Data Security System architecture shall Consider each type of security from the perspective of: • Malicious attack, including service denial • Technical Failure • Privacy and confidentiality of information • System reconstruction • Support for Business Continuity Plans and Strategies Internal security should support the following security standards: • SAML 1.1 and SAML 2.0 • SAML Bindings 1.1 (SOAP binding) • WS-Security: SOAP Message Security 1.0 • WS-Security Username Token Profile 1.0 • WS-Security SAML Token Profile 1.0
NFR 1.8	ERP, SRM and CRM	Non Functional requirement	System Security	System must authenticate user login's with the AD server If user logon id has not been authenticated with AD server, system must give error message and stop logging into the application
NFR 1.9	ERP, SRM and CRM	Non Functional requirement	System Security	System should be able to hold various roles for different users and provide authorizations required for the roles assigned.
NFR 1.10	ERP, SRM and CRM	Non Functional requirement	Disaster Recovery	During Disaster recovery period, application will setup in the failover location and it must access from this location. All the business functionality and data that is available in the primary server must be available for the users.
NFR 1.11	ERP, SRM and CRM	Non Functional requirement	Data Security & Auditability	All the master and transaction data should be protected from un-authorized access. Data should be backed up daily. In case data getting corrupted, it should be restored within 8 hours. All data changes should logged, and system should provide functionality to trace the data changes. Systems should provide complete auditability of data changes. Any data transmitted, should be encrypted.
NFR 1.12	ERP, SRM and CRM	Non Functional requirement	Upgrade	All applications should be upgraded to recommended versioning in compliance with manufacturer's upgrades and warranties. All upgrades should be performed and tested on development and test environment first and tested. Only on acceptance of testing the upgrade should be performed on the production environment.
NFR 1.13	ERP, SRM and CRM	Non Functional requirement	Scalability	All the applications and processes should be scalable to accommodate increase in users and data as the city population grows. System should allow to enhance the processes and further automation in future.
NFR 1.14	ERP, SRM and CRM	Non Functional requirement	Performance	System response time for user on transaction screens < 3 seconds Response time for simple query < 4 seconds Response time for complex query < 5 seconds

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR 1.15	ERP, SRM and CRM	Non Functional requirement	Data integrity	System and its design should assure the accuracy and consistency of data, over its entire life-cycle, and is a critical aspect to the design, implementation and usage of the system which stores, processes, or retrieves data. Data should be mastered in single application and synchronized with other related applications. Any exceptions in data synchronization should be highlighted and managed by support team.
NFR 1.16	ERP, SRM and CRM	Non Functional requirement	Usability	Applications screens should be intuitive and provide ease of use for users. User experience and consistent screen design should be key considerations. Appropriate online help should be provided on the screens. Error messages should be clear and precise.
NFR 1.17	ERP, SRM and CRM	Non Functional requirement	Reliability	System and its various components should function under stated conditions for the life span of the application.
NFR 1.18	ERP, SRM and CRM	Non Functional requirement	Supportability	All the systems and its components should be supportable.

City Asset Management

Integrated City Asset Management module should support functional services such as Asset Maintenance, Asset Replacement, Asset installation and commissioning, Field resource management, Contracts Management, Contractors delivery, Work execution, Analytics and Reporting (Management Information and Operational Analytics and Reporting).

Functional and Technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-AM 1	ERP	Manage Asset	Organization structure	Functionality to define the organization structure like the maintenance planning plant, maintenance plant. Functionality to support centralized as well as de-centralized maintenance planning.
ERP-AM 2	ERP	Manage Asset	Configuration	Functionality to configure various work order types, settlement profiles, work order and operation statuses, operation control keys, requirement profiles, scheduling profile etc.
ERP-AM 3	ERP	Manage Asset	Master Data	Functionality to maintain the Asset registry for all the city assets across all the domains like but not limited to: 1. Water/Sewage network assets 2. Water/Sewage treatment plant assets 3. CIOC assets 4. Traffic management network assets 5. Street lighting poles and electricity distribution related assets 6. Bus stops and transport related assets 7. Network and plant assets for waste management 8. City signage and kiosks 9. Fiber Network related assets 10. Citywide Wi-Fi related assets 11. Sensors and other environment monitoring assets 12. any other DICDL owned network or plant assets
ERP-AM 4	ERP	Manage Asset	Master Data	Functionality to define the technical objects structure like but not limited to: 1. Function locations, Function location hierarchy and its BOM 2. Equipment and its BOM 3. Production resource tools 4. Object links 5. Installed base 6. Equipment/ Function location task lists 7. Maintenance strategies 8. Maintenance package 9. Measuring points
ERP-AM 5	ERP	Manage Asset	Master Data	Functionality to define work centers and its hierarchy, assignment of resources to the work centers, scheduling and planning parameters for the work center, cost center for the work center, activities and activity rates etc.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-AM 6	ERP	Manage Asset	Master Data	Functionality to capture various attributes for the technical objects based on its classification, serial no, Vendor warranty details, manufacturer details, manufacturers drawings and other specification documents.
ERP-AM 7	ERP	Manage Asset	Master Data	Functionality to capture the task lists for technical objects with all the relevant details, maintenance plans with single / multi cycle plans.
ERP-AM 8	ERP	Manage Asset	Preventive Maintenance	Functionality to setup Preventive Maintenance plans based on the manufacturers recommendations. Functionality to fine tune the maintenance frequencies to optimize maintenance costs. Functionality to define various maintenance planning strategies like periodic maintenance, maintenance based on measuring points or a combination of both.
ERP-AM 9	ERP	Manage Asset	Preventive Maintenance	Functionality to create preventive maintenance work orders automatically at configurable number of days in advance to allow for necessary planning. The work orders should be created with the correct operations pertaining to the maintenance schedule indicating clearly the activities to be performed, skill set required, planned duration and work and any permits required to perform the work, priority, work center etc.
ERP-AM 10	ERP	Manage Asset	Planning	Functionality to plan the resources required to perform the maintenance of the assets. Functionality to look up the worklist of work orders that can be grouped together, based on location, priority, due date etc. Functionality to plan and arrange for the required permits if applicable to perform the maintenance activities. Functionality to book Customer appointments based on the availability using scheduling application.
ERP-AM 11	ERP	Manage Asset	Breakdown maintenance	Functionality to create breakdown maintenance work orders with the correct asset, location, breakdown description, work center to perform the repair, duration and work, required skill set, operations details etc.
ERP-AM 12	ERP	Manage Asset	Breakdown maintenance	Functionality to create work orders from CRM system when an issue is reported by citizen / customer via the call center, by capturing the correct asset number (by using GIS, or location search functionality) , details of the issue, work center, details of the operations to be performed, skill set required, duration and work.
ERP-AM 14	ERP	Manage Asset	Execution	Functionality to update the status of the work order at work order/operations level. Functionality to create further work request from field / back office. Functionality to update the comments from the field and other update forms. Functionality to create operations for external contractors to perform the repair and maintenance activities. Functionality to capture various statuses from field like Enroute, Health and Safety analysis performed, work in progress, abandoned, cancelled, completed etc. Functionality to perform and capture the Health and Safety assessment being carried out in the field and take corresponding action based on the risk score.
ERP-AM 15	ERP	Manage Asset	Contractors	Functionality to create operations for the contractors to perform. Functionality to create PR and subsequently PO for the work and services required assigned to the contractor. Functionality to select the right contractor to perform the work. Functionality for the contractors to update the progress and other details related to the work. Contractors should not be able to create additional payable work for themselves, without being approved by DICDL users. Functionality for DICDL users to authenticate and approve (multi-level approval based on the value) the work to be performed by the contractors before the PO can be released.
ERP-AM 16	ERP	Manage Asset	Completion	Functionality to report back the work performed, confirm the labor and materials consumed. Functionality to generate the actual cost for the work order. Functionality to update the completion status. Functionality to generate revenue related billing, settle the work order costs based on the cost receiver assigned, verify the services performed by the contractors and confirm the same, approve and release the payments to the contractors based on the work performed.
ERP-AM 17	ERP	Manage Asset	Integration	Integrate with various applications like but not limited to: 1. CRM - to create work order and update the status back from work management system to CRM system. 2. GIS - to select the correct asset, the location details and help field resources with the necessary spatial information and other asset attributes. 3. SRM- to integrate the purchasing functionality to enable R&M contractors to perform the work and be paid 6. IoT/SCADA- to be able to generate breakdown work orders based on the inputs received from the IoT devices in the field.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-AM 18	ERP	Manage Asset	Reporting	Functionality to generate various report like but limited to: 1. worklist reports based with ability to prioritize the work based on various criteria and monitor and plan the work execution. 2. Cost reports to analyze the planned and actual costs on the work orders 3. Work order status reports 4. Field resource utilization reports 5. Production Resource utilization reports 6. Missed SLA reports 7. Asset availability reports, Mean time to repair and mean time between repair 8. Other PMIS reports with roll up functionality based on the Installed base hierarchy
ERP-AM 19	ERP	Manage Asset	Warranty Management	Functionality to execute the Vendor warranty process if the asset is broken-down within the warranty period. Functionality to update and track the warranty process.
ERP-AM 20	ERP	Manage Asset	SCADA integration	Functionality to be able to convert SCADA alarms into breakdown work orders with the correct information about the asset and type of issue, priority etc.
ERP-AM 21	ERP	Manage Asset	Execution	Functionality to report time spent on work order. Functionality to capture time that field resource travels, arrives on job site, departs from job site after completion (via status change or other functionality).
ERP-AM 22	ERP	Manage Asset	Execution	Functionality to view all the job details, historical work done for the same asset, appointments, customer details, attachments etc.
ERP-AM 23	ERP	Manage Asset	Execution	Functionality to update status, comments and other forms like but not limited to: 1. Raise further work 2. Asset update 3. Health and Safety Assessment 4. Replace / Return Asset 5. Request for additional resources 6. Request for material / service 7. Consume material from van stock 8. Time confirmations 9. Leave / absence request 10. Expense claims 11. Stock availability 12. Update measuring points 13. Inspection check lists 14. Survey etc.
ERP-AM 24	ERP	Manage Asset	Operations	Functionality to attach files to work orders.
ERP-AM 25	ERP	Manage Asset	Execution	Functionality to capture photos taken while a work order is being completed should automatically be associated with the work order.
ERP-AM 26	ERP	Manage Asset	Operations	Functionality to record history, especially for time and material jobs, including status change history.
ERP-AM 28	ERP	Manage Asset	Scheduling	Functionality to prevent assignment of work to specific inspectors or authorized contractors, based on configurable business rules (lapsed credentials, etc.).
ERP-AM 29	ERP	Manage Asset	Scheduling	Functionality to assign work by the system directly to inspectors.
ERP-AM 30	ERP	Manage Asset	Operations	Functionality to subject some work orders to supervisor review and assignment.
ERP-AM 31	ERP	Manage Asset	Operations	Functionality to have review queues for supervisors to review the work done by inspectors in the field.
ERP-AM 32	ERP	Manage Asset	Operations	Functionality to triage queues for accounts that require manual intervention.
ERP-AM 33	ERP	Manage Asset	Security	Functionality to have role based access privileges.
ERP-AM 34	ERP	Manage Asset	Execution	Functionality to create a service order from another service order.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
ERP-AM 38	ERP	Manage Asset	Security	Functionality to provide administrative tools for managing user profiles and permissions.
ERP-AM 39	ERP	Manage Asset	Reporting	Functionality to provide for standard statistical reports by order type, field personnel, service center, etc.
ERP-AM 42	ERP	Manage Asset	Operations	Functionality for mass-creation of work orders through spreadsheet or upload.
ERP-AM 43	ERP	Manage Asset	Planning	Functionality to assign costs to types of work.
ERP-AM 44	ERP	Manage Asset	Operations	Functionality to associate a specific list of parts with a work group.
ERP-AM 45	ERP	Manage Asset	Reporting	Functionality to report on total costs per work group per month for approved work.

Non-Functional requirements for ERP and CRM

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR 1.0	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Service Support	For all the critical applications in the portal service support is require. Any priority 1 incident should be resolved in 3 hours. Priority 2 incidents should be resolved in 5 hours. Priority 3 incidents should be resolved in 16 hours. Priority 4 incidents should be resolved in 40 hours. All the MIS requirements required should be provided by the Service Support function once the new system is live. Daily health checks should be performed and published on the above systems to ensure their availability and performance.
NFR 1.1	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Service Support	System housekeeping, maintenance resulting in system downtime or partial unavailability should be performed during the low usage window of the application in consideration.
NFR 1.2	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Operational Window	Where the systems are expected to employ batch/background processing, the batch/background processing should be scheduled and completed outside of the service window of the application to reduce the impact on the users
NFR 1.3	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Operational Window	For all the external interfaces, based on type of interface and the need, system should restrict receiving, sending or processing external data in a selected time window.
NFR 1.4	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Performance	All synchronous interfaces should have a response time of < 3 seconds
NFR 1.5	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Operational Window	Peak usage hours for the system are expected to be 09:00 – 18:00 Monday to Friday.
NFR 1.6	ERP,SRM,AM , CRM & ISU	Non Functional requirement	Background processing	As this is an online system there is no batch window. The overnight interface file sent from Insight needs to be received and imported prior to the start of peak hours.
NFR 1.7	ERP,SRM,AM , CRM & ISU	Non Functional requirement	System Security	All applications should provide • Physical Security • Access Security • Data Security System architecture shall Consider each type of security from the perspective of: • Malicious attack, including service denial • Technical Failure • Privacy and confidentiality of information • System reconstruction • Support for Business Continuity Plans and Strategies Internal security should support the following security standards: • SAML 1.1 and SAML 2.0 • SAML Bindings 1.1 (SOAP binding)

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				• WS-Security: SOAP Message Security 1.0 • WS-Security Username Token Profile 1.0 • WS-Security SAML Token Profile 1.0
NFR 1.8	ERP,SRM,AM, CRM & ISU	Non Functional requirement	System Security	System must authenticate user login's with the AD server. If user logon id has not been authenticated with AD server, system must give error message and stop logging into the application.
NFR 1.9	ERP,SRM,AM, CRM & ISU	Non Functional requirement	System Security	System should be able to hold various roles for different users and provide authorizations required for the roles assigned.
NFR 1.10	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Disaster Recovery	During Disaster recovery period, application will setup in the failover location and it must access from this location. All the business functionality and data that is available in the primary server must be available for the users.
NFR 1.11	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Data Security & Auditability	All the master and transaction data should be protected from un-authorized access. Data should be backed up daily. In case data getting corrupted, it should be restored within 8 hours. All data changes should be logged, and system should provide functionality to trace the data changes. Systems should provide complete auditability of data changes. Any data transmitted, should be encrypted.
NFR 1.12	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Upgrade	All applications should be upgraded to recommended versioning in compliance with manufacturer's upgrades and warranties. All upgrades should be performed and tested on development and test environment first and then tested. Only on acceptance of testing the upgrade should be performed on the production environment.
NFR 1.13	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Scalability	All the applications and processes should be scalable to accommodate increase in users and data as the city population grows. System should allow to enhance the processes and further automation in future.
NFR 1.14	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Performance	System response time for user on transaction screens < 3 seconds Response time for simple query < 4 seconds Response time for complex query < 5 seconds
NFR 1.15	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Data integrity	System and its design should assure the accuracy and consistency of data, over its entire life-cycle, and is a critical aspect to the design, implementation and usage of the system which stores, processes, or retrieves data. Data should be mastered in single application and synchronized with other related applications. Any exceptions in data synchronization should be highlighted and managed by support team.
NFR 1.16	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Usability	Applications screens should be intuitive and provide ease of use for users. User experience and consistent screen design should be key considerations. Appropriate online help should be provided on the screens. Error messages should be clear and precise.
NFR 1.17	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Reliability	System and its various components should function under stated conditions for the life span of the application.
NFR 1.18	ERP,SRM,AM, CRM & ISU	Non Functional requirement	Supportability	All the systems and its components should be supportable.

3.2.2. Master data governance & Data Migration

Dholera DICDL requires multiple applications to manage its functions. Most of the master data used across these applications will be common; hence it is important that these master data entities are managed and governed centrally.

Master Data Management should provide people, processes, policies and technology to formally manage and protect structured and unstructured data assets to guarantee commonly understood, trusted and secure data throughout the enterprise. This will lead to simplification, reducing complexity, lowering cost and increasing integration across the enterprise for data management.

MSI shall:

- Create a vision and strategy for information management for the DICDL.

- Create the right organizational structure (people) to govern data.
- Nominate, standardize and define the data to be managed and governed.
- Create the right processes to manage and govern data.
- Define policies and policy scope to manage and govern specific data items.
- Follow an implementation methodology to get data under control.
- Use technology in each step of the methodology to help implement the policies and processes to manage and govern the data.
- Produce and publish trusted data and services for search, order and consume.
- Define business glossary and information catalogue.
- Re-usable services to manage and process data.
- Role-based data management tools aimed at IT and business

Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
MDM 1	MDM	Master Data Management	Data content	MDM system shall unify Master data for all domains in a single platform. Each data entity / attribute should be mastered in a single system and synchronized with other related systems. All the systems should have a unified data identification for a master data.
MDM 2	MDM	Master Data Management	Data quality	MDM system should have capability to ensure quality of the data. MDM system should take care of duplicate records creation, mandatory attributes, standard drop down lists etc. to ensure data quality.
MDM 3	MDM	Master Data Management	Data quality	System should provide functionalities like data profiling and allow for mass correction by authorized users.
MDM 4	MDM	Master Data Management	Change management	Any changes to master data entities / attributes should be managed via the change management functionality and the changes should be synchronized with all the related systems. Some data entities/attributes will require immediate synchronization with other systems, others can be synchronized in daily batch mode during off-peak times.
MDM 5	MDM	Master Data Management	Processing	Certain master data entities will require an approval before creation/changes, MDM system should integrate with workflow system for necessary approvals. System shall align Data Management with Business Objectives through Dynamic Governance, Adaptive workflows and reporting capabilities that shall help identify bottlenecks in processes.
MDM 6	MDM	Master Data Management	Rules/policy	MDM system shall provide flexible rules/policy definition functionality to define for each master data entity/attributes: 1. Systems to be synchronized 2. Data transformation specific to the system to be synched with 3. Frequency for data update 4. Approval workflow requirements 5. Exception management workflow
MDM 7	MDM	Master Data Management	Change Audit	System shall provide a detailed change audit for all master data entities/attributes.
MDM 8	MDM	Master Data Management	Integration	MDM system shall integrate with all the related systems to create / synchronize the master data. MDM system shall have ability to integrate using various integration methods like but not limited to web-services, API calls, file transfers, etc.
MDM 9	MDM	Master Data Management	Exception management	MDM system shall provide the exception management functionality to cater to errors occurred during data synchronization with other systems. Wherever required the exceptions should trigger a workflow to correct the synchronization errors. A worklist should be provided for all the exceptions and for its corrections. Once corrected MDM system shall trigger the updates to relevant system.
MDM 10	MDM	Master Data Management	Data access and navigation	System shall provide restricted access to users to manage the master data and its changes. The authorization should be available at master data entity / attribute level where relevant.
MDM 11	MDM	Master Data Management	Reporting and Analytics	System shall provide reporting and analytics for areas like but not limited to: 1. Data quality 2. Data profiling 3. Exceptions in data synchronization 4. Data changes

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				5. Data inconsistencies 6. Data conflicts, etc.
MDM 12	MDM	Master Data Management	Data Archival	System shall provide data archival process based on data usage and retention period as customized for each data entity. Data archival procedure shall be run periodically to keep the systems clean. Data archival should take care of data across all the systems.
MDM 13	Master Data Management	Master Data Management Open Data Platform	Specification	Open Data Platform: - Embedded SLAs to reflect the operational requirements of the organization. - Ownership of the data generated to be made clear - A business model predicated on the data alone, and be open to 'subsidize' the capital costs to achieve this. - Integration of all data sources including the IOT, SCADA and the IS ERP platform is critical for whole process enablement. - A route map to delivery with key dependencies to ensure that the organization has the freedom to monetize its increasingly valuable data.
MDM 14	Master Data Management	Master Data Management Open Data Platform	Specification	Open Data Platform, IOT and API: - Integration and ability to share freely IOT data - Corporate and municipal data creates revenue generation possibilities through mobile apps - Enhanced citizen information / dashboarding apps - Work flow, directed at delivering actionable outcomes, is integrated with the analytics. - All of the data should sit on open APIs - Combine data across multiple organizations, commercial and local government - This should be a fit for put pose model to be developed as a cost optimized solution - AI integrated IOT analytics & modelling should be incorporated.
MDM 15	Master Data Management	Master Data Management Open Data Platform	Specification	Open City Data Platform (OCDP): - Associated analytics and integration of several technologies incorporated at DSIR should occur. - Data Sharing - Peer to Peer Security - Visualization - Infrastructure Sharing - Essential data and processes within DSIR to be controlled, using easy to use web based technologies. - Open source web technology
MDM 16	Master Data Management	Master Data Management Open Data Platform	Specification	Open City Data Platform (OCDP), Enterprise data adaptors: - Integration with traditional Enterprise database technology and state of the art super scale. - Use an open sourced library to streamline this integration, sharing efforts between cities and lowering integration costs. - integrate data from all of these sources in a secure way, and make it available in a unified fashion. - Unique peer-to-peer security model to help manage and control complex suite of data sources, whilst at all times ensuring each data supplier remains in absolute control of their data. - Create algorithms to analyze data in real time and identify trends. - Provide predictive analytics and trigger warnings of impending events.
MDM 17	Master Data Management	Master Data Management Open Data Platform	Specification	Create paperless operations: - Data to be on shared platforms making operations streamlined and transparent, waiting times reduced, verification is automated and decision-making is swift.
MDM 18	Master Data Management	Master Data Management Data Security	Specification	Data Security: - Physical network security is fundamental to data security. - Open data to require confidence that transmission, storage and use are robust and carefully managed. - Ensure only the people who have the appropriate permissions can access the data. - Peer to peer security model. - Security architecture is key.
MDM 19	Master Data Management	Master Data Management Data Visualization	Specification	Data visualization: - Graphical drag and drop interface to be provided for rapidly creating graphical visualizations, data processing elements, culminating in full-fledged applications.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				- Democratization of data access, ensuring non-programmers and programmers alike are given the tools to fully exploit the data.
MDM 20	Master Data Management	Master Data Management Data Visualization	Specification	Data visualization to include the following: - Fleet Management - Agricultural IOT - Green Energy Production - anaerobic digesters - Housing Affordability - Homelessness Reporting - Mayors Dashboard
MDM 21	Master Data Management	Master Data Management Open Data Platform	Specification	Open Data Platform: - Embedded SLAs to reflect the operational requirements of the municipality. - Ownership of the data generated to be made clear - A business model predicated on the data alone, and be open to 'subsidize' the capital costs to achieve this. - Integration of all data sources including the IOT, SCADA and the IS ERP platform is critical for whole process enablement. - A route map to delivery with key dependencies to ensure that the municipality has the freedom to monetize its increasingly valuable data.

Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR 1.0	MDM	Non Functional requirement	Service Support	For all the critical applications in the portal service support is require. Any priority 1 incident should be resolved in 3 hours. Priority 2 incidents should be resolved in 5 hours. Priority 3 incidents should be resolved in 16 hours. Priority 4 incidents should be resolved in 40 hours. All the MIS requirements required should be provided by the Service Support function once the new system is live. Daily health checks should be performed and published on the above systems to ensure their availability and performance.
NFR 1.1	MDM	Non Functional requirement	Service Support	System housekeeping, maintenance resulting in system downtime or partial unavailability should be performed during the low usage window of the application in consideration.
NFR 1.2	MDM	Non Functional requirement	Operational Window	Where the systems are expected to employ batch/background processing, the batch/background processing should be scheduled and completed outside of the service window of the application to reduce the impact on the users
NFR 1.3	MDM	Non Functional requirement	Operational Window	For all the external interfaces, based on type of interface and the need, system should restrict receiving, sending or processing external data in a selected time window.
NFR 1.4	MDM	Non Functional requirement	Performance	All synchronous interfaces should have a response time of < 3 seconds
NFR 1.5	MDM	Non Functional requirement	Operational Window	Peak usage hours for the system are expected to be 09:00 – 18:00 Monday to Friday.
NFR 1.6	MDM	Non Functional requirement	Background processing	As this is an online system there is no batch window. The overnight interface file sent from Insight needs to be received and imported prior to the start of peak hours.
NFR 1.7	MDM	Non Functional requirement	System Security	All applications should provide • Physical Security • Access Security • Data Security System architecture shall Consider each type of security from the perspective of: • Malicious attack, including service denial • Technical Failure • Privacy and confidentiality of information • System reconstruction • Support for Business Continuity Plans and Strategies Internal security should support the following security standards:

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				• SAML 1.1 and SAML 2.0 • SAML Bindings 1.1 (SOAP binding) • WS-Security: SOAP Message Security 1.0 • WS-Security Username Token Profile 1.0 • WS-Security SAML Token Profile 1.0
NFR 1.8	MDM	Non Functional requirement	System Security	System must authenticate user login's with the AD server. If user login id has not been authenticated with AD server, system must give error message and stop logging into the application.
NFR 1.9	MDM	Non Functional requirement	System Security	System should be able to hold various roles for different users and provide authorizations required for the roles assigned.
NFR 1.10	MDM	Non Functional requirement	Disaster Recovery	During Disaster recovery period, application will setup in the failover location and it must access from this location. All the business functionality and data that is available in the primary server must be available for the users.
NFR 1.11	MDM	Non Functional requirement	Data Security & Auditability	All the master and transaction data should be protected from un-authorized access. Data should be backed up daily. In case data getting corrupted, it should be restored within 8 hours. All data changes should be logged, and system should provide functionality to trace the data changes. Systems should provide complete auditability of data changes. Any data transmitted, should be encrypted.
NFR 1.12	MDM	Non Functional requirement	Upgrade	All applications should be upgraded to recommended versioning in compliance with manufacturer's upgrades and warranties. All upgrades should be performed and tested on development and test environment first and then tested. Only on acceptance of testing the upgrade should be performed on the production environment.
NFR 1.13	MDM	Non Functional requirement	Scalability	All the applications and processes should be scalable to accommodate increase in users and data as the city population grows. System should allow to enhance the processes and further automation in future.
NFR 1.14	MDM	Non Functional requirement	Performance	System response time for user on transaction screens < 3 seconds Response time for simple query < 4 seconds Response time for complex query < 5 seconds
NFR 1.15	MDM	Non Functional requirement	Data integrity	System and its design should assure the accuracy and consistency of data, over its entire life-cycle, and is a critical aspect to the design, implementation and usage of the system which stores, processes, or retrieves data. Data should be mastered in single application and synchronized with other related applications. Any exceptions in data synchronization should be highlighted and managed by support team.
NFR 1.16	MDM	Non Functional requirement	Usability	Applications screens should be intuitive and provide ease of use for users. User experience and consistent screen design should be key considerations. Appropriate online help should be provided on the screens. Error messages should be clear and precise.
NFR 1.17	MDM	Non Functional requirement	Reliability	System and its various components should function under stated conditions for the life span of the application.
NFR 1.18	MDM	Non Functional requirement	Supportability	All the systems and its components should be supportable.

- **Application Software Certification**

- Upon successful UAT and prior to Go Live, MSI shall undertake testing and certification of the Software by the Standardization Testing and Quality Certification (STQC) Directorate or any other CERT-In empaneled IT Security Auditors from functional and security perspective.
- MSI needs to engage with the 3rd party auditor at an early stage to avoid any unnecessary re-work as well as the audit gets completed on time. The audit needs to be completed before Go-Live of separate phases. MSI needs to prepare and provide all requisite information/documents to third party auditor and ensure that there is no delay in overall schedule.
- Rectification of non-compliances should be carried out by MSI and the charges for the same would be borne by the MSI.

- **Testing and Acceptance Criteria**

- MSI needs to demonstrate the following mentioned acceptance criteria during the system implementation phase as well as during project operations phase, in respect of scalability, performance, etc. The MSI may propose further detailed acceptance criteria at the time of project implementation phase and the same needs to be reviewed and agreed upon by authorized officials from DSIR. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified as well as resolved by the development/testing team.
- The following table depicts the details for carrying out various kinds of testing envisaged for the project: (indicative list)

Type of Testing	Responsibility	Scope of Work
Unit Testing	MSI	• Prepare Unit test plans, test scripts and test cases, review and rework on the same as per the developments taking place in the application. • Perform unit testing on all the applications and share the test results with authorized officials at DSIR. • Unit testing to be carried out in such a manner that it should be able to promptly catch any defects introduced due to the change in the application. • Test codes should be modular and reusable. • Testing needs to be carried out using manual as well as automated methods. • Automation testing tools needs to be provided by MSI.
System Testing	MSI	• Prepare test plans and test cases and update the same regularly. Test plans, test cases and testing results needs to be shared with DICDL/DSIR as and when requested by DSIR. • Carry out System testing • Testing needs to be carried out using manual as well as automated methods. • Automation testing tools needs to be provided by MSI.
Integration Testing	MSI	• Prepare integration test plans and update the same regularly. • Carry out integration testing as per the approved test plans • Testing needs to be carried out using manual as well as automated methods. • Automation testing tools needs to be provided by MSI
API Integration Testing	MSI	• Prepare integration test plans and update the same on regular basis. • As per requirement analysis, create environment plan set up and test execution plan. • Testing needs to be carried out using various documents and manuals according to automated methods. • Automation testing tools to be provided by MSI.
Performance & Load Testing	MSI 3 rd Party Auditor (STQC/Cert-In certified agency)	• Performance parameters such as response time, page loading time, throughput, etc. needs to be included in performance testing. • Load and stress testing of the project to be performed on business transaction volume • Test cases and test results of performance and load testing to be shared with DSIR

Type of Testing	Responsibility	Scope of Work
		- Performance testing to be carried out in a similar architecture vis-à-vis the architecture that would be set up for production environment. - Performance and Load testing tools to be used for testing. - Third part auditors would be involved to monitor/validate the performance and load testing carried out by the MSI. Cost for such audits would be paid by MSI
Security Testing (including Penetration and Vulnerability testing)	MSI 3 rd Party Auditor (STQC/Cert-In certified agency)	- Developed Solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, data center(s) as well as security monitoring system deployed by the MSI - Developed solution should pass vulnerability and penetration testing. Solution should also pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure. - MSI should carry out security and vulnerability testing on the developed solution. - Security testing to be carried out in a similar architecture vis-à-vis the architecture that would be set up for production environment. - Test cases and test results of security testing to be shared with DSIR - Testing tools if required needs to be procured/provided by MSI. - During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. - Third part auditors would be involved to monitor/validate/review the security testing carried out by the MSI. Cost for such audits would be paid by MSI
User Acceptance Testing (UAT)	MSI 3 rd Party Auditor (STQC/Cert-In certified agency)	- Test plans and test cases for User Acceptance testing (UAT) to be prepared by MSI and shared with DSIR. - Perform UAT as per the test cases and share the results with DSIR - UAT to be carried out in the same environment/architecture that would be set up for production. - MSI should fix bugs and issues observed/raised during UAT and get approval on the fixes from DSIR / third party auditor before deploying the same on the production environment - Changes in the application as an outcome of UAT shall not be considered as Change Request. MSI should rectify the observations from their end and before Go-Live of the system.

- Apart from the above given tests, there are some other tests which should be conducted by MSI as per applicability. Some of those tests are Synchronous Testing, Stress and Failover testing, etc.
- MSI needs to provide the approach and methodology for testing along with the intended

tools/environment to be setup/used for various testing in the technical proposal to be shared at the time of bidding.

- MSI needs to adhere to the testing approach and methodology outlined in the technical proposal. Deployment of required resources and tools would be sole responsibility of MSI.
- Testing to be performed by MSI in line with the approved test plan share the test results and fix the bugs (if any) observed/popped up during testing process. It is the responsibility of MSI to ensure that the product delivered meets all the requirements specified in the RFP. MSI needs to take remedial action and resolve the bugs based on outcome of the tests.
- MSI needs to arrange for setting up testing environment and testing tools for testing as well as training purpose. Post Go-Live, the production environment should not be used for testing and training purpose. If any production data is to be used for testing, it should be masked and protected. Detailed process for the same including data security requirement should be mentioned/shared in the technical proposal to be submitted by MSI.

3.2.3. GIS Integration

A Smart City's ICT ecosystem will involve multiple technologies for various city services. The primary thread that connects these technologies is spatial data or location information associated with the area of interest of each function. The integration, coordination and synergistic functioning of these technologies with spatial data or Geospatial technology (GIS) becomes the key for success of smart city ICT ecosystem.

GIS and other technology are complementary to each other, when integrated, could support broadest range of services and management activities more efficiently and effectively than either one independently.

GIS will have to be integrated with all the city technology platforms like (but not limited to) SCADA, ERP, EAM (Enterprise Asset Management), CCTV, Communication Sensors and similar ICT platforms to be developed and integrated in future with GIS system.

MSI will have to identify the best approach for integration – Open application programming interface (API based), Map it or fully integrated GIS based.

3.2.4. City Applications – eGovernance Integration

All the city applications designed by various System Integrators at Government of Gujarat (GoG) such as eOlakh, eNagar, etc. needs to be used as eGovernance system for DSIR.

MSI shall provide an interface on the DICDL Webportal to connect to the existing GoG eGovernance applications where citizen would request various services related to building permission, land management, lease management, etc.

MSI shall design and develop various API services to connect to various eGovernance applications implemented and operated by different SI's in GoG department.

MSI needs to propose a comprehensive solution in line with the functional requirement specified in the tender document. Various applications/systems such as ERP system, Integrated Command & Control Centre (ICCC), Power & Utilities system, State/Central/other Government entities for sharing requisite data, payment/SMS/email gateway, etc.

All the efforts required for integration of existing modules with the proposed solution will have to be taken

in to consideration by MSI during the effort calculation and the same will have to be part of the commercial bid submitted by the MSI.

City Wide Integration for Operational Optimization: In order to achieve operational optimization across all the city disciplines such as utilities, infrastructure, packages, systems, subsystems, components, elements etc. being sourced by respective disciplines individually in smart city Dholera, the MSI will study their entire automation, control, monitoring, display, alarming, reporting etc. processes, in order to deploy the detailed framework for achieving high degree of automation, optimization, monitoring, displaying, controlling, reporting etc., as also MSI shall integrate them in to city ICT for optimal operations of city infrastructure in all spheres of Dholera. Additionally, the MSI shall prepare and get successfully implemented its city's integration design and engineering for the aforementioned purposes that will include all the disciplines as stated above.

The approach of the MSI's implementation plan will also ensure an integrated approach by working closely with various system vendors and sub-contractors, so that benefits such as mentioned below also are achieved

- i. Open Architecture and System Integration
- ii. Better cost control and flexibility for future upgrading and expansion
- iii. Simplified operating model, interface and procedures

3.2.5. City Applications - Web Portal

Governments around the world are experiencing the first line of contact with citizens is fast changing, as citizens are less likely to come into the city council for city services. Citizens want to be able to request and use government services, pay taxes and discuss issues online. As part of the smart city of Dholera, a city portal will be deployed that provides citizens and businesses in Dholera access to these services.

The portal will provide access to different kinds of applications, such as paying taxes, requesting building permit, waste, birth and death registration and will be accessible by using computers and mobile devices with an internet connection. Secondly, the portal will also provide information to citizens; e.g. on city news, progress of city development, future plans and emergency announcements. Thirdly, it will also integrated with the payment gateway and other services that allows citizens to pay their taxes and fees as well as request for city services.

DICDL is having their web portal as www.dicdl.in where MSI needs to amend the same with the requirements mentioned in the current RFP. DICDL will provide further details over and above the requirements on designing and implementation of secure Webportal with requisite certification and standards as shared by MeitY and Gol.

MSI shall provide an interface on the DICDL Webportal to connect to the existing GoG eGovernance applications (eOlakh, eNagar, eMamta, etc.) where citizen would request various services related to building permission, land management, lease management, etc.

Functional and Technical requirements

Following services are being envisaged as part of City Portal Solution (indicative only, and not restricted to).

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WBP-POR 1.0	Webportal	Portal	System design	Portal to be robust, reliable and scalable.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WBP-POR 2.0	Webportal	Portal	System design	System to be flexible regarding adding/modifying data entry fields without having to modify the source code and/or requiring additional development tools
WBP-POR 3.0	Webportal	Portal	System design	Portal to have a caching infrastructure to reduce the load and increase its performance
WBP-POR 4.0	Webportal	Portal	System design	Portal to be equipped with a content management system that allows for creation of ad hoc as well as new pages
WBP-POR 5.0	Webportal	Portal	System design	Portal to be Unicode compliant
WBP-POR 6.0	Webportal	Portal	System design	All-important data entities to be in line with standards published by DIT
WBP-POR 7.0	Webportal	Portal	System design	All application to comply with localization standards as published on http://egovstandards.gov.in
WBP-POR 8.0	Webportal	Portal	System design	Portal to be compliant to code standards and pass through various validation tools, e.g. HTML validator, CSS validator etc.
WBP-POR 9.0	Webportal	Portal	System design	Portal to be designed on an open data policy
WBP-POR 10.0	Webportal	Portal	System design	Portal design to include standard features, but not limited to: - Provision to navigate to list of applications - Provision to navigate to homepage - Provision to navigate to important content - A reset button
WBP-POR 11.0	Webportal	Portal	System compatibility	Portal to be compatible with mobile OS like Android, iOS and other industry standard platforms. All the important features and functionalities mentioned in the RFP should be made available through the mobile application
WBP-POR 12.0	Webportal	Portal	System compatibility	Portal to be flexible enough to run on any device, without needing high-end devices
WBP-POR 13.0	Webportal	Portal	System compatibility	Portal to be compatible with all types of browsers (Microsoft Internet Explorer, Chrome, Mozilla Firefox, etc.)
WBP-POR 14.0	Webportal	Portal	System compatibility	Minimum specifications for the device to open the portal to be clarified later
WBP-POR 15.0	Webportal	Portal	System compatibility	Portal to be fully compliant with HTML 5.0 or higher
WBP-POR 16.0	Webportal	Portal	System compatibility	Portal to allow usage of authenticated plug-ins
WBP-POR 17.0	Webportal	Portal	General	The portal to be the single window service to citizens at anytime and anywhere basis, available 24/7
WBP-POR 17.1	Webportal	Portal	General	Portal to fulfil all requirements for citizens towards city administration and state government
WBP-POR 18.0	Webportal	Portal	General	Portal to be the primary source of information for all city's stakeholders, such as but not limited to: - Citizens - Corporates - Tourists - Commercial entities - Governmental departments and its employees - Healthcare providers - Educational institutes - Third party vendors
WBP-POR 18.1	Webportal	Portal	General	Portal to be a comprehensive information source
WBP-POR 18.2	Webportal	Portal	General	Portal to cater for the different needs and requirements of all stakeholders
WBP-POR 19.0	Webportal	Portal	General	Portal to be an open platform with primary, secondary and tertiary content

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WBP-POR 19.1	Webportal	Portal	General	The portal to have primary content like, but not limited to, - City applications - Information generation through system integrations - City information - Progress of city development - Geographical information - Future plans of the city - Static city and corporate data - City board members information - City mayor as well as commissioner information
WBP-POR 19.2	Webportal	Portal	General	The portal to have secondary content like, but not limited to, - Grievance redressal - Polls - Social media feed - Discussion forums (specific forums for groups with special interests) - City guide - City announcement - City agenda with events - Emergency announcement and events page with audio and video upload - User policy/house rules - Related links
WBP-POR 19.3	Webportal	Portal	General	The portal to have tertiary content like, but not limited to, - Contact information - About the website - Website feedback system - Navigation pane - Contact list of departmental offices - User assistance (help/FAQ) - Terms and conditions
WBP-POR 20.0	Webportal	Portal	General	The portal to be state of the art
WBP-POR 21.0	Webportal	Portal	General	Portal upkeep to be available during business hours
WBP-POR 22.0	Webportal	Portal	General	Portal upkeep center to be part of the CIOC building
WBP-POR 23.0	Webportal	Portal	User interface	User interface to be intuitive, user friendly and dynamic
WBP-POR 24.0	Webportal	Portal	User interface	Users to be able to customize their personal home page, e.g. by shuffling favorite applications
WBP-POR 25.0	Webportal	Portal	Role based functions	System to provide role based authorization to all concerned officials
WBP-POR 25.1	Webportal	Portal	Role based functions	Portal to be equipped with dual authentication allowing citizens access to the portal and to request services
WBP-POR 25.2	Webportal	Portal	Role based functions	Portal to have ability to show certain content only to authenticated users
WBP-POR 26.0	Webportal	Portal	Functionality	The portal its functionalities to have end-to-end business process perspective, cutting across business applications.
WBP-POR 27.0	Webportal	Portal	Functionality	Portal to have search functionality on the homepage
WBP-POR 27.1	Webportal	Portal	Functionality	Search functionality to have capability to search using keywords and comprehensive full-text searching for all information within the portal
WBP-POR 27.2	Webportal	Portal	Functionality	Search feature to have advanced search based on multiple metadata
WBP-POR 27.3	Webportal	Portal	Functionality	Search results to be role based and authorization level of a user
WBP-POR 27.4	Webportal	Portal	Functionality	Portal to support parallel querying for improved search capabilities

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WBP-POR 28.0	Webportal	Portal	Functionality	The portal to have download and upload functionalities for documents, audio and video for all stakeholders
WBP-POR 29.0	Webportal	Portal	Functionality	Portal to be multi-lingual; English, Hindi, Gujarati
WBP-POR 30.0	Webportal	Portal	Functionality	Portal to have a repository with links to download documents and templates
WBP-POR 31.0	Webportal	Portal	Functionality	Features to be incorporated to make the portal accessible for visually impaired and disabled people, in compliance with ISO/IEC TR 29138-1 (Accessibility considerations for people with disabilities)
WBP-POR 31.1	Webportal	Portal	Functionality	Portal to have a narrator feature for visual impaired users
WBP-POR 32.0	Webportal	Portal	Functionality	System to have following, but not limited to, functionalities: - SMS & email gateway integration - Mobile device compatibility - Dashboards - Regular Management Information System reports - Payment gateway integration
WBP-POR 33.0	Webportal	Portal	Functionality	Portal have provision to integrate all domain wide services as well as any other system deployed by Dholera as in when required
WBP-POR 34.0	Webportal	Portal	Functionality	Portal to be equipped with an auto/smart fill feature
WBP-POR 35.0	Webportal	Portal	Functionality	Portal to provide a constantly updated news feed on the home page
WBP-POR 36.0	Webportal	Portal	Functionality	Portal to provide a calendar that displays events
WBP-POR 37.0	Webportal	Portal	Functionality	Portal to have links to allow individuals to contact corporations and institutions affiliated of Dholera
WBP-POR 38.0	Webportal	Portal	Functionality	Portal to have a jobs section where citizens can apply for jobs and companies can publish vacancies.
WBP-POR 39.0	Webportal	Portal	Functionality	User to have a facility to request for a service and get an update on the same on real-time basis
WBP-POR 40.0	Webportal	Portal	Functionality	Users to be able to send messages with attachments through the portal
WBP-POR 40.1	Webportal	Portal	Functionality	User to be able to communicate with the relevant department user/customer care official to get the request furnished
WBP-POR 40.2	Webportal	Portal	Functionality	Message system to have encryption
WBP-POR 41.0	Webportal	Portal	Functionality	Portal to have a facility to securely capture data from various systems and showcase it on dashboards for city analysis and performance
WBP-POR 42.0	Webportal	Portal	Functionality	Portal to have the CAF available to citizens
WBP-POR 43.0	Webportal	Portal	Functionality	Portal to show the status of public transport reservations and bookings made by a user
WBP-POR 43.1	Webportal	Portal	Functionality	Portal to interface with public transport partners' bookings system
WBP-POR 44.0	Webportal	Portal	Portal integration	Portal to integrate with sub portals such as education, eGovernance, health, ERP and state and central government portals/systems
WBP-POR 45.0	Webportal	Portal	Portal integration	Portal to have integration with payment gateway with banks and intermediaries
WBP-POR 46.0	Webportal	Portal	Portal integration	System to allow for seamless integration of application and modules to prevent data deduplication

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WBP-POR 47.0	Webportal	Portal	Portal integration	Portal to be integrated with the city wide kiosk
WBP-POR 48.0	Webportal	Portal	Portal integration	The portal provides a single window interaction interface for all partners through city kiosk (payments, bills, etc.)
WBP-POR 48.1	Webportal	Portal	Portal integration	The portal to exchange information between the city kiosk terminal and partner system
WBP-POR 49.0	Webportal	Portal	Security	Information security policy to be maintained (standard for information security to be mentioned)
WBP-POR 50.0	Webportal	Portal	Security	Portal to have SSO functionality or facility implemented
WBP-POR 51.0	Webportal	Portal	Security	Digital signature certificate for login for authenticated user
WBP-POR 52.0	Webportal	Portal	Security	Portal to have a multi-level security system included (firewall)
WBP-POR 53.0	Webportal	Portal	Security	Account creation for authorized users to be done by authorized user
WBP-POR 54.0	Webportal	Portal	Security	Portal to have profile management, and password recovery features
WBP-POR 55.0	Webportal	Portal	Security	Portal to have security features, but not limited to, password complexity, periodical reminders to change password, password recovery, automatic user blocking after failed login attempts and logging security incidents
WBP-POR 56.0	Webportal	Portal	Security	Portal to have secure and controlled access for authorized users to the analytics console (dashboard, portal/community traffic, search queries/keywords, no result searches, system response time)
WBP-POR 57.0	Webportal	Portal	Security	System to have error and fraud detection features (e.g. anti-identity theft)
WBP-POR 58.0	Webportal	Portal	Security	System to have an audit trail feature to identify which user made changes
WBP-POR 59.0	Webportal	Portal	Security	System to generate audit log reports
WBP-POR 60.0	Webportal	Portal	Security	Contact form to have anti-spam functionality
WBP-POR 61.0	Webportal	Portal	Content management	Portal to support integration with content management system for web content management and publishing on the portal
WBP-POR 62.0	Webportal	Portal	Content management	Portal to be equipped with a single portal content management system for both structured and unstructured content.
WBP-POR 63.0	Webportal	Portal	Content management	Portal to feature a site map that ensures the index of the portal is updated on a daily basis
WBP-POR 64.0	Webportal	Portal	Workflow	Portal to facilitate for conducting tasks or transactions to respective department official
WBP-POR 65.0	Webportal	Portal	Workflow	Portal to automatically provide the status of a task
WBP-POR 66.0	Webportal	Portal	Workflow	Portal to be equipped with a feature to return request to an individual for clarification or corrections.
WBP-POR 67.0	Webportal	Portal	Notification system	System to support personalized notifications and alerts
WBP-POR 67.1	Webportal	Portal	Notification system	Notification system using SMS or email to notify individuals, e.g. about escalations and clarification requests
WBP-POR 68.0	Webportal	Captive portal	Captive portal	Captive portal to show up when a client enters a Wi-Fi zone within Dholera
WBP-POR 68.1	Webportal	Captive portal	Captive portal	The captive portal to have a customizable GUI and allow for local branding depending on the location

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WBP-POR 68.2	Webportal	Captive portal	Captive portal	Captive portal to have the following functionalities but not limited to: - Allowing user to change his password - Allowing user to create new Wi-Fi accounts - Alert users to regularly change or update access password - Update personal details and contact information
WBP-POR 69.0	Webportal	Captive portal	Functionality	Self-service portal to be available for public hotspot non-local users in Dholera showing information on Wi-Fi services, tariffs and procedure to subscribe to services.
WBP-POR 69.1	Webportal	Captive portal	Functionality	Search functionality to have capability to search using keywords and comprehensive full-text searching for all information within the website
WBP-WEB 70.0	City Website	Website	Integration	Website to be integrated with the payment gateway with required PCI compliance
WBP-WEB 70.1	City Website	Website	Integration	System to have a facility to redirect directly to the requested application/service/link after login to the web portal
WBP-WEB 70.2	City Website	Website	Integration	Website to be integrated with social media, such as but not limited to: - Twitter - Facebook - LinkedIn - Instagram
WBP-WEB 70.3	City Website	Website	Website design	Website to follow the DICDL branded theme/color code throughout all pages
WBP-WEB 70.4	City Website	Website	Website design	Website to have adequate security measures in place

- MSI shall document detailed requirements.
- All documents needs to be reviewed and approved by relevant authorities.
- MSI shall document the solution architecture related artifacts to cover areas like Application architecture, system architecture, component models, walk-through models, Data architecture, security architecture, infrastructure architecture, etc. These documents needs to be reviewed and approved by the relevant authorities.
- MSI shall document detailed solution design related artifact to cover areas like Functional specification, configuration, data model, technical specification, etc. These documents needs to be reviewed and approved by the relevant authorities.
- Requirements that cannot be delivered as standard out of the box functionality or with configuration needs to be agreed with the design authority. If it is envisaged by design authority a prototype or proof of concept shall be provided by MSI.
- MSI shall be responsible to supply and install all required hardware/ software/ tools to meet the RFP requirement without any deviation. Any additional hardware or software necessary to meet the technical, functional and performance requirement of the project but not mentioned in RFP shall be factored and supplied by MSI as part of this RFP.
- MSI shall define the development and configuration standards. MSI shall be responsible to configure, build, enhance and customize the applications to ensure it meets the requirements without any deviations.
- MSI shall define in agreement with the relevant authorities the exit criteria for each type of testing. MSI shall perform all the necessary testing like Unit testing, System Integration testing, load and performance testing. MSI shall assist in user acceptance testing. MSI shall develop the test strategy and test scenarios to cover all the process variants and requirements. MSI shall use industry standard tools required for testing. MSI shall ensure that the minimum exit criteria (as agreed by the relevant authority) is met to conclude the completion of the testing. MSI shall manage and monitor all the stages of the testing. MSI shall document all the artifacts required for testing phase like, testing strategy, test plans, test scenarios, test results with evidences, test cycles, etc. These documents needs to be reviewed and approved by the relevant authorities.

- MSI shall manage the commissioning, deployment, roll out, intensive go-live support and transition of support to support team. All relevant documentation like Go-live plan, roll out plan, roll back plan, transition strategy, Service Management Transition document, Service support requirements etc. shall be provided by MSI. MSI shall ensure a smooth transition from deployment team to operate and maintain team.
- MSI shall be responsible for the training of trainers and end users and will provision for all the required documents and guides for training.
- MSI will be responsible for data collection, transition, data cleansing and data migration required for all the master and transaction data to be migrated to Production environment. MSI shall be responsible for the reconciliation of the data. MSI shall provide the necessary templates for data collection to DICDL. All relevant documentation like Data migration strategy, data cleansing and migration plan, Data Model, etc. shall be provided by MSI.
- MSI shall undertake the Business Change Management. MSI shall manage and anchor the BCM activities like collaboration hub, road shows, change champions grooming, communications etc.
- MSI shall assist and anchor the ongoing benefit realization for DICDL.
- MSI shall provide the Operations and Maintenance Services for a period of 5 years from the date of Go-Live.
- The MSI shall be responsible for following but not limited to:
 - Provide all necessary manpower resources onsite to manage and resolve any issues/incidents and carry out required changes, optimizations and modification
 - Responsible for identification, diagnosis and resolution of problem areas and maintaining the defined SLA levels.
 - Provision of skilled and experienced manpower resources to administer and manage solution.
 - Provision and management of the service management tool to manage the tickets.
 - Periodic health checks of the systems and applications to ensure the system performance.
 - Users and authorization management
 - Periodic system patching and upgrade as recommended by the application vendor.
 - Management and maintenance of integrated environments like Development environment, Testing environment, Production environment and Training environment.
 - Management and maintenance of configuration, development and data on these environments.
 - Users and authorization management
- The MSI shall arrange for environments and tools for testing and for training as envisaged.
- Production environment should never be used for testing and training purpose. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected MSI.
- The MSI is responsible for all tools/environment required for testing and sufficient training shall be given.
- MSI shall provide a well-prepared build documentation / user manual for users, also a clear plan for user training, education & hands training on installed solution.
- MSI is also responsible to deliver all documents approaches for entire solution with proper training and knowledge transfer.
- MSI shall adhere to the agreed SLA for deployment and operate and maintain.

Standards for Portal

The portal has to comply with the following standards:

- The platform should be created as open web platform for application development using the standards as defined by the World Wide Web Consortium (W3C) – <https://www.w3.org/standards/>
- The portal, the associated applications, and its contents should also be available to people with disabilities. To ensure this, the portal should comply with standards as defined in the Web Content

Accessibility Guidelines (WCAG) - <https://www.w3.org/WAI/intro/wcag>

- The portal is a governmental initiative and therefore it should comply with the standards as laid down in the Guidelines for Indian Government Website (GIGW) – <https://guidelines.gov.in/>
- The portal needs to be a secure environment and therefore it should comply with the standards as described by OWASP - https://www.owasp.org/index.php/Main_Page

3.2.6. City Applications - Multi service kiosk

- Solution Design
 - Kiosk solutions are one of the smartest solutions for service delivery in any Smart City. The citizen, visitors, vendors, etc. can access the applications as well as communicate with the system from Kiosk. This is the best example of anytime anywhere access for the system. So, one can have single point access to the system easily with the help of interoperable kiosks on the ground.
 - Through the smart kiosks which should be operational, transactional, informative. The individuals can navigate, browse, recharge, access applications, charge phones/tablets, book travel tickets, book parking space, announcing alert, publishing public notices, traffic conditions, weather information and forecasting etc. seamlessly. Kiosk can play major part in revenue generation for Government.

The multi service kiosks includes the following components which are not limited and can be extended as per scope:

- Maps for navigation
- City information
- Mobile device power charging
- Monitor with sufficient size for browsing and viewing city applications and maps
- Advertising screen on one side the unit only – some screen space given to local authority information.
- Vibration and tilt monitors built in to monitor for vandalism, and temperature of unit, etc.

The services from Government to Citizens, Businesses, other entities and vice versa to be seamlessly carried out through Kiosk solution.

- Solution Architecture

The kiosk system is not only about the User Interface but its robust hardware and software architecture does play the key role in the efficient smart city system.

The following diagram is indicative for requirements of Kiosk solution for DSIR.

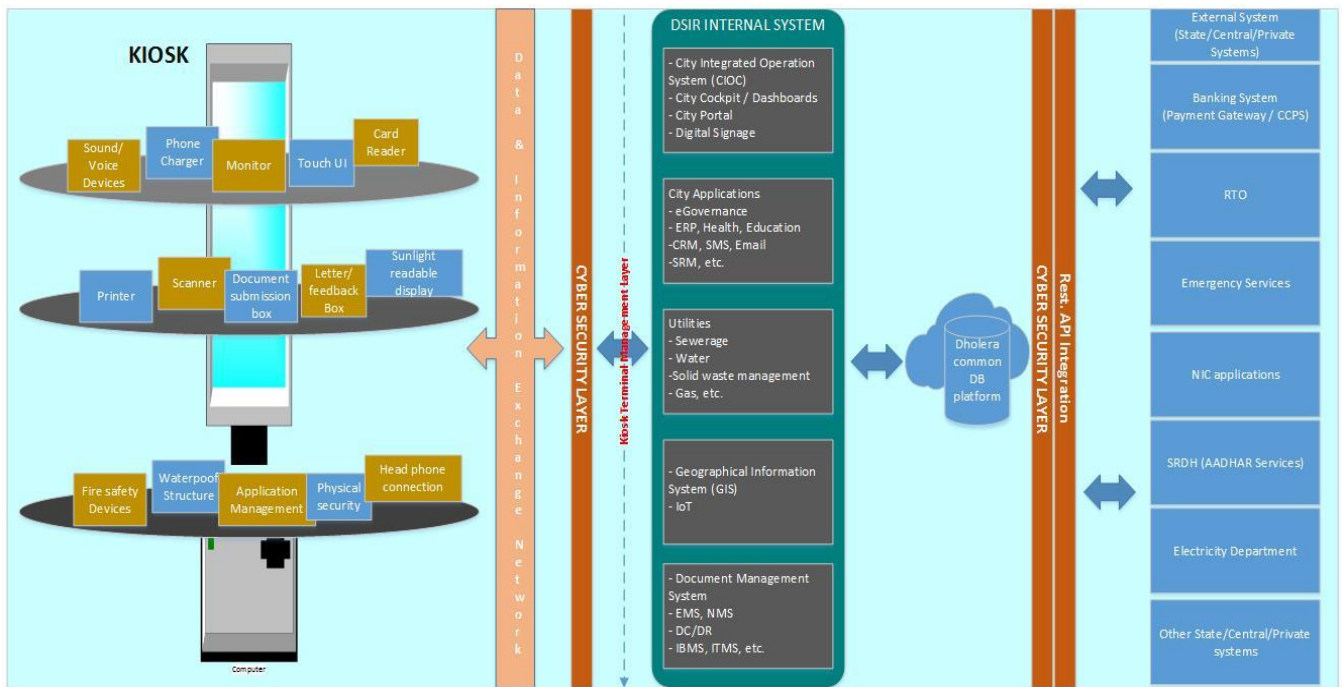


Figure - 27 Multiservice Kiosk high level architecture

The MSI should be liable for the following responsibilities but not limited to for the success of Kiosk solution for DSIR –

- MSI should submit the business model for Kiosk system for DSIR.
- UI (User Interface) for Kiosk solution should be user friendly
- The technology options such as input device, Monitors (LCD), sound-voice instruction devices, etc. should be fitted as per user requirements.
- The kiosk cabinet design should be submitted by MSI.
- The pilot run should be conducted by MSI
- The kiosk solution must have –
 - Sunlight readable display
 - Armored Touchscreens
 - Metal/Molded casing
 - Waterproof Seals
 - Robust locking system (Multipoint)
 - Protection for printer/card slots
 - Internal design for liquid run off, slot entry
 - Agency approvals for outdoor electronics enclosures for fire, water, disaster safety
 - Use rugged kiosk printer and avoid receipt printer
 - Touchable areas obvious
 - Limit the choices
 - Guide the user as much as possible
 - Simple yet large navigation buttons (e.g. start, back, forward, submit, etc.)
 - Title bars
 - Avoid double clicking
 - Avoid pull down menus
 - Avoid dragging
 - Bright background colors
 - Avoid reflections and fingerprints
 - Avoid cursors
 - Avoid mouse

- Touchscreens have no tactical feedback – users must know it ‘accepted/took’ or they will touch again
- Sound effects should be there
- Use sounds on touch
- Multilingual facility to be available
- Avoid sound cards and apply/load freshly recorded announcements in Gujarati, Hindi and English languages
- Design and colors should match for the cabinet
- Avoid flat surface/spills in the cabinet design of the kiosk
- Proper ventilation should be there for kiosk

MSI would be responsible for maintaining the physical cleanliness of the kiosk body as well of physical security of the same.

Multi-services digital kiosks will be deployed at ABCD building in DSIR to deliver various citizen services through a single integrated platform.

Functional and Technical requirements

Following services are being envisaged as part of Kiosk Solution (indicative only, and not restricted to).

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
KSK-1.0	Kiosk	Kiosk Management	Information Management	Kiosk to provide various types of information to citizen which is given as follows but not limited to - - City Map - Navigation - Emergency Contacts - Ambulance / Emergency vehicle Service - Public Notices - Publications - Schools - Hospitals - ATMs - Public Restrooms (Urinals) - Government Departments / Offices - Tourist Attractions - Businesses - Markets - Hotels / Restaurants - Nearby Vehicle Parking - Public Transport - Police Station
KSK-2.0	Kiosk	Kiosk Management	Transaction Management	Kiosk to have provision to process following transactions but not limited to - - Submission of application for various citizen services - Payment for respective eGovernance applications e.g. Property tax, Building permission, Birth and death, Marriage certificate, etc. - Bills Payments(e.g. electricity, water, telephone, etc.) - Tracking status of various respective applications - Create / Edit / Update citizen profile
KSK-3.0	Kiosk	Kiosk Management	Feedback Management	Kiosk to provide system for citizen to submit feedback related to any service / work done by urban local body within the city.
KSK-3.1	Kiosk	Kiosk Management	Feedback Management	Kiosk to provide an option for opinion poll for citizen on various public issues. Also, it should have provision to submit detailed feedback on any Government regulation.
KSK-4.0	Kiosk	Kiosk Management	Help / Emergency management	Kiosk to provide an option (e.g. Emergency alert / alarm button) for citizen to raise alert/alarm in any emergency
KSK-5.0	Kiosk	Kiosk Management	Kiosk Portal	The unique portal should be there for access rights to various authorized government and semi government departments, schools, colleges, public transport systems, traffic management systems, Hospitals, etc.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
KSK-5.1	Kiosk	Kiosk Management	Kiosk Portal	The kiosk to have provision of Touch UI with user-friendly design supporting multilingual/Unicode interface.
KSK-5.2	Kiosk	Kiosk Management	Kiosk Portal	The kiosk portal to have provision to publish various advertisements related to public and business
KSK-6.0	Kiosk	Kiosk Management	Infrastructure	The kiosk to have following hardware infrastructure essentially deployed, operate and maintained for Kiosk - - Camera - Emergency push button (Panic Button) - Mobile Charger with 1 or 2 ports - Keyboard for Input - Smart Card Reader - Speakers - Headphone inputs - Microphone - Credit/Debit card reader - QR code interface - Interface for accepting NFC (Near Field Communication) payments - Dropbox for Cheque/letters
KSK-6.1	Kiosk	Kiosk Management	Infrastructure	Kiosk to be integrated with any cameras and public surveillance CCTV systems
KSK-7.0	Kiosk	Kiosk Management	Data Management	Kiosk system to have provision of open data platform to manage and handle isolated data and information of transactions through different applications.
KSK-8.0	Kiosk	Kiosk Management	Integration	System to have integration with City Operation Center for effective data and service management.
KSK-9.0	Kiosk	Kiosk Management	Infrastructure	System to have provision to send and display alerts on the screen for every respective transaction.
KSK-10.0	Kiosk	Kiosk Management	System Security	System to have provision for data and cyber security for the kiosk.
KSK-11.0	Kiosk	Kiosk Management	Physical Security	System to have provision to adopt and deploy solutions catering to protect kiosk terminal from physical damage from weather or environment.

3.2.7. City Applications - Mobile applications

With rapidly increasing levels of mobile penetration, continuous improvement in bandwidth with the use of fiber optic network, and accessibility of citizen convenience, it has been envisaged to develop the required mobile applications for various platforms (android, iOS, etc.). With an aim to enhance the civic service delivery mechanism and citizen interaction with government entities the MSI needs to continuously innovate, upgrade and incorporate latest emerging technologies for the development of mobile applications considering multiple aspects. (Ease of use, cyber security, compatibility, etc.)

Salient features of Mobile application:

- Multi-Platform or Open-ID Integration with User Authentication (Login from Facebook, Google, twitter, etc.). Facility to be provisioned where user can create his/her account, proceed with the payment (if paid app) and use the same.
- Updating user profile settings
- Credential of mobile app store will be provided by DICDL
- UX Simple Minimalist Interface – Displaying Video, Audio, Images by People, Location, Date/Time, Event (Filter)
- Facility to read photo gallery from the device (Video, Image, or directly Image Capture from Mobile Device)
- Social Media Sharing – Sharing of data with other App Users
- Facility for In App Editing – Photo Filters – Cropping – Amendment of Orientation – Audio Overlay and Muting – Clip Editing and Organization – Add Text or Images
- Video Casting to Chrome Cast, etc.

- System to have a facility to enable field employees to share job and inventory details and confirm re-assigned jobs and inventory transfers with just a click
- System to have a functionality for Improving citizen satisfaction by receiving timely feedback and respond to citizens faster.

Functionality Requirements for Mobile Applications needs to be based on project requirements and shall include as applicable but not limited to following.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
MOB - 1.1	Mobile App	Mobile Application	Mobile Application	Facility of link sharing for application download with fellow citizens
MOB - 1.2	Mobile App	Mobile Application	Mobile Application	Mobile app to have a facility to integrate with various payment gateways as well as other related systems/application to fetch and share data as required.
MOB - 1.3	Mobile App	Mobile Application	Mobile Application	Smart environmental mobile application to demonstrate the air pollution levels as recorded by environment sensors. The said application needs to trigger the alarm and notification of environment pollution levels to all the citizens of the city.
MOB – 1.4	Mobile App	Mobile Application	Mobile Application	Mobile applications developed for various domains/services needs to be integrated with various state and central government legacy applications for validation and verification of citizen data. (e.g. Birth/death registration database, etc.)
MOB - 1.5	Mobile App	Mobile Application	Mobile Application	Considering aspects viz. simplicity—low development effort and cost, high user buy-in & acceptance and fast speed to market the mobile application needs to support mobile forms design and development (mobile form builder - MGovernance) to be used by field level officers to insert requisite details directly in to the database system ruling out chances of errors and time lags for work completion as well as real time reporting.
MOB - 1.6	Mobile App	Mobile Application	Mobile Application	Mobile application will have an integration with existing GoG / DICDL grievance redressal system.
MOB - 1.7	Mobile App	Mobile Application	Mobile Application	Develop Resolution independent design structure where the Mobile Apps adjusts itself automatically as per the screen resolution of the Mobile i.e. 1024*768, 1200*800 etc. Resolution independent Mobile Apps will automatically expand/compress itself as per the screen resolution and hence there should not be any horizontal scroll in the Mobile Apps structure
MOB - 1.8	Mobile App	Mobile Application	Mobile Application	Mobile application should support multilingual functionality as well as it should be Unicode compliant.
MOB - 1.9	Mobile App	Mobile Application	Mobile Application	The mobile apps need to alert the user to download the latest version (whenever one is available) and if required prompt for compulsory upgrade.
MOB - 1.10	Mobile App	Mobile Application	Mobile Application	Architecture of the mobile app should be robust, scalable and compatible with legacy applications (web/mobile) for sharing of data through APIs or another required medium.
MOB - 1.11	Mobile App	Mobile Application	Mobile Application	Facility to PUSH through and PULL through mechanism to get and receive information using SMS service
MOB - 1.12	Mobile App	Mobile Application	Mobile Application	Mobile app needs to capture critical data such as user identification and location information including latitude, longitude and altitude to be shared/integrated with other related applications/services as and when required.
MOB - 1.13	Mobile App	Mobile Application	Mobile Application	Facility to be incorporated where mobile app shall have the ability to broadcast live video streams to the CIOC.

Mobile application platform

- Applications and services including all appropriate channels such as SMS/USSD/IVRS and development of corresponding mobile applications to the applications and services leveraging the Mobile Service Delivery Gateway (MSDG) and Mobile App Store. (Android, iOS, etc.)
- Open standards to be adopted for design, development and implementation of mobile applications leading to sharing of permissible citizen data as well as ensuring the interoperability of applications across varied operating systems.

- Application platform should support all smart phone mobile OS's prevailing at the time of system design and deployment phase.
- Mobile Application platform should be able to;
 - Support target packaging components like (Mobile Website, Hybrid App, Native App, Web App and Application Development, Eclipse and other tooling platforms).
 - Support the ability to write code once and deploy on multiple mobile operating systems through common platform.
 - Support integration with native devices using APIs
 - Support utilization of all native device features
 - Support development of applications in a common programming language
 - Support integration with mobile vendor SDKs for app development and testing
 - Support HTML5, CSS3, JS and other required features for smartphone devices
 - Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML, etc.)
 - Support JSON to XML, provide XHTML message transformations as well as other messaging components.
 - Support multi-lingual and language internalization
 - Support encrypted messaging between server and client components

User interface

- All icons must be crisp, clean, and distinguishable and should be as per guidelines of mobile application platform.
- All buttons and objects must be reactive to touch and work as intended.
- All functions must stay within the mobile platform boundaries.
- All data must be easily viewable on all Mobile platforms prevailing in the market.

The mobile application should be designed in such a manner that it should address the following key issues:

- Authentication and Authorization: Failing to authenticate in occasionally connected scenarios
- Caching: Caching unnecessary data on a device that has limited resources
- Communication: Failing to protect sensitive data over any carrier
- Data Access: Failing to implement data-access mechanisms that work with intermittent connectivity.

3.2.8. Process workflow

To enhance the efficiency, effectiveness and transparency of service delivery for citizens and to internal and external customers as well as its stakeholders DICDL envisages to use ICT in developing a comprehensive workflow solution leading to electronic movement and delivery of work within various departments and or groups.

The key objective of the proposed workflow Solution are;

- Improve the quality of Citizen Service Delivery System and offer these services with optimal effectiveness and transparency.
- Allow data sharing across respective departments as well as other government agencies using open Data platform, and bringing about the efficiency in administration.
- Provide a single platform integrated to various applications and enable smooth process flow across systems, departments and groups.
- Standardize and automate the process flow to enable increased efficiencies, throughput and SLA compliance.
- Facilitate in the decision-making process of senior stakeholders by furnishing the real time information along with MIS reports, data analytics trends with help of smart reporting, analytics and query tools

- Help different departments to improve their efficiency.
- Harness the use of technology to create sense of achievement amongst employees and citizens
- Improve the internal management of the Special Purpose Vehicle (DICDL) created for City administration.

Following services are being envisaged as part of workflow Solution (indicative only, and not restricted to);

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WKF 1.0	Workflow	Workflow	Definition	Functionality and flexibility to define workflow templates using graphical user interface with logical constructs and tasks with dynamic agent assignment.
WKF 1.1	Workflow	Workflow	Definition	Functionality to dynamically determine agent based on organization structure, role, position or named user.
WKF 1.2	Workflow	Workflow	Definition	Functionality to integrate with multiple systems and perform transactions against action taken by agents via workflow tasks.
WKF 1.3	Workflow	Workflow	Definition	Functionality to define various workflow task library which can be used to define the workflow template.
WKF 1.4	Workflow	Workflow	Definition	Functionality to automatically initiate the specific workflow/s based on event across various systems.
WKF 1.5	Workflow	Workflow	Definition	Functionality to configure steps at workflow generation as required, optional, or not applicable.
WKF 1.6	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to be completed sequentially or in parallel.
WKF 1.7	Workflow	Workflow	Definition	Functionality to configure steps in the workflow as sub groups to be completed in parallel then sequentially with another sub-group.
WKF 1.8	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to be checklists (i.e. for required customer documentation, check for outstanding customer debt).
WKF 1.9	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to auto-generate tasks to staff.
WKF 1.10	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to auto-generate e-mails or other mediums of contact to staff.
WKF 1.11	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to auto-generate e-mails to Government departments outside of DICDL
WKF 1.12	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to auto-generate a customer / contractor /citizen communication letter.
WKF 1.13	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to auto-generate a customer / contractor / citizen communication e-mail.
WKF 1.14	Workflow	Workflow	Definition	Functionality to configure steps in the workflow to auto-start a process
WKF 1.15	Workflow	Workflow	Definition	Functionality to configure initiation / waiting for additional event in the workflow template.
WKF 1.16	Workflow	Workflow	Definition	Functionality to configure steps in the workflow that require staff approval to move forward.
WKF 1.17	Workflow	Workflow	Definition	Functionality to automatically set a due date for task completion based on task definition.
WKF 1.18	Workflow	Workflow	Definition	Functionality to create letter templates can be configured to pull data from any field in the database.
WKF 1.19	Workflow	Workflow	Definition	Functionality to apply approval parameters that require another identified staff person or group to approve the task.
WKF 1.20	Workflow	Workflow	Definition	Functionality to easy configure graphical user interface
WKF 2.0	Workflow	Workflow	Operations	Functionality for user's inbox to manage work items assigned to them.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WKF 2.1	Workflow	Workflow	Operations	Functionality for users to delegate/substitute their work items to other users.
WKF 2.2	Workflow	Workflow	Operations	Functionality to configure several different workflow types.
WKF 2.3	Workflow	Workflow	Operations	Functionality to handle inter-departmental activities through workflows
WKF 2.4	Workflow	Workflow	Operations	Functionality to handle inter-system activities through workflows
WKF 2.5	Workflow	Workflow	Operations	Functionality to have dynamic workflows based on previous steps' outcomes will change future steps.
WKF 2.6	Workflow	Workflow	Operations	Functionality for the workflow to age.
WKF 2.7	Workflow	Workflow	Operations	Functionality for the workflow to age show aging details by assigned person work queue, department, etc.
WKF 2.8	Workflow	Workflow	Operations	Functionality for the workflow to expire.
WKF 2.9	Workflow	Workflow	Operations	Functionality for the workflow to provide notification of expiration.
WKF 2.10	Workflow	Workflow	Operations	Functionality for the aging to be retained for management action.
WKF 2.11	Workflow	Workflow	Operations	Functionality to report on the aging of the workflow.
WKF 2.12	Workflow	Workflow	Operations	Functionality for a work item action to complete a workflow step and move to the next step.
WKF 2.13	Workflow	Workflow	Operations	Functionality for a supervisor to reassign a task.
WKF 2.14	Workflow	Workflow	Operations	Functionality to delegate workflow tasks to other user
WKF 2.15	Workflow	Workflow	Operations	Functionality for completing a task to display a completion date.
WKF 2.16	Workflow	Workflow	Operations	Functionality for completing a task to display who completed the task.
WKF 2.17	Workflow	Workflow	Operations	Functionality for canceling a task to display who cancelled the task.
WKF 2.18	Workflow	Workflow	Operations	Functionality for canceling a task to display a cancellation date.
WKF 2.19	Workflow	Workflow	Operations	Functionality to indicate that letter was sent via certified mail and the certified number.
WKF 2.20	Workflow	Workflow	Operations	Functionality to easily sign in to workflow application using single sign on.
WKF 2.21	Workflow	Workflow	Operations	Functionality to easily access the workflow transaction history.
WKF 2.22	Workflow	Workflow	Operations	Functionality to easily access the transaction history by operator ID.
WKF 2.23	Workflow	Workflow	Operations	Functionality to easily access the transaction history by transaction type.
WKF 3.0	Workflow	Workflow	Alerts	Functionality to configure that alerts are set when actions are triggered.
WKF 3.1	Workflow	Workflow	Alerts	Functionality to set alerts to expire automatically (without user intervention) when certain conditions are triggered.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
WKF 3.2	Workflow	Workflow	Alerts	Functionality to set end dates on Alerts to expire automatically.
WKF 4.0	Workflow	Workflow	Reminders	Functionality to easily set a reminder to expire automatically at expiration date.
WKF 4.1	Workflow	Workflow	Reminders	Functionality to easily set a reminder for a staff member on a specific date.
WKF 4.2	Workflow	Workflow	Reminders	Functionality to easily set a reminder for a department on a specific date.
WKF 4.3	Workflow	Workflow	Reminders	Functionality to easily set a reminder for a department for a specific number of days considering working days calendar.
WKF 4.4	Workflow	Workflow	Reminders	Functionality to easily set a reminder for a staff member for a specific number of days considering working days calendar.
WKF 4.5	Workflow	Workflow	Reminders	Functionality to easily configure condition-driven reminders and actions.
WKF 5.0	Workflow	Workflow	Reporting	Functionality to notify a supervisor of a missed task due date.
WKF 5.1	Workflow	Workflow	Reporting	Functionality for a supervisor may view all tasks showing aging by assigned staff person.
WKF 5.2	Workflow	Workflow	Reporting	Functionality to easily access the transaction history for quality checking and reviewing.
WKF 5.3	Workflow	Workflow	Navigation	Functionality to easily maintain user and role based security that supports multiple levels of security and permissions for various user profiles.
WKF 5.4	Workflow	Workflow	Navigation	Functionality for minimal clicks navigation with no screen more than three clicks from the initial screen.
WKF 5.5	Workflow	Workflow	Navigation	Functionality to configure a home screen with easily accessible work queues and dashboards.
WKF 5.6	Workflow	Workflow	Navigation	Functionality to easily search notes.
WKF 5.7	Workflow	Workflow	Navigation	Functionality to easily utilize "help" functionality.

3.2.9. City Applications – Non-Functional requirements

The non-functional requirements as presented below apply to all city applications.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIT-PER 1.0	City Applications	Performance		The system to be eligible to perform on unique parameters mentioned as but not limited to Response times, throughput, Utilization, etc.
CIT-PER 1.1	City Applications	Performance		The system should be able to perform efficiently to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction
CIT-PER 1.2	City Applications	Performance		The performance of various modules should be independent of each other to enhance the overall system performance and also in case of disaster; performance of one module should not impact the performance of the other modules in the system.
CIT-PER 1.3	City Applications	Performance		Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
CIT-PER 1.4	City Applications	Performance		The solution should provide optimal and high performance for Module's Portal Solution (e.g. eGovernance, ERP, Utilities, etc. portal and dashboard) satisfying response time for slow Internet connections and different browsers.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIT-SCA 2.0	City Applications	Scalability		The solution should be responsible for its robustness, reliability and scalability.
CIT-SCA 2.1	City Applications	Scalability		The Integrated Applications should support common web and mobile browsers like Google Chrome, Internet Explorer, Firefox, Safari, Opera, etc.
CIT-SCA 2.2	City Applications	Scalability		The solution to have capability where any services like Payment Gateway, the mobile devices for queries/ reporting and providing day-to-day approvals by competent authorities as per authorized workflow for different kind of requests; and external entities like bank, departments and others can invoke this framework by passing the required parameters and specifying the desired output.
CIT-SCA 2.3	City Applications	Scalability		The system shall be designed for scalability and allow future expansions in terms of subsequent project phases, increased user density (demography) and geographical coverage.
CIT-SCA 2.4	City Applications	Scalability		The system to have provision for integrating various services and be able to monitor them and operate them.
CIT-SCA 2.5	City Applications	Scalability		The solution should provide option to integrate existing deployed solution under City DICDL and also need to provide scalability option to implement new use cases.
CIT-SCA 2.6	City Applications	Scalability		System to have capability to source data from various systems implemented in City to create actionable intelligence.
CIT-SCA 2.7	City Applications	Scalability		The technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 5 years from Go-Live.
CIT-SCA 2.8	City Applications	Scalability		The system should have ease of compliance to lead to the projected growth of the project.
CIT-SCA 2.9	City Applications	Scalability		Every component of Dholera SIR needs to scale horizontally to very large volume of data.
CIT-SCA 2.10	City Applications	Scalability		The Application Software to have the capability to scale up to future requirements.
CIT-SCA 2.11	City Applications	Scalability		The system should be capable enough of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal efforts.
CIT-SCA 2.12	City Applications	Scalability		The design of the system to consider future proofing the systems for volume handling requirements.
CIT-SCA 2.13	City Applications	Scalability		The application functions to be divided logically and developed as Modular solution.
CIT-SCA 2.14	City Applications	Scalability		The system should be able to scale horizontally & vertically.
CIT-SCA 2.15	City Applications	Scalability		The system to have ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.
CIT-SCA 2.16	City Applications	Scalability		The system should be designed to support the overall SLA requirements around scalability, availability and performance.
CIT-SCA 2.17	City Applications	Scalability		The system should also support horizontal scalability so that depending on changing requirements from time to time, the system may be scaled horizontally.
CIT-ACC 3.0	City Applications	Accessibility		The system to have provision for user to access directly or indirectly in case of disability with the help of assistive technology.
CIT-ACC 3.1	City Applications	Accessibility		Various users should be able to access the system using portal or any other means and should be role based. Different roles which could be defined (to be finalized at the stage of Gap analysis study and documentation) could be Administrator, Supervisor, Officer, Operator, etc.
CIT-ACC 3.2	City Applications	Accessibility		The architecture and application solutions to be designed should promote simplicity and ease of use to the end users while still meeting business requirements. It should provide a simpler and more cost-effective solution. Reduces development time and makes the solution easier to maintain when changes in requirements occur.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIT-CAP 4.0	City Applications	Capacity		Application should have anytime, anywhere access and to address auto sync/ save, efficiency, and peak load handling issues.
CIT-CAP 4.1	City Applications	Capacity		Application should be accessible on all popular devices (PC, mobile or tablets) and across all popular operating system platforms like Windows/ Apple for PCs and Android/ IOS for mobiles.
CIT-CAP 4.2	City Applications	Capacity		The solution should support the proposed hardware and software components (IT and Non-IT) deployed over the tenure of the Contract.
CIT-CAP 4.3	City Applications	Capacity		System should not allow database/system administrators to make any changes to data. It should ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data of invoices and final returns) could be used to reconstruct derived data such as ledgers and system generated returns.
CIT-CAP 4.4	City Applications	Capacity		System should be able to detect any data tampering through matching of hash value and should be able to reconstruct the truth.
CIT-CAP 4.5	City Applications	Capacity		Services/solutions should be flexible and extensible to respond to, accommodate and adapt to changing business needs and unanticipated requirements easily. Consolidate and simplify technology applications wherever possible to minimize complexity.
CIT-CAP 4.6	City Applications	Capacity		Software should use meta-data to configure itself (using declarations rather than coding).
CIT-CAP 4.7	City Applications	Capacity		System should be adhering to latest industry best practices and technical standards.
CIT-AVA 5.0	City Applications	Availability		The system to have provision for high availability for all the services of the system.
CIT-AVA 5.1	City Applications	Availability		The system to have capability for the Deployment of multiple application instances.
CIT-REL 6.0	City Applications	Reliability		The system should serve as the integration point for all domains within the city, operating with strong security and high reliability for 24 hours per day and 7 days a week.
CIT-REL 6.1	City Applications	Reliability		The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.
CIT-REL 6.2	City Applications	Reliability		The system should be reliable handling every request and yield a response. It should handle error and exception conditions effectively.
CIT-MAI 7.0	City Applications	Maintainability		System to ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system, etc.
CIT-SER 8.0	City Applications	Serviceability		Application shall support at least Unicode 5.1/ 6.0 standard based Tri-lingual versions for user interface. It is expected to be in the Gujarati, Hindi and English (India) languages.
CIT-SEC 9.0	City Applications	Security		Application shall support both HTTP and HTTPS (SSL certificate shall be provided).
CIT-SEC 9.1	City Applications	Security		The system must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc.
CIT-SEC 9.2	City Applications	Security		MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. The virus and worms attacks should be well defended with gateway level Anti-virus system, along with workstation level anti-virus mechanism.
CIT-SEC 9.3	City Applications	Security		All the system/Audit logs should be properly stored & archived for future analysis and forensics whenever desired.
CIT-SEC 9.4	City Applications	Security		System to have provision to build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
CIT-SEC 9.5	City Applications	Security		The system's security services should cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components.
CIT-SEC 9.6	City Applications	Security		Third party / Public access – The system to have provision to publish all public contents made available to all users without authentication. The service will

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				authenticate users and allows access to other features of the envisaged application for which the user is entitled to.
CIT-SEC 9.7	City Applications	Security		The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the system should ensure the legacy data confidentiality and data integrity.
CIT-SEC 9.8	City Applications	Security		Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to the application services.
CIT-SEC 9.9	City Applications	Security		Encryption Confidentiality of sensitive information and data of users and Application information should be ensured.
CIT-SEC 9.10	City Applications	Security		Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication should be implemented.
CIT-SEC 9.11	City Applications	Security		Data security policies and standards to be developed and adopted across the Smart City DICDL departments and systems
CIT-SEC 9.12	City Applications	Security		In order to adequately provide access to secured information, security needs must be identified and developed at the data level.
CIT-SEC 9.13	City Applications	Security		System to have provision for role based access for all the stake holders envisaged to access and use the system
CIT-SEC 9.14	City Applications	Security		System to have appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
CIT-SEC 9.15	City Applications	Security		System to have provision through which an authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the authorized user.
CIT-REG 10.0	City Applications	Regulatory		Solution should be compliant with industry standards (their latest stable versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to design, development, security, installation, and testing.
CIT-USA 11.0	City Applications	Usability		Standard and consistent usability criteria must be defined.
CIT-USA 11.1	City Applications	Usability		Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. An intuitive, user friendly, well-articulated navigation method for the applications enhances the usability of the application.
CIT-INT 12.0	City Applications	Interoperability		The system should be interoperable and should comply with open standards for easy integration.
CIT-INT 12.1	City Applications	Interoperability		The entire system/ subsystem should be interoperable, to support information flow and integration. Operating systems and storage technologies from several suppliers must interact well with each other.
CIT-INT 12.2	City Applications	Interoperability		The solution should adhere to the Industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility
CIT-INT 12.3	City Applications	Interoperability		The system should have capability to take inputs from other third party systems as per situational requirements

3.3. Integrated Operations Work Package

3.3.1. CIOC – City Integrated Operations Center

This section covers the Scope of Services of Integrated Operations, Emergency Response Systems, Surveillance and video analytics and AV Hardware & Software.

MSI must conduct a survey of the CIOC at every location that audio visual equipment is to be installed. This is to ensure the site readiness and that all the dimensions, weight loading, network and power cabling is in place ready for the equipment to be installed.

The CIOC incorporates many different software applications. For the dashboards in the CIOC it is crucial that the data required for the CCTV, dashboarding application and other services is available. A data architecture detailing how these applications will be integrated is essential.

Low-level design documentation, BoM and system drawings must be completed prior to installation by MSI. This must include ergonomic studies and sightlines for all audio-visual systems. System designs must be approved by the DICDL prior to procurement.

It is necessary for the MSI to supply and install all of the hardware and software, and to configure the same for operation in the CIOC. Prior to installation on site a factory approval test (FAT) must be conducted to ensure functionality of systems. The FAT does not need to include every individual system but must include at least one type of each system, i.e. one LED display system, one video conferencing system, one video wall system, etc. These systems should be selected to ensure each different type of equipment is tested at least once. The FAT test procedure must be drafted in advance and approved by the DICDL.

Dashboard application and components must be tested (mocked-up using a sample data set) and demonstrated during FAT. AV control platform and UC integration must be tested to ensure end-to-end functionality. Digital signage integration with displays and kiosks must be demonstrated on different types of display LED, LCD, VMS, Kiosk, etc.

User, support staff, and train the trainer training must be provided covering user level and administration interaction with all systems. Training materials and quick reference guides must be supplied. On-going training and user support is to be considered.

MSI shall be responsible for preparing and sharing documents but not limited to;

- Data architecture as part of solution architecture
- Full documentation for CIOC design and implementation along with O&M is required to be handed over. This includes specification of every device used, its maintenance, its firmware version and IP address table. Operations and Maintenance manual must be provided including asset tag register with serial numbers, cabling schematics with cable numbers and types, schedule of maintenance intervals, and actual power and heat loading figures.
- Physical arrangements in plan and elevation showing the location of every device, in floors, wall mounted, under desks, and ceiling mounted.
- Rack cabling diagrams and loading drawings, Configuration data book for all devices and configuration of software, back-up and recovery data.

The CIOC – City Operations Centre is comprised of a number of IOCs (Integrated Operations Centre). Each of the IOCs has a specific function or focus area.

An IOC is a room / space where people can work to run concurrent operations which are all aligned to meeting

the same goal or business function, generally the personnel within an IOC are from different disciplines. An example of this for Dholera would be the Surveillance Centre. There will be CCTV operatives, Police, Traffic and Parking management personnel, Transport coordinators and others, all working within the Surveillance Centre.

CIOC are equipped with large screens for the display of dashboards pertinent to the teams located in the IOC, as well as workstations for each operator or manager. The dashboards provide situational awareness across the function while the workstations provide task focused application and further functionality.

The tools within CIOC are hardware and software applications each provided for a specific function and possibly by different vendors. The application need to expose their data to a dashboard application so it can be displayed on screen. In other cases, the data may also be used for analytics and artificial intelligence.

This section provides information on each of the IOCs and also some of the technologies to be used in the CIOC. In cases where specialist applications are used these are not described in detail here as they are to be found in other parts of this document.

Other than the IOCs, the CIOC may have other technical rooms including but not limited to:

- Supervisors Offices
- Meeting Rooms
- Videoconferencing Rooms
- Utilities monitoring room
- SCADA & Simulation Room
- Training Rooms

CIOC - Overview

The intent of this concept design was to design a CIOC tailored to Dholera's specific requirements and operating procedures, this has been established through learnings and global best practice, while all the time looking towards the future. The requirements for Dholera as captured through the benchmarking exercise and through working with key stakeholders, has been the key information, which has defined this design.

The key considerations are;

- to enable enhanced command and control through integration of technologies, co-location of related functions, and extension of collaborative practices
- deployment of a single platform to ensure interoperability and media-rich communications / collaboration between all users
- provide a common user experience regardless of device or service
- to build a technical landscape which is intuitive in operation, agile, and which presents few boundaries to organic growth / development going forward
- to deliver tangible benefits by taking the user on a journey; Data to Information to Insight; through the use of data sharing, dashboards, Visual Management and Applications
- to specify resilient systems with a 24h/365d high-availability duty cycle systems must work *first time : every time : all the time*
- to virtualize as much of the required functionality as possible, reducing hardware requirements, reducing software proliferation, promoting resilience, and facilitating support
- deployment of a scalable, hybrid on premise / hosted platform with edge services to allow collaboration with external parties
- enable interconnectivity and network traversal for any connected device in terms of on-LAN, on MAN, on-WAN, Internet, or 3rd party infrastructure (i.e. corporate network or mobile telecoms operator)

- a great opportunity exists to unify all systems at the design stage and not integrate post implementation or work around legacy technologies

TECHNICAL DESIGN

The proper operation of the city's IOC's is dependent on people, and their ability to access the right information at the right time and to be able to accurately share this information with others. The systems must be, as far as possible, uncomplicated and intuitive in operation.

To meet the intent of the design and the requirements, the systems must be designed from the outset with a set of standards which can be applied to all the sub-systems. This ensures the sub-systems are compatible and available to operators in the various IOC's.

The IOC's are not only about technology, but also about business process and human factors. These considerations are vital for the IOC's to operate properly and to be comfortable, efficient workspaces.

The guiding principles applied to the technical considerations are:

- to use open standards to enable interoperability and allow additional services to be added seamlessly as the city grows; i.e. for CCTV to use the ONVIF (Open Network Video Interface Forum) standard in all cases
- to integrate between services; Ambulance, Fire, Police, Utilities, Transport, Incident Management, etc. as and when it becomes up and running in future.
- to provide interoperability across "in the field" LTE radio or mobile systems to desktop (softphone, IM), to rooms, to command and control systems, or to situation rooms
- to provide 'portable / scalable' communications (i.e. mobile phone call can be promoted to video capable endpoint or meeting room system)
- to provide easy collaboration from any device (laptop, smartphone, tablet) to other users in the same or different location through wireless sharing of content to displays and to call participants
- wider communication footprint available through call manager / edge services, and federation with other parties
- to utilize the network / structured cabling as primary distribution, control, and physical infrastructure for all systems
- to leverage technologies by fully utilizing the tool sets available in each device or application
- To ergonomically design the spaces for operator wellbeing. This includes sightlines, personal space and furniture considerations.

Technologies used within CIOC:

Telephony: Conference phones (physical / hybrid), Softphones, Desk phones, Cordless

Text: Instant Messenger, Email

Radio: Nextel, UHF, VHF, Airband / Marine, LTE

Videoconference: Telepresence (Room systems), Desktop (codec and software), Mobile

Integration: Calendar Connector, Active Directory, Room Booking, Radio Gateways

Content Sharing and Wireless Connectivity: PC, BYOD

Web conferencing

- **Mobility – Enabled by UC**

Remote / On-scene video; send and receive

Mobile Data Terminals

BYOD

Remote expert access i.e. telemedicine

- **Applications/Platform**

Unified Communications

Mapping

- SCADA
- CCTV
- AV Control and Analytics
- Web / IIS
- Data dashboards
- **Network**
 - WAN – LAN – WLAN
 - Network transport of all video, audio and control protocols
 - Network provision of all situational awareness and focus content
 - Network used to connect sensors, actuators, CCTV, and control devices
- **Audio Visual**
 - Display technologies; LED, LCD, Projection, Signage and Content creation
 - Audio; Radio Integration, Microphones, PAGA, Speakers
 - UX and UI

Operations and Control Centre (OCC)

OCC function is to manage planned events and unplanned incidents of all types. The center will not be manned during periods when there is no event but will be mobilized as and when needed. The center will also be used during incident management exercises to prepare the teams for real incidents

The center has been designed to provide a scalable solution to managing events. There are three areas, separated by an operable / folding wall, in the main room which can be used to manage up to three events concurrently or to be team areas for larger incidents where the whole facility is required.

Situation rooms have been specified so that specific tasks / teams can be working collaboratively on a sub-task without impacting the whole effort.

The CCTV monitoring station is provided to act as a local control for CCTV surveillance which may be required to handle an event. CCTV will be displayable on the large screens in the OCC these operators facilitate that requirement.

General Facilities

- Can scale to handle one or more events, or different aspects of same event
- Displays walls with access to Applications / Dashboards
- Event / Incident Management Software (IMS)
- CCTV control area

Requirements from benchmarking space planning, Occupancy for Cluster A1 numbers show actual on plan count in CIOC, numbers in brackets, where shown, what was estimated based on benchmark study. Where a change exists is it due to different processes / systems in Dholera versus benchmarking sites, in some cases seat counts are affected by building layout.

Sr. No.	Operations Center type	Seating capacity	Desk Console	Video wall
1	WTP	3	1	6x3
2	STP	3	1	
3	CETP	3	1	
4	Dist. Network	3	1	
5	Spare	3	1	
6	CIOC (utility + smart components+ e-Gov)	6		

Sr. No.	Operations Center type	Seating capacity	Desk Console	Video wall
7	ITSM – NOC	2	1	
8	ITSM	2	1	
9	Public display in lobby	NA	NA	-
10	Dispatch and control room for police	4	1	4x2
11	Ambulance	2	1	
12	Fire	2	1	

There is considerable room for expansion in this center and it can handle a significant growth in the city's CCTV system without needing to be enlarged or additional centers to be built.

CCTV coverage will range from; internally within buildings on the ABCD campus, the exterior areas of the campus, and citywide. All cameras will be available in the surveillance operations center – traffic, security; it should be noted that cameras on third party property should also be integrated.

NETWORK CONSIDERATIONS

Network Impact & Architecture

The ABCD network will be impacted by the technologies being proposed for the different IOCs. This impact must be fully understood and the network must be designed accordingly.

Some of these design considerations are:

- Network Topology
- Application Protocols
- Virtual Local Area networks VLANs
- Bandwidth Requirements; WLAN, LAN, WAN
- Hardware Impacts; PoE, PoE+, Ports
- Cabling; IP CATx, Structured, Tie-Lines, Fiber
- Heat Loads and Power Consumption
- Shared or Separate AV / Office Domain Infrastructure
- Redundancy / Resilience
- VLAN Traversal and Protocols (Multicast / Jumbo Packets)
- Security LAN / WAN

This section describes in more details the network dependencies of the audio-visual systems as laid out in this AV design concept for the ABCD building.

- AV Networks

AV devices are segregated into various Virtual LANs (VLANs) as per the requirements. A logical grouping separating devices based on differing network configuration requirements is presented;

1. Audio VLAN
All networked audio devices are covered by this VLAN.
2. AV Streaming VLAN
All video streaming is transported over IP. AV Streaming VLAN consists of the AV streaming devices requiring 200Mbps bandwidth
3. AV VLAN
This is the control VLAN for the AV devices.

4. VM VLAN

Visual Management devices and IPTV are covered under this VLAN.

Signage receiver devices are spread across to pass on the signage content digitally over the network.

3.3.2. CIOC – Technical Specification for Control Room Interiors

Scope of Work

This project is being the first of its kind, scale & prestige so demands for a contemporary, aesthetically appealing, functionally superior, ergonomically designed, safe and 24X7 working facility. In Command Control Room area; conventional wooden cladding, painting, gypsum, 2’X2’ metal ceiling & POP ceilings shall not be accepted.

Materials having adverse impact on the environment and nature shall not be accepted. To ensure the quality of the execution and integrity of the components it is mandatory for the main MSI that they get a qualified agency with experience of turnkey supply and design of Command and Control Rooms or War rooms, including but not limited to Control desk, Illumination, Floorings, Custom designer metal ceilings, wall claddings and doors. Conventional office designers shall not be accepted.

The design of systems, equipment and facilities shall reflect human factors requirements including the following:

- Satisfactory environmental conditions for operator personnel. Including noise, air flow, temperature and humidity, and precautionary measure under uncontrolled conditions (like fire) beyond acceptable limits.
- Adequate space for personnel and equipment for the movements and activities they are required to perform during operation and maintenance, under both normal and emergency conditions.
- Adequate visual / auditory status information and other communication links between personnel and equipment under normal and emergency conditions.
- Adequate illumination for the performance of operation, control, maintenance and training.
- The control room shall be built as per the criteria of “Human Factor Engineering” to improve the efficiency utilization of the operators and provide them Fatigue free working environment.
- Objective: -
 - Ensure maximum standard of safety.
 - Allow Flexibility
 - Minimize maintenance
 - Improve operator’s efficiency & alertness.
- Designing, manufacturing, testing, integration etc., all complete preparation of the related drawings, documents, etc. of the Command and Control room shall be in the supplier's scope. The design shall confirm the requirements & specifications of this bid document.
- In broad, the scope of work and supply shall consist of the following parts: -
 - Interior Design, engineering of Command and Control room.
 - All related services for supply, installation, testing.
 - Spares & Documentation
- Detailed scope of work and supply shall include but not be limited to the following: -
 - Data Collection: Gather all information related to design of the Command and control rooms.
 - Design Proposal: - Submission of various options of Command and Control room layout for client’s approval, strictly complying to international ISO ergonomic norms.
- General: -

- The tentative room area shall be provided to the Command and Control room designer to develop the various options.
 - Supply of the product catalogue, technical proposals including but not limited to drawings, documentation, 3D views, color pallets, for the complete solution.
 - Spares: -A list of manufacturer's recommended spares for operation and maintenance shall be provided.
 - Provide commissioning & warranty spares (Contractor shall utilize these spares of all the equipment that may be required during commissioning & warranty period separately).
 - Manufacturer shall be responsible for safety and security of the installed items till commissioning and final acceptance by Owner (before start of warranty period).
 - Quality assurance & commissioning of the complete system at site to the complete satisfaction of the Owner/Consultant.
- **Control Room Design: -**

Control Room Top View

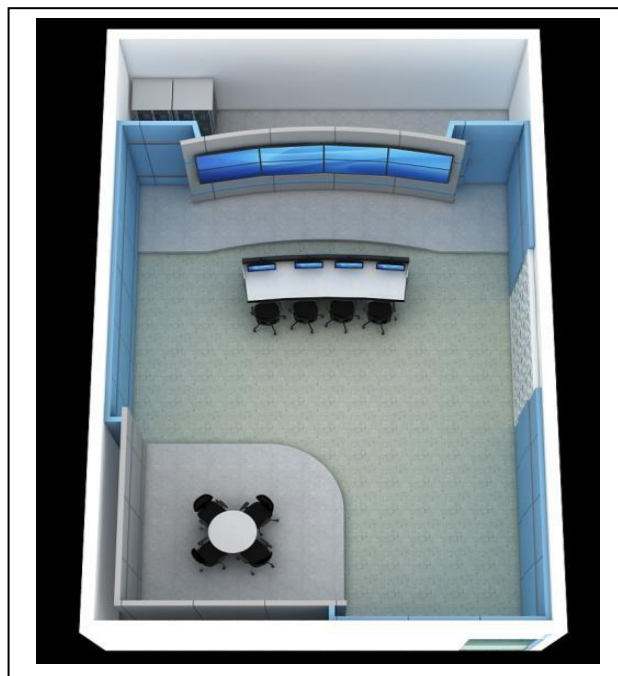


Figure - 28 Control Room design overview (illustrative)

View 1(From Entrance)

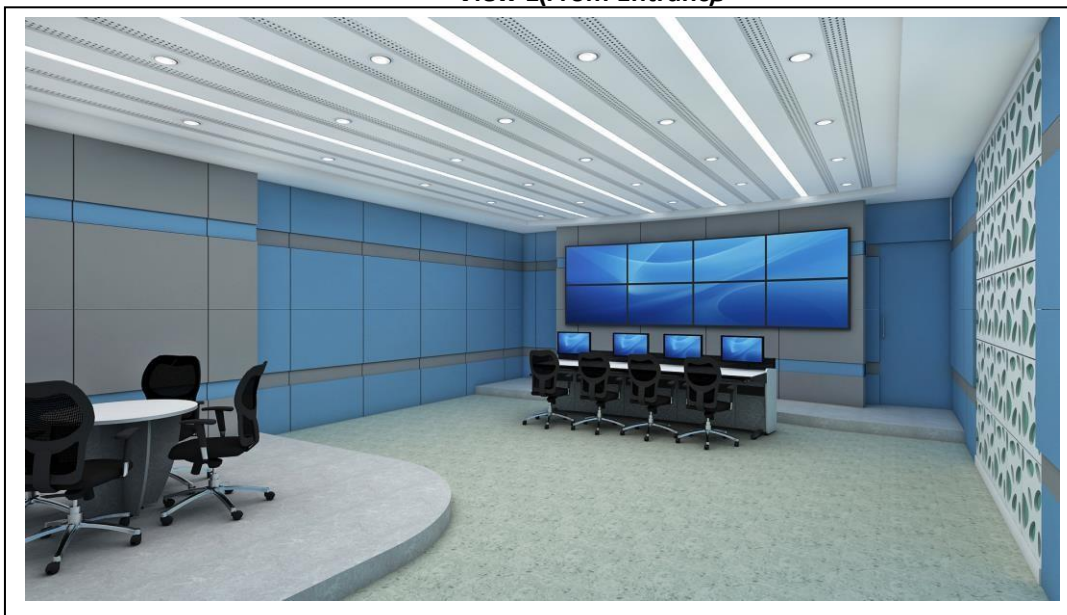


Figure - 29 CIOC – Entrance view (illustrative)

View 2 (Side View)

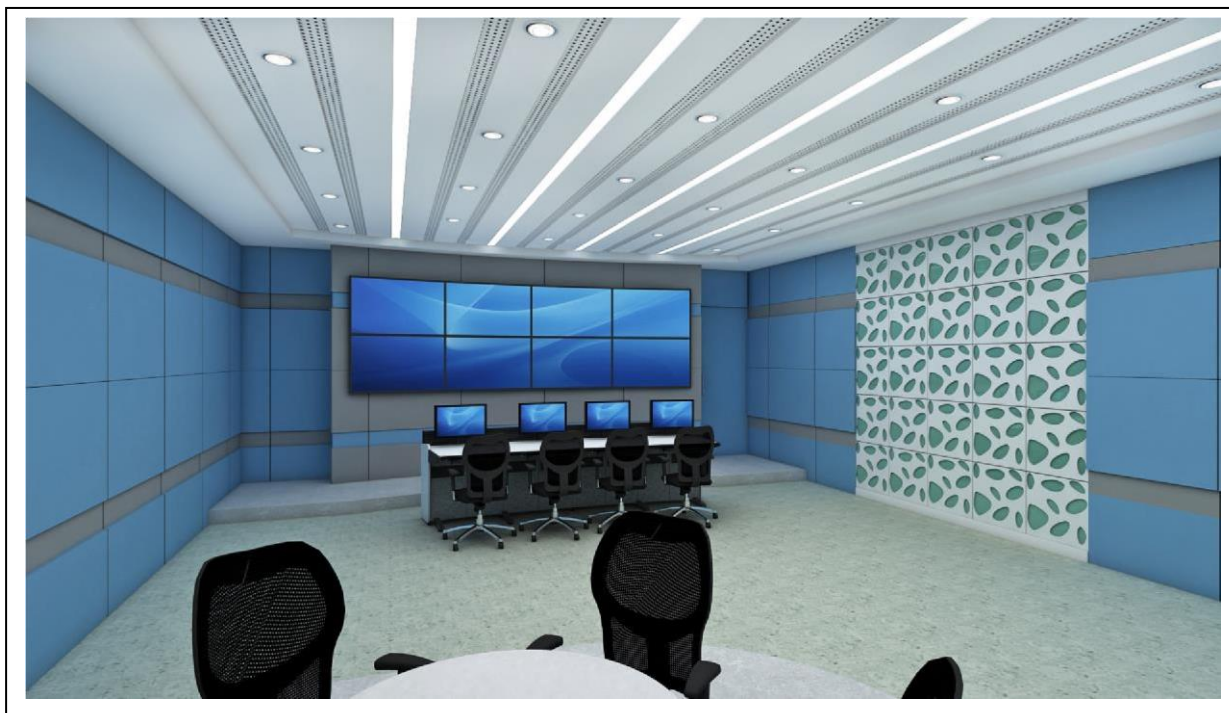


Figure - 30 CIOC – Side view - 1 (illustrative)

View 3

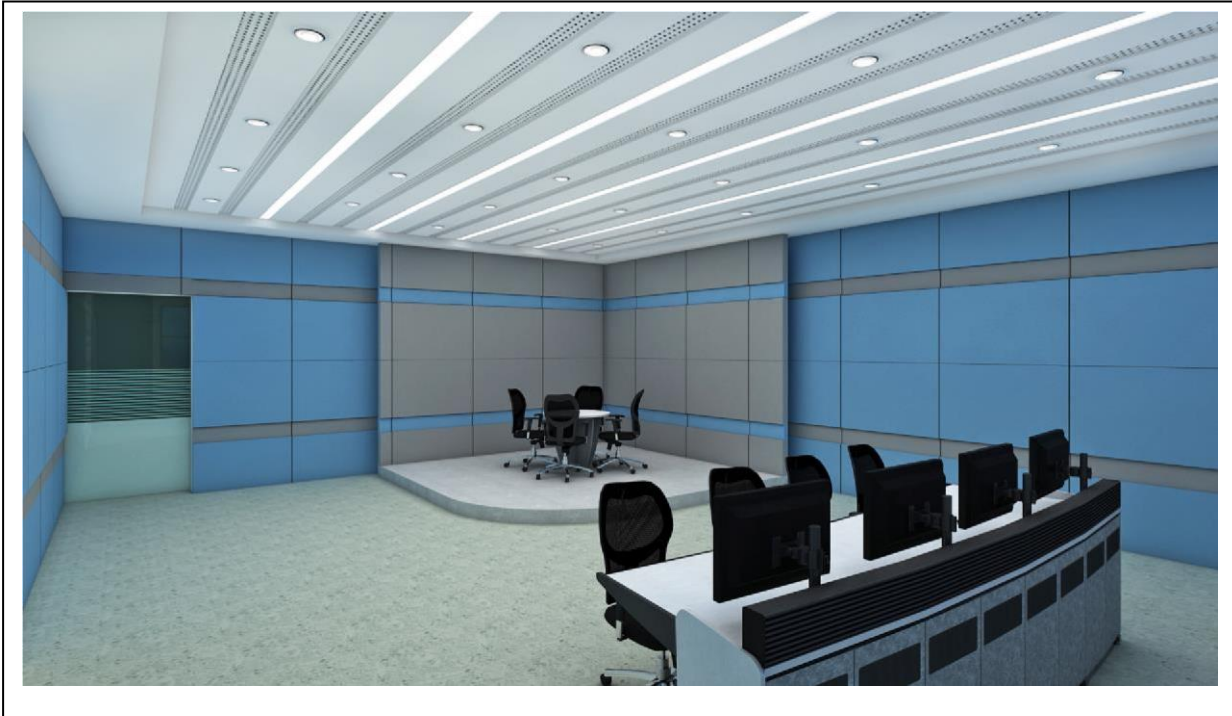


Figure - 31 CIOC – Side View -2 (illustrative)

Mandatory Requirement:

The project demands for a contemporary, aesthetically appealing, ergonomically designed, safe and 24X7 working facility. Conventional wooden cladding, painting, gypsum, POP ceilings (for Command and Control Room area) shall not be accepted.

- Submittals (MSI to produce these documents from control room interior Manufacturer OR supplier along with the bid): -
 - Certificate for ISO 9001-2015 quality certification as a proof of quality management system implementation in Manufacturing processes for at least 5 years.
 - Certificate for ISO 14001:2004 for Environment Management System.
 - Certificate for OHSAS 18001:2007 for Occupational Health and Safety.
 - Ergonomic compliance report for control room layout as per international ISO ergonomic norms to be submitted along with the bid.
 - Manufacturing Unit/Capability: If asked, supplier to arrange factory and product inspection before placement of order, to ensure that the vendor is capable of in-house production of the ordered goods.
 - To prove supplier's seriousness in the business; Printed Catalogues and Locations of Demo rooms to be furnished.
- Warranty:
 - Five year's warranty against any manufacturing defect on Control Room design & Control Desk including but not limited to Floorings, Custom designer metal ceilings, wall claddings and doors.
- Proven Track Record:
 - The MSI/supplier to produce following documents from the control room interior Manufacturer along with the bid: -

- Minimum 10 installations of control rooms/ NOC areas with appreciation letters for the turnkey scope including but not limited to control desks, ceiling, flooring, illumination and wall cladding from reputed companies to be submitted along with the bid. These packages should have been executed on or before Bid release date.
- Design Criteria: -
 - The ceiling, paneling and partition must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure.
- Product Specific Mandatory Requirement
 - Copy of Test certification for ASTM E84 for the surface burning characteristics of wall paneling tiles and ceiling tiles to be submitted along with the bid. This is mandatory requirement from Fire safety point of view.
 - Raw-material supplier data alone is not acceptable.
- Quality Criteria: -
 - To ensure uniformity, consistency & quality in final product the Command & Control manufacturer should have In-house Powder Coating Plant, metal manufacturing and wood processing plant.

TECHNICAL SPECIFICATIONS:

- The Control Room & Conference Room must be compliant to international control room ergonomic norms (ISO-11064) MSI to enclose a report for the same.
- In Addition to it a 60 Sec. simulation Video/Walk through to be provided with technical Bid.

CONTROL DESK:-



Reference Image

Figure 32 CIOC- Control Desk (illustrative)

1. Equipment Mounting
 - a. The control desk shall house computer equipment's, HMIs, Ethernet switches, Rack mounted equipment's, Power Distribution Unit. The CPUs shall be mounted on Slide out CPU trays (mounted on Heavy-duty slides) for ease in maintenance.

2. Structure

- a. Made of heavy-duty Extruded Vertical and Horizontal Aluminum profiles of 6063T6 grade. The Extrusions shall be duly powder coated with 40+ micron over all surfaces.
- b. All sheet metal parts must be finished with a durable, black, electrostatic powder coating with average application of 60-90 microns over all surfaces.
- c. Pre-treatment process shall not generate sludge or heavy material.
- d. The supplier to perform following tests during inspection: -
 - i. Adhesion test: ISO 2409:
 - ii. Impact test: ASTM D 2794: 40kg
 - iii. Conical mandrel test: ASTM D 522:
 - iv. Scratch test: IS 101-1964:
 - v. Salt spray (FOG) test: ASTM B 117: 600 hrs.
- e. To allow future extension and expansion; a weld free system to be proposed. Interconnecting joints should not be visible.
- f. The Entire console must be UL Listed. Certificate need to be submitted along with the bid.
- g. The desk must be Greenguard Gold Certified. Certificate need to be submitted along with the bid.
- h. The structure should be rigid enough to withstand BIFMA X5.5. The structure should allow easy assembly of Hinged Shutters, Slat wall, Gland Plate, Monitor arms in extremely rigid manner. Certification of BIFMA X5.5:2014 (on all test parameters) by a Reputed test facility to be enclosed with the tender proposal.
- i. Grouting of the desk is not allowed for BIFMA test as well as site installation.
- j. Standard office type, panel, post and open furniture will not be acceptable. Structural integrity of the Console System is a priority; therefore “cubicle” type walls shall be deemed unacceptable.
- k. Console should be tested for Seismic Zone 4 or better, valid report from government approved research institute to be enclosed with technical tender proposal
- l. The OEM should have trade mark registration issued by Government of India for the console offered in this tender.

3. Work Surface: -

- a. The material of the working surface should be minimum 25 mm thick MDF with High Pressure Laminate finish. The laminate shall be Scratch resistant and high hardness.
 - i. The MDF shall confirm to ANSI A208.2
 - ii. The Laminate shall be scratch resistant with ANSI/NEMA LD3 certification. iii. The laminate shall be Greenguard certified. This laminate shall have added benefit of an extra-wear surface and provide a high resistance to scuffing, and cigarette burns. The material shall also have a skid resistant surface.
 - iii. The Desk manufacture must be FSC certified. The manufacture must have had this certification from last one year. Certification to be submitted with the tender bid.
 - iv. Copy of Test certification for ASTM E84 (from UL) for the surface burning characteristics of products and materials. Test must reference the actual assembled components for wood-core panels including core, laminates, edging.
 - v. Raw-material supplier data alone is not acceptable.

4. Designer Front Edging Option:-
 - a. Front ergonomic edge shall be injection moulded polyurethane edge (minimum 50-60mm in depth) on the profiled wooden core and must not be inserted or glued. Consoles must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure. Sample to be produced for technical approval before opening of price bid.
 - i. PU edge shall have flexibility to design at radius.
 - ii. T shape of PU / PVC / PP shall not be acceptable as they can be pulled out manually.
 - iii. Shape of the PU shall have an ergonomic slant with min 50-60 mm depth at the operator's sitting area. This is to give a grand look and maximum comfort.
 - iv. The overall thickness of the PU shall be within a range of 30-40mm.
 - v. Other open edge shall be of PVC / ABS / PP with Greenguard specs. vi. Manufacturer to show in-house facility to ensure smooth service in case of any such requirement in future.
5. Shutters & Side Legs
 - a. Front, back shutters shall be of 18 mm Laminated MDF Board with premium finish. Side leg shall be of 25mm of the same finish. The Laminated MDF shall confirm to E1 Grade, ANSI A208.2 and CARB certified and must follow EN 622-5 standard. Hinges shall have life time warranty. Entire console to be RoHS certified (from Intertek). Certificate to be submitted along with the bid.
6. Monitor Arms/Arrays and Attachments
 - a. Die cast mounted Aluminum arm; fixed firmly on MS Pole.
 - b. These poles will have same powder coating as that of Modular Rear wall.
 - c. Monitor and Functional holder shall guarantee optimum viewing distance. All ergonomic aspects shall be taken in to account. It shall be capable for mounting all type of LCD display with Dimensions between 17" to 27" using suitable adopter/additional base plate for complying VESA standards 75 x 75, 100 x 100, 200 x 100 & 200x200 mm.
 - d. For configuration of working position, it shall allow the technical staff to rotate/ tilt/ raise/the monitors as well as fix their adjustment in a quick and easy manner.
 - e. The Monitor and functional holder shall bear the weight of the mounted Monitors; hold the monitors firmly without shaking. Max load for monitor shall be 10kgs for single & dual tier arrangements.
 - f. The monitor arm should be Articulating monitor arm.
 - g. Up-down moment can be performed without tools.
 - h. Pole Height - 455mm
 - i. Extension - 400mm
 - j. Tilt - 180 Degrees
 - k. Swivel - 270 Degrees
 - l. Rotation around Monitor Pole 360
 - m. It shall be designed to enable replacement of existing LCD display with other type during monitor changes necessitated by future developments.
 - n. Articulating monitor arm, Flexible monitor arm, depending on console configuration. e. Upper-level articulating monitor arm (Double high option).

7. Modular rear walls shall be made of heavy-duty extruded aluminum profile with better aesthetic appeal; allowing for various viewing levels and privacy. Conventional office type slat wall shall not be accepted.
 - a. Modular walls shall be made of approx. 2mm-6mm thick Extruded Aluminum (HE9WP aluminum alloy). 6063T6 shall not be acceptable for this Rear wall as rear wall shall be subjected to Shearing / sliding loads.
 - b. Shall be designed in such a way that no joints or gaps are visible in the entire width of the console.
 - c. Load bearing capacity shall be min 30 kg per meter.
 - d. It should have linear slots running throughout the length to accept modular components (slat wall mounting system, telephone arms, pen holders, paper holders).
 - e. It should have high Load bearing capacity.
 - f. No buckling when arms are fully extended
 - g. No screws should be visible when joining table top to the Slat wall and on the top of the slat wall. OEM to produce sample before commencing the manufacturing activities.
 - h. MSI to ensure that the desk manufacturer has done minimum 20 projects with Slat wall (this is a mandatory requirement). The reference unpriced POs must be submitted along with the bid.
8. Electricals
 - a. Each console shall be equipped with individual power distribution unit. The Electrical power distribution unit shall be capable of being switched on/off and provide safe supply to all the consuming equipment individually. The console should be electrically earthed for all the body part which are conductive.
 - b. Power supply socket should be dual type i.e. Universal type.
 - c. Rear vertical mounting with powder coated CRCA body with RAL 9005 color having universal sockets with Inbuilt 16A single pole MCB.
 - d. Entire console to be RoHS certified (From Intertek). Report to be enclosed with the technical bid proposal.
 - e. Shall confirm to BS 546. Entire console to be ROHS certified.
9. Cable Routing Arrangement
 - a. Designed with vertical and horizontal cable trays to allow for continuous cable management between the cabinets. The design of console shall allow cable run, from the floor hollow channel
10. Cooling (Datasheet to be submitted along with the technical bid)
 - a. Rear shutters of each console should have provision of Airflow opening for cooling and heat dissipation effect.
 - b. Rear panel/door-mounted ventilation fans (optional).
 - c. Ventilation fans shall have the following properties:
 - i. Fans must be available for mounting on the doors. The individual situation may dictate a change in the ventilation requirements.
 - ii. Axial fans should be aerodynamically shaped with metal construction and metal blades for longer life
 - iii. Can operate in -10deg to +55 deg
 - iv. Noise level should be below 50dB
 - v. Air flow should be approx. 105 CFM
 - d. Screws shall not be visible on the front metal plate where the fan shall be mounted.

11. Hardware
 - a. All bolts must be of SS material to avoid rust due to environment. Remaining hardware shall be Nickle Plated with RoHS certificate.
12. Warranty
 - a. 05 years against manufacturing defects.
 - b. 05 years on structure stability.
 - c. 05 Years on all moving / non-moving parts.
13. Quality Assurance of Consoles
 - a. The proposed console must have been supplied & working satisfactorily to reputed government agency (either directly or through system integrator).
14. Undertaking on letter head for Maintenance Support
 - a. Supplier to generate the same with BID document.
 - i. Supplier to maintain the components for 5 years to support expansion and similarity
15. Self-Declaration format
 - a. Vendor to declare; whatever has been complied will be there in the end-product. If anything is faulty then the consoles are liable for rejection and shall be replaced on FOC.
16. Checklist for Certificates, Norms etc. (Valid certificates and reports to be submitted along with the bid):-
 - a. Certification of BIFMA X5.5:2014 (on all test parameters) by a Reputed test facility.
 - b. The consoles shall be suitable for areas of Seismic zone 4 or better. MSI to provide Seismic Test Report from government approved research institute along with the bid.
 - c. Entire console should be RoHS (UL/Intertek) certified.
 - d. Copy of Test certification for ASTM E84 (from UL) for the surface burning characteristics of products and materials. Test must reference the actual assembled components for woodcore panels including core, laminates, edging.
 - e. The Entire console must be UL Listed. Certificate need to be submitted along with the bid.
 - f. The desk must be Greenguard Gold Certified. Certificate need to be submitted along with the bid.
17. In House Quality Lab
 - a. Supplier to demonstrate in-house test lab to prove quality consciousness / seriousness.

Interior (Agency must submit Greenguard Certificate for Control Room Interior along with the technical bid)

1. ITEM NO. 1 STRAIGHT METAL PANELLING

- A. Panel should comprise of perforation for making the cladding and partitions acoustically sound. Min 20% panels shall be perforated or as specified by the consultant.

- B. There should be possibility of wide variety of colors and images to be used on the wall elements to give the aesthetic and state of the art look to the control room.
- C. Panel design to support proper LVS integration.
- D. Gluing, screwing, ACP, Laminates are not allowed.
- E. Panel design should ensure that when the tiles need to be removed for service maintenance of Lighting & AC ducts & itself cleaning, the risk of tile damage is minimized.
- F. Structure should allow uninterrupted flow of wires/cable/tubes of max. dia 25mm.
- G. Special connection joineries to take care of seismic vibration.
- H. Design & Material Specification for Paneling
 - i. Factory made removable type self inter lockable metal panels of Preformed textured Hot dip galvanized strips and sheets of low carbon steel coated on one side with rigid polyvinylchloride (PVC) film and on the other side a coating based on cross linkable polyester resins (sheet thickness 0.6mm & PVC Coating 0.15mm). Make shall comprise of specially designed combination of perforated and non-perforated panels through CNC laser Cutting, bending & punching. Panel shall be of 0.75mm thick galvanized metal of approved color. Panels shall be designed to achieve shape and design as per the design consultant. Panels shall be fixed using hook fitting on structure. Overall system thickness for paneling shall be 70mm to 85mm and for partition shall be 85mm to 110mm.
 - ii. As per design panel shall comprise of hexagonal perforation for making paneling and partitions acoustically sound. Acoustic grade fire retardant fabric (min 1.5mm thick) will be fixed at some parts of the control room.
 - iii. Panel shall be design in such a manner that it takes care of undulation of civil walls and Gives perfect flat surface finish and compile easy service & maintenance procedure.

I. Design:

- i. The cladding panels shall be made up of combination of two sheets locked and riveted together and polystyrene shall be used as infill to achieve strength and acoustics. The front tile (PVC pre-coated metal sheet) shall be perforated/ non-perforated as per the design requirement and the back tile (Powder coated 0.6mm GI sheet) shall be designed in such a manner that it fits on the back portion of the front tile. Once the tiles are fitted together then these will be manually riveted. These tiles shall be bend through CNC, machine punched & laser Cut to achieve perfect accuracy.
- ii. Structure shall be made from heavy-duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm) and shall allow uninterrupted flow of wires/cable/tubes of max. dia. 25mm.
- iii. Structure shall be securely grouted from wall, roof and floor. It shall be made up of 1- 1.6mm thick vertical Slotted rolled C sections (Upright) and horizontal rolled 'C' connectors. Grid of desired dimension shall be formed by Vertical and horizontal sections having 50mm pitch.
- iv. Wall panelling system must be RoHS certified from UL/Intertek. Valid certificate to be submitted along with the technical Bid.
- v. Panel shall be design in such a manner that it takes care of undulation of civil walls and gives perfect flat surface finish and compile easy service & maintenance procedure.

- vi. Sound transmission class (STC) value of 35 for Wall Panelling & Partition. (According to IS: 9901 (Part III) – 1981, DIN 52210 Part IV- 1984, ISO:140(Part III) -1995, test report from reputed agency to be submitted along with the technical Bid.
- vii. Wall Panelling & partition shall be Seismic Zone 5 Tested & certified from approved government agency, relevant certificate to be submitted along with the technical Bid.
- viii. The frame should be securely grouted from roof and floor with flexible joints to absorb seismic vibration.
- ix. All the paneling structures shall be seismically qualified and the test certificates to be provided before commencement of the job.
- x. Panel shall provide better thermal, electrical insulation as compared to normal GI panels. It shall be non-reflective/glare free and be eligible for food contact.

J. Material Selection:

- i. Available Width- 300mm to 1200mm (in multiples of 150mm).
- ii. Available Height- 150mm to 750mm (in multiples of 150mm).
- iii. Thickness- 10mm to 15mm for perforated tiles with acoustic fleece without back cover
- iv. 25mm to 30mm for non-perforated tiles with back covers

K. Material Testing/Certification:

- a.) **PVC pre-coated sheet:** The front PVC sheet must qualify reaction to fire tests for building products; Ignitability when subjected to direct impingement of flame. The top finish sheet must be Food Grade. Front sheet must have these certifications and the same must be submitted along with the bid:-
 - i. Fire rating and Low flame spread: EN ISO 11925-2, EN 13823 and ASTM E-84.
 - ii. Food grade: EU10/2011
- b.) **Core material (compressed polystyrene):** Must comply to meet or exceed the requirements of Specification for Rigid, Cellular Polystyrene Thermal Insulation and applicable building codes and following tests. The reports to be enclosed with technical bid proposal.
 - i. ASTM C 578.
 - ii. 9301/ ISO: 140/ASTM 413.
- c.) **Powder coating:** Must qualify 600 hours' salt spray test.
- d.) Wall Paneling tile must be ASTM E-84 certified from UL for surface burning characteristics. Valid report to be submitted along with the bid.

L. Component Specification:

- a.) **Floor Mounting: -**
 - i. 3mm thick C channels welded together to form 'I' section having minimum height of 150mm. This I section shall be welded on 3mm thick MS grouting plate.
 - ii. This assembly shall be grouted on the floor with the help of M10 Anchor Fasteners.
 - iii. These Floor Mountings shall be the base support for the vertical uprights spaced at a center to center distance of 1200mm maximum.
 - iv. Contractor must ensure proper marking and levelling before proceeding with any floor grouting.
- b.) **C Section (Upright) fixing: -**
 - i. 56 mm wide Slotted rolled C section (UPRIGHT) (1 to 1.6 mm thick CRCA). Maximum single piece Length shall not exceed 2700mm.
 - ii. All sections will be dual slotted with 50 mm pitch.
 - iii. These Uprights shall be mounted over the floor

mountings and shall be connected by C connectors made up of 1.0mm to 1.6mm thick cold rolled 'C' sections. iv. The installation to be carried out with Uprights spaced at 1200 mm (center to center) securely fixed to the floor slab by means floor mountings.

v. The uprights shall be firmly held with L shaped wall mounts made up of 2 mm thick MS sheet duly powder coated. One portion of L mount shall be grouted with wall and other will be having a minimum slot length of 75mm.

vi. The L clamp and the upright will be bolted together with M6 bolts.

c.) End Cap

i. 0.6mm to 0.75mm thick C shaped tile; like the panel tile will be bolted on the extreme end Uprights to hide the grid structure.

M. Panel:

i. The panels shall be hooked on the uprights. ii. Panels shall have integrated hooks (which shall cut and bend on high precision laser machines). iii. The panels shall have minimum gap of 5mm between two tiles (on vertical and horizontal edges) so that the tiles can be replaced and installed easily.

iv. The hooks of the Panels shall have a length of 20mm (for the upper hook) and 10 mm (for the bottom hook). So that these panels are firmly held on the uprights.

v. The panel shall have HOOK in arrangement (With gravity lock).

vi. The hooks of the Panels should have a length of 20mm (for the upper hook) and 10 mm for the bottom hook. So that these panels are firmly held on the uprights during seismic vibrations

N. Corner Cap:

i. On extremes ends of control room the wall connector (L- profile) shall be fixed on the perimeter walls. This L-section shall be snap fitted and then bolted to the walls.

O. Door Profile:

i. Door frame shall be fixed with these profiles only to have proper integration of doors with the overall system.

P. Feature:

i. Raw material for tile & powder coating should not affect environment, vendor to provide necessary test certificate. ii. Color should not fade over 10 years.

iii. No sagging iv. Easy and quick installation

v. Low cleaning effort

vi. Vendor to demonstrate one portion at wall paneling & ceiling at their premises before dismantling & shipping to site. In short, a FAT (Factory acceptance test) to be carried out at vendors works for ceiling & paneling. MSI to submit an undertaking for the same.

vii. 100 % modular design. At site, no cutting, chipping work is allowed. viii. The tile shall be bend resistant. ix. Copy of Test certification for ASTM E84 (from UL) for the surface burning characteristics of wall paneling tiles and ceiling tiles to be submitted along with the bid. This is mandatory requirement from Fire safety point of view. Raw-material supplier data alone is not acceptable.

x. User's Health: Agency to submit GREENGUARD Certification for compliance with minimum indoor air quality standards per ANSI/BIFMA M7.1-2007 for Control room interiors. This is mandatory requirement from operator's health safety point of view and certificate must be submitted along with the bid. Raw-material supplier

data alone is not acceptable.

Q. Curvilinear Metal Paneling:-

- i. All the properties and material of construction shall be like Straight Metal paneling however the front tiles shall be having perfect curve to meet the aesthetical requirement of the Control room and shall allow easy installation of the LVS/Screens on it.

R. Lattice Paneling



Figure - 33 Lattice paneling (illustrative)

- a.) **All the properties shall remain like Metal paneling. The tile size shall be 2'X2' or 1M X 1M. The front tile shall have laser cut designs (as per approval) and another tile shall be fitted into it to have Highlighter view.**
 - i. The tiles will be having cut-outs in such a way that when the tiles are rotated by 90 degrees the design pattern of the entire wall shall be changed. Using the same tiles and different orientations we will have multiple design possibilities. ii. The aim is to provide a contemporary look to the CCR. It shall be a tool less & screw less fixing.

2. ITEM NO. 3 DOORS

a.) Metallic Door

- i. Door with spring and locking arrangements and both way handle made with rigid thermo fused film metal panels. Specification: 0.6mm thick Metal panel sheets, cavity filled with honeycomb in roll form of make inside adequate quantity. Material of the paneling and that of metal door will remain the same.

b.) Glass Door:-

- i. 12mm thick tempered clear glass door with door spring and locking arrangements and both way handle with patch fittings.
- ii. Glass Properties:
 - a. Safety (tempered): when broken, must split into tiny harmless pieces.
 - b. Dimensions as per the BOQ.

c.) Automatic Power Operated Sliding Door:-

- i. Door shall be complete with 12mm thick frameless tempered clear glass leafs with all hardware and miscellaneous equipment. Power connection and cabling: Conceal within the Door head unit cover. Include operator, header with roller track, carrier assemblies, framing jambs, sliding door panel(s), activation, safety devices and accessories required for complete installation. ii. Accessories :
 - a. Center Lock Housings
 - b. Vertical Stiles
 - c. Floating Header Bars

- d. Door Patches
- e. Channels and Header Bars
- f. 12mm thick tempered clear glass leaf etc.

3. **ITEM NO. 4 FALSE CEILING**



Figure – 34 CIOC - False ceiling (illustrative)

1. **Designer Acoustic Metal False ceiling with Straight/Curvilinear linear Plank Ceiling (Main Control Room)**

- i. Factory made acoustic modular metal false ceiling of powder-coated panels. Make shall comprising of perforated and non-perforated metal panels made through CNC laser cutting, bending & punching. Panel shall be of 0.6mm galvanized metal of approved powder coating finish. Panels shall be designed to achieve shape and design as per the design consultant with the combination of acrylic panels with lights, designed to enhance visual feel, with provision for easy installation and maintenance, integrated lighting and scope for integration of building services like HVAC and fire detection/ fighting system. Metal modular false ceiling must have Sound absorption coefficient (NRC) value 0.30 according to IS:8225-1987, ISO: 354-1985 and ASTM 42390. These certificates must be submitted along with the bid.
- ii. As per design panel shall comprise of micro perforation for making false ceiling acoustically sound. The non-perforated ceiling tile shall be Class A fire rated as per ASTM E-84. Test certifications to be submitted along with the bid.
- iii. Structure shall be made from heavy-duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm). It shall be securely grouted from roof with help of anchor fastener and GI self-threaded rods. It shall be formed with the help of slotted rolled W sections (stiffener) and M section (Master) with help of M6 cage nut and bolts.
- iv. The powder coating metal sheet shall have possibility of being formed mechanically per the specific needs of the project. The powder coating shall be able to undergo stretching up to 100% and therefor follow (adhere to) bend with the steel in all its deformation.
- v. UL Certified Integrated channel in ceiling for quick installation & replaceability of continuous linear light: The ceiling system having integrated inbuilt channel for installation of cove lights and shall permit quick and easy replacement of cove light without using any tools. Replacement to be carried out within 120 Seconds per meter.
- vi. The Ceiling must be RoHS certified (from UL/Intertek) to ensure restriction of hazardous substance in any of the materials. (Certificate to be submitted along with the technical Bid)
- vii. The Ceiling must be tested and certified for Seismically Zone 4 or better earthquake vibrations. Bidder/MSI to provide Seismic Test Report from government approved

research institute along with the bid Certificate to be submitted along with the technical Bid).

- viii. The master section shall have laser cut profile to enable fixing of perforated, Non-Perforated & diffused continuous LED section with acrylic sheet.
- ix. The ceiling system should have double safety system to take care of seismic vibrations. Seismic joint clip on main W & cross runner will be made up of section having sizes 100 mm by 20mm. vii. The ceiling planks shall have locking redundancy to enhance seismic impact resistance.
- x. Panels are then snap fitted individually on the grid framework. The panels are also hold by safety wire to ensure that these tiles do not fall during seismic vibrations.

a.) Dimensional Details:

- i. Non- Perforated Tile: - Machine profiled GI sheet of 290mm (Wide) available in various length of 600mm to 1800mm in multiple of 300mm
- ii. Perforated Tile: - Machine profiled GI sheet with fleece of 146mm (Wide) in various length of 600mm to 1800mm in multiple of 300mm.
- iii. Type- Clip on with double locking arrangements. (Key requirement). Should be easily openable to access above ceiling services. Special connection joineries to take care of seismic vibration.

b.) Material Testing/Certification:

- i. Powder coating: Must qualify 600 hours' salt spray test.

c.) Component Specification:

i. Master M Section:

- a. 1.2 mm thick GI section length 1200mm. the installation to be carried out with runner's spaces at 1200/1500/2100 mm center to center securely fixed to the hanging "c" section by means at M6Nut and bolts.
- b. The end section shall be covered by 0.8mm thick powder coated MS sheet.
- c. The master section shall have laser cut profile to enable clip on tiles viz. perforated, Non- Perforated & diffused continuous LED section with acrylic sheet.

ii. Hanging W Section:

- a. Specially machine profiled W section 65x15x0.8mm. the section should be 2400 mm long & shall run across the length at the room.
- b. Centre to center distance between W section shall be 1000mm.
- c. These sections are securely fixed to the slab by means of Metal fastener and 8mm GI rod fully threaded (with hex nut for precision level adjustment.)
- d. The two-master section shall be attached to each other by means at fixing plate 45x34mm & M6 cage nut & bolts.

iii. U Section:

- a. Machine profiled 'U' Section 150x77x0.6mm section to accurate continues running light.
- b. It shall have provision for fixing acrylic sheet.
- c. This whole assembly shall be hang from roof slab with help of anchor fastener and full threaded GI rod.

iv. Ceiling Plank:

- a. It shall have Laser cut holes/cut-outs for light fixing as per defined lux requirement and approved layout.
- b. Non-perforated tile slots to be punched to accommodate AC grills.

2. 2' X 2.5' Designer Acoustic Metal Plank False ceiling (Call Center, Server Room, Admin Office, VIP Lounge & Small Meeting Room Area)

- i. Factory made acoustic modular metal false ceiling of powder-coated panels. Make shall comprise of perforated and non-perforated metal panels (2' X 2.5') made through CNC laser cutting, bending & punching. Panel shall be of 0.6mm galvanized metal of approved color. Panels shall be designed to enhance visual feel, with provision for easy installation and maintenance, integrated lighting and scope for integration of building services like HVAC and fire detection/ fighting system.
- ii. As per design panel shall comprise of micro perforation for making false ceiling acoustically sound with fire rated acoustic fleece.
 - a. Ceiling Plank:
 - i. Plank shall be made from 0.6mm thick GI powder coated sheet of approved shade and sizes.
 - ii. Light fitting can be defined as per the LUX requirement.
 - iii. It shall have Laser cut circular hole for light fixing as per defined lux requirement and approved layout.
 - iv. Non-perforated tile slots to be punched to accommodate AC grills.
 - b. Properties:-
 - High NRC (Noise Reduction Co-efficient)
 - Better Light reflectance & Fire performance.
 - Humidity Resistance.

3. Calcium Silicate Board ceiling on the periphery of the Control room, Conference Room Lobby Area, Call Center, VIP Lounge, Conference & Server Room:

- i. Plain Calcium Silicate Acoustic Boards for false ceiling with 12mm Approx. thick, Structure for underside of suspended grid formed of GI perimeter channels. Wood screws and metal expansion raw plugs for fixing with wall. Plastic emulsion paint of approved make and shade for finishing surface of Calcium Silicate Boards.
- ii. General Specification of Calcium Silicate Board: this board is manufactured from a mixture of Portland cement, fine silica, special cellulose fibers and selected fillers to impart durability, toughness, fire and moisture resistance.
- iii. Expansion after expose to the water for 24 Hr.: 0.12%, Noise Resistance: B38, Water absorption by Weight: 34%, Fire resistance: BS 476 incombustible A1 Class.

4. ITEM NO. 5 LIGHTING AND ILLUMINATION

i. LED lights

- a. Brief: - The lights shall be available in flat panels. These shall be designed and developed with slim shape for stylish look. The product shall have better color rendering index for interior illumination.
- b. In LED shall have three basic choice of colors like cool white, warm white and neutral white. The LED lights shall have uniform light distribution without any spots on surface of panel, to make it highly luminous.
- c. **Features: -**

1. Round LED Lights

- a) Temperature- 3000 K to 6500K
- b) CRI >70
- c) Power Consumption 12W to 24W
- d) Aesthetically designed enclosures
- e) Highly efficient constant current LED drivers
- f) Ideal replacement for traditional PAR/CFL lamp
- g) Up to 80% energy saving.
- h) LED's life >25,000 hrs. @ L70

2. LED based Square Light

- a) Make: OSRAM/Philips/Wipro/Pyrotech
- b) Light source: LED
- c) Lumen output: 2800 – 3500
- d) Light color: 3000K - 6500K
- e) Power consumption: 29 to 38 W
- f) Voltage: 220-240V AC 50Hz
- g) Color: White
- h) Lifetime: 35000 burning hrs. (At L70)

3. LED based Strip Light

- a) Make: OSRAM/Philips/Wipro
- b) Light source: LED
- c) Lumen output: 840 lm/Mtr.
- d) Light color: 3000K/6000K
- e) Power consumption: 9.8 W/Mtr.
- f) Voltage: 12V AC 50Hz
- g) Optics: Sand-blasted matt finish reflector
- h) Color: White
- i) Lifetime: 40000 burning hrs. (At L70)

5. ITEM NO. 6 WIRING FOR CEILING LIGHT

- i. Wiring for ceiling lights: For ceiling wiring inter looping will be done and switches will be provided.
- ii. The system of wiring shall consist of PVC insulated copper conductor stranded flexible FRLS wires of 1100 volts grade of insulation, in metallic conduits for all exposed wiring and PVC/ metallic conduits for all concealed wiring. Minimum size of copper conductor shall be 1.5 sq. mm for lighting and 2.5 sqmm for power. Color code shall be maintained for the entire wiring installation that is Red/Yellow/Blue (or as per Local Standards) for the all single phases, Black for neutral and Green for earthing.
- iii. Appropriate ferrule will be used in both the side (LDB Side & Switch's Side)
- iv. Note – Each Light Fixture will have 3 Wires: Phase, Neutral & Earth individually & If there is a need of another wire for Dimming/Dynamic Lighting Purpose then it will add on.
- v. **SWITCHES & SOCKETS**

- a) Compliance to stringent quality norms, Dual shutter mechanism for easy & better fitment Wide & flat switch knob for easy operation. FR grade polycarbonate with high impact resistance, shock proof & UV rays stabilized.

vi. **MCBs**

- a) For the control and protection of low voltage installations against overload and short circuits.
- b) Ripping characteristic: C Curve – 5 to 10 x In
- c) Rated at 25°C to -50°C
- d) Isolation function
- e) Double entry points, separate bus bar entry, open mouthed terminal and lift clamps.

6. ITEM NO.7 PVC CONDUIT

- i. The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit 1.6 mm thick as per IS 9537/1983. ii. All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- iii. No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- iv. All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- v. Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
- vi. Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.

The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

7. ITEM NO. 8 FLOORING

- 1. **Acoustic Laminate Flooring in Control Room, Conference Room and Waiting Room:-**
Acoustic flooring (shall reduce impact sound by 14dB (ISO 717-2)). It shall be twin layer linoleum built up from 2 mm acoustic and a 2 mm Corkment backing. Flooring shall be decorative type of approved shade, pattern, texture and design and of approved manufacturer. Flooring shall be laid over concrete floor with laying compound strictly as per manufacturer's specification. The Acoustic Laminate

Flooring must be Greenguard certified.

For fixing details please refer the procedure mentioned below.

- i. Areas to receive material should be clean, fully enclosed and weather tight with the permanent HVAC in operation. A minimum temperature 68° F to be maintained during the installation, and for at least seven days following the installation.
- ii. Concrete substrates shall be structurally sound, rigid, smooth, flat, clean, and permanently dry. The concrete surface must be free of all foreign materials including, but not limited to, dust, paint, grease, oils, and solvents, curing and hardening compounds, sealers, asphalt and old adhesive residue.
- iii. Concrete substrates shall have a minimum compressive strength of 3,000 psi and a dry density of at least 150 pounds per cubic foot.
- iv. Concrete substrates on or below grade are required to have an effective moisture vapor retarder installed directly below the slab. The vapor retarder shall be puncture and tear resistant with a minimum thickness of 0.010" and a presence of 0.1 y. (Refer to ASTM E 1745.).
- v. Use material from the same batch/dye lot.
- vi. Do Not Reverse sheets for seaming.
- vii. Remove fresh adhesive residue immediately with a clean white damp cloth. Dried adhesive can be removed with a clean white cloth and mineral spirits.
- viii. When installing acoustic laminate and linoleum with jute backing on porous substrates, no open time is necessary before placing the flooring material into the adhesive.
- ix. After adhering, immediately roll the flooring in both directions using a 100-pound roller. Roll first across the width and then along the length so that any trapped air pockets will be removed.
- x. The flooring material must also remain in contact with the adhesive while the adhesive is drying and curing.
- xi. Adequate relaxing should enable the material to remain in contact with the adhesive, but if necessary, weight should be applied after rolling to ensure that the flooring material remains in full contact with the adhesive while the adhesive is drying.

Note: To ensure proper transfer of adhesive to the material backing at walls and fixtures, roll the edges of the material with a steel steam roller.

Note:- The control room interior design must be Greenguard certified.

2. False Flooring

Mandatory: Top Surface Shall be Green Guard (UL) certified to avoid VOC free / low emitting surface and finish shall be similar to the Acoustic Laminate flooring.

- i. Height above the RCC floor – 300mm to 600mm (for details please refer the plan).
- ii. The flooring should be manufactured of fiber reinforced Calcium Sulphate panels having edges finished with PVC edge band and top surface should be finished with durable & environment friendly acoustic laminate pasted with special glue serving life of 5 years' minimum. Tile Size should be 600mm X 600mm.
- iii. The panel should;
 - a Have density not less than 1650 KgM³

- b Have DIN 4102 class A1 for Heat Resistance & - BS 476 for fire resistance
 - c Core material thickness should not be less than 30mm
- iv. The acoustic laminate should be made up of twin-layer linoleum built up from 2 mm acoustic Laminate and a 1/2 mm Cork backing.
- v. The laminate should be made up of natural products and should not emit any volatile organic compounds, should be Sustainable & 100% biodegradable. Also, it should be Impact, chemical & fire resistant with anti-bacterial & anti-static properties with Colors & patterns permeate through the surface to reduce noticeable wear.
- vi. This false floor panel should rest on Edge support rigid grid system having Galvanized Iron base plate dimensions as 100mm X 100mm. The stringer should be fixed on pedestal having height adjustment of ± 25 mm.
- vii. The flooring in all the MCR area and inside rooms shall be antistatic as per spec. The test certificates to be provided before commencement of the job.

3. Granite Flooring in other areas: -

The perimeter floor of the control room and other rooms shall be done with Granite Stone. The stone shall be of approved make and shall be machine cut, machine polished (pre polished), 18mm thick which will be laid over 20mm thick bedding of cement mortar 1:4, jointed with Laticrete including rubbing, curing etc.

8. MISCELLANEOUS:

- i **Designer Privacy Film for Glass Partition and Glass Door:-** Decorative glass films for creating different environments and desired ambience. There shall be choice of multiple colors and exclusive designs.
- ii **Plastic Emulsion Paint:-** Painting to new walls with 3 coats of plastic emulsion paint of approved brand and shade after thoroughly brushing the surface to remove all dirt and remains of loose powdered materials including cost and conveyance of all materials to work site and all operational, incidental, labor charges etc. complete for finished item of work over one coat of primer total 3 coats
- iii **Wall Putty:-** Providing and applying synthetic plaster putty or equivalent putty such as Birla wall care putty of average 1 to 2 mm thick over plastered surface to prepare the surface even and smooth after thoroughly brushing the surface to remove all dirt and remains of loose powdered materials, applying emery paper, sand the surface, clean & wipe off loose dust, applying, knifing paste filler by putty knife / muslin pad, air dry for 2-3 hrs., sand with 180 and 320 no. Emery paper for the surface preparation including cost and conveyance of all materials to site, all operational, incidental, labor charges etc., complete for finished item of work for internal walls.

3.3.3. CIOC - Surveillance and video analytics

Protecting citizens and ensuring public safety is one of the topmost priorities for any Government agency. It requires advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, random acts of violence, and all other forms of crime. CCTV based video surveillance is a security enabler to ensure public safety. Government of [State], under the smart city initiative, intends to implement a holistic City Surveillance System in City Police Jurisdiction limits in the city.

MSI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of city Surveillance System of the respective phase independently.

Min Surveillance System Infrastructure at field locations (not limited to)	Supply, install, implement and maintain: • Full HD IP Pan-tilt-zoom camera (PTZ) camera • Full HS IP Bullet camera • Pole, junction box, LAN Switch, passive items, etc.
Network Infrastructure	Between camera & aggregation point – Field location
	Between aggregation points & Server Room (Central Video Data Repository)
	Between Server room & Police Department / Stations / Viewing / Monitoring Center
	Between Server room and Gandhinagar Central Monitoring Command Control Center.
Server Room	Supply & installation of IT Infrastructure including server, storage, network components and peripherals to handle 100% load of video data coming from various surveillance cameras deployed across city along with provisioning for redundancy at 5:1 Ratio
	Supply & installation of Non IT infrastructure like furniture, AC, and interior work etc. excluding civil work at the space provided by DICDL.
Command Control Center	Supply & installation of IT & Non IT infrastructure like video wall, workstation, furniture, AC, interior work, etc. excluding civil work at the space provided by DICDL
Surveillance System Applications	Video Management System (VMS)
	Video Analytics (VA)
Training / Capacity Building	Technical & functional training to the designated officials on a continuous basis

Surveillance System Infrastructure At Field Locations

This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at identified locations. Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage shall be done in consultation with the authority.

MSI shall carry out detail site survey and finalize the position of all field equipment's and the orientation / field of view of the cameras post approval of the same from authorized representative from DICDL as well as ICT Consultants. The surveyors shall also finalize the approximate location of foundation for junction box and camera poles.

System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. MSI shall prepare the detailed report for field level requirements e.g. Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of Authority. Indicative list of the field level hardware to be provided and installed by MSI is as follows:

- Cameras - Fixed Bullet, Box, Dome, PTZ Types
- Field Network Switches
- Outdoor Junction box
- Networking and power cables and other related infrastructure etc.

There will be few Fixed Indoor Dome and Panoramic Cameras to be deployed within City Integrated Operations Building, service areas and other strategic locations for general surveillance purpose.

MSI needs to design, develop and implement a server based surveillance system architecture where the required servers should be considered to comply with the requirements shared in the RFP.

The said architecture should be scalable for future enhancements where the number of cameras can be scaled up without any changes to architecture.

Supply & installation of CCTV surveillance infrastructure:

MSI shall be required to supply, install and commission the surveillance system at the identified locations and thereafter undertake necessary work towards its testing.

MSI shall use industry leading practices during the implementation phase with respect to positioning and mounting the cameras, poles and junction boxes. Some of the check-points that need to be adhered to by the MSI while installing / commissioning cameras are as follows:

- Ensure surveillance objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey
- Ensure camera is protected from the on-field challenges of weather, physical damage/vandalism and theft.
- Make proper adjustments to have the best possible image / video captured.
- Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.
- Collusion preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.
- Appropriate branding or color coding (Police/Authority Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.

Outdoor Cabinets / Junction Boxes;

- Each intersection shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP.
- MSI shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements
- The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby. Boxes shall be dustproof and impermeable to splash-water. They shall be suitable for the Dholera's environmental conditions. They shall have separate lockable doors for:
 - Power cabinet: This cabinet shall house the electricity meter, online UPS system and the redundant power supply system
 - Control cabinet: This cabinet shall house the controllers (if any) for all the field components at that particular location e.g. PTZ, Fixed cameras, etc.
 - Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
 - The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
 - Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the

entry of elements that might endanger system operation.

MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in city throughout the year.

Surveillance: Electrical Works

- MSI shall be responsible to facilitate with provisioning of electricity to the cameras through the aggregation point. Since this component has dependency on approval from local/respective authorities, it is recommended that MSI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, as applicable.
- MSI shall carry out all the electrical work required for powering all the components of the system
- Electrical installation and wiring shall conform to the electrical codes of India.
- MSI shall make provisions for providing electricity to the cameras via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup as defined in this RFP

Storage and backup (including data archiving)

MSI is expected to carry out the storage requirement estimation and supply as per the solution proposed, if the estimation is more than below specified. In addition, the proposed storage solution should be scalable to meet the sizing and the growth requirements.

MSI may supply the storage in modular manner during the implementation (i.e. initially to cater to Phase 1 requirement, then to further phases & then entire requirement).

Storage for all cameras for 24 hours (Video storage required to be stored on Centralized Primary storage for 7 days & 90 Days on Secondary Storage).

- Primary Storage capacity for 7 Days, MSI to calculate the capacity.
- Secondary Storage capacity for 90 Days
- Flagged data (critical incidents) will be stored for minimum 365 days, permanent storage envisaged on Backup device.
- It shall allow online expansion and retirement of storage capacity and disk array swap-outs without taking it off line. This includes adding addition disks to existing storage arrays, adding incremental or new storage arrays, and/or the removal of older arrays in replacement of new storage subsystems regardless of capacity, Make & Model.

Storage feeds-

- Viewing at 25 FPS
- Storage Frames - 18 FPS during day/movement period
- Specific data as notified by the department will be stored for long term records

The list of functional requirements for surveillance and video analytics are mentioned as below; (but not limited to)

Functional, Technical and Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DS-1.0	CCTV & Security Surveillance systems	Server	Database/Management Server	Database/Management server manages all information handled by the VMS system, including Recorders Management, Decoders management and event triggers, User management
CIO-RS-1.0	CCTV & Security Surveillance systems	Server	Recorder Server	Multimedia capture server that responsible for managing edge devices and archive and stream multimedia.
CIO-APP-1.0	CCTV & Security Surveillance systems	Applications	DICDLs Applications	The Client system must provide remote users with rich functionality and features as described below. Quickly searching selected areas of video recording for motion (also known as Smart Search). This application shall support minimum 15 client workstations and scalable further for viewing and managing events. All clients continuously receive updates from the server. Similarly, all permissions and notifications are also managed by the server.
CIO-HA-1.0	CCTV & Security Surveillance systems	HA	High Availability /Failover	Failover of data center/server room must be considered in such a way that there shall not be any loss of data. Primary failover is considered with in the server room, and in any case if server room fails the backup solution and backup should be used to get the system up and running at the earliest.
CIO-VA-1.0	CCTV & Security Surveillance systems	Analytics	Video Analytic	Video Analytics is a generic term that describes computerized processing of video streams. The term Video Analytics is typically associated with surveillance system video streams and the tasks it can perform range from immediate detection of events to analyzing video to extract data and events.
CIO-VA-1.1	CCTV & Security Surveillance systems	Analytics	Video Analytic	Video analytics must help taking proactive action, which helps police department to take fast decisions.
CIO-VA-1.2	CCTV & Security Surveillance systems	Analytics	Video Analytic	Video analytics services will be working with video management software, the VA services are working as a back-end service. Video analytics application service work tightly with VMS for video data processing the Video analytics rules can be considered either Server base or Edge base depending on final solution considered by MSI.
CIO-VA-1.3	CCTV & Security Surveillance systems	Analytics	Video Analytic	The baggage detection application is based on background model and a tracking technology. According to this approach, a Background Model (BM) describes the scene when it is empty (without foreground pixels). The background model is learned and maintained online. In each frame, the deviation of the current frame from the BM is measured. This deviation is then sent to the tracker, which is a higher-level process that searches and tracks foreground objects.
CIO-VA-1.4	CCTV & Security Surveillance systems	Analytics	Video Analytic	The baggage must be visible at a minimum contrast of 20% of the dynamic range of the image. For example, when we assume 256 gray levels, the contrast between the baggage and the background should be at least 50 gray levels.
CIO-VA-1.5	CCTV & Security Surveillance systems	Analytics	Video Analytic	Minimum baggage area in CIF resolution should be 40 pixels.
CIO-VA-1.6	CCTV & Security Surveillance systems	Analytics	Video Analytic	Once the baggage has been located in unauthorized location, the baggage cannot be occluded by other objects. For optimal performance, the camera must maintain line of sight with the baggage and the area beside the baggage should be illuminated in a constant level.
CIO-VA-1.7	CCTV & Security Surveillance systems	Analytics	Video Analytic	The time until a baggage will generate an alert is recommended not to be shorter than 1 minute.
CIO-VA-1.8	CCTV & Security Surveillance systems	Analytics	Video Analytic	As the algorithm is based on a background model, abrupt illumination transitions can create dummy objects that might reduce detection rate and increase false alarm rate.
CIO-VA-1.9	CCTV & Security Surveillance systems	Analytics	Video Analytic	Any other static object that is similar in size to a typical baggage can generate an alert.
CIO-VA-1.10	CCTV & Security Surveillance systems	Analytics	Video Analytic	The Intrusion detection application is based on a background model and a tracking technology. According to this approach, a background model (BM) describes the scene when it is empty (without foreground pixels). The background model is learned and maintained online. In each frame, the deviation of the current frame from the BM is measured. This deviation is analyzed the

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				tracker, which is a higher-level process that searches and tracks foreground objects.
CIO- VA- 1.11	CCTV & Security Surveillance systems	Analytics	Video Analytic	The application must detect and track multiple objects.
CIO- VA- 1.12	CCTV & Security Surveillance systems	Analytics	Video Analytic	The object must be continuously visible in order to maintain its identity.
CIO- VA- 1.13	CCTV & Security Surveillance systems	Analytics	Video Analytic	An occlusion of the object (e.g. by other objects, walls etc.) may result in the object losing its' history information.
CIO- VA- 1.14	CCTV & Security Surveillance systems	Analytics	Video Analytic	The intrusion detection application can track objects at both outdoor and indoor scenarios.
CIO- VA- 1.15	CCTV & Security Surveillance systems	Analytics	Video Analytic	For outdoor or semi-outdoor scenarios, the camera must be of a Wide dynamic range type.
CIO- VA- 1.16	CCTV & Security Surveillance systems	Analytics	Video Analytic	The detected object must be visible at a minimum contrast of 20% of the dynamic range of the image. For example, when assuming 256 gray levels, the contrast between the object and the background should be at least 50 gray levels.
CIO- VA- 1.17	CCTV & Security Surveillance systems	Analytics	Video Analytic	Consider a CIF input stream and a human target, the minimum object size that will be detected is 30 pixels.
CIO- VA- 1.18	CCTV & Security Surveillance systems	Analytics	Video Analytic	As the algorithm is based on a background model, abrupt illumination transitions can create dummy objects that might reduce detection rate and increase false alarm rate.
CIO- VA- 1.19	CCTV & Security Surveillance systems	Analytics	Video Analytic	Low video quality that results from weather conditions (fog, etc.) or poor illumination during night time will result in unstable tracking and reduce detection.
CIO- VA- 1.20	CCTV & Security Surveillance systems	Analytics	Video Analytic	The overcrowding application monitors the crowd level (percentage of area occupied) in a specified area of interest (AOI). Alerts will be generated according to rules that were defined by the user. For example: generate an alert whenever the overcrowding level is higher than 80% during 5 minutes.
CIO- VA- 1.21	CCTV & Security Surveillance systems	Analytics	Video Analytic	Accurate results are best achieved when the camera has a top view of the AOI. When objects become small as they are getting far from the camera (the scene has perspective), people may hide each other. Occlusions results in lower overcrowd estimation accuracy.
CIO- VA- 1.22	CCTV & Security Surveillance systems	Analytics	Video Analytic	Foreground area must be visible at a minimum contrast of 20% of the dynamic range of the image. For example, when assuming 256 gray levels, the contrast between the object and the background should be at least 50 gray levels.
CIO- VA- 1.23	CCTV & Security Surveillance systems	Analytics	Video Analytic	In a top view installation, the minimum object area (in pixels) in CIF resolutions should be around 20 pixels. Maximum object size must not exceed 80 pixels.
CIO- VA- 1.24	CCTV & Security Surveillance systems	Analytics	Video Analytic	Stationary objects (static for approximately more than 5 seconds) might eventually be considered as part of the background. Therefore, the accuracy might decrease when the crowd is static.
CIO- VA- 1.25	CCTV & Security Surveillance systems	Analytics	Video Analytic	Baggage or moving foreground objects are counted as foreground areas.
CIO- VA- 1.26	CCTV & Security Surveillance systems	Analytics	Video Analytic	Poor illumination will result in unstable and low accuracy of the crowd occupancy (especially when handling relatively dark foreground figures). For nighttime dark scenarios, it is highly recommended to equip with an appropriate light source.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO- VA-1.27	CCTV & Security Surveillance systems	Analytics	Video Analytic	Car Traffic Events (Start/Stop/Illegal parking/wrong direction/Speed)
CIO- VA-1.28	CCTV & Security Surveillance systems	Analytics	Video Analytic	System must configure to detect Illegal parking in a sterile zone, Wrong direction.
CIO- VA-1.29	CCTV & Security Surveillance systems	Analytics	Video Analytic	The solution must offer a suite of analytics rules to provide automatic detection of a range of motion and non-motion behavior of persons, objects and vehicles: Analytics Applications - Crowd & Traffic Monitoring o Unlawful gathering/crowd formation o Vehicle Moving Wrong Way o No Parking o Broad Object Classification o Object Speed - Camera Tampering Suite o Camera Moved/tempered o Camera Defocused, Blocked or Covered
CIO- VA-1.30	CCTV & Security Surveillance systems	Analytics	Video Analytic	Detects any event that significantly changes the field of view of the camera, such as the camera being panned away from a known view.
CIO- VA-1.31	CCTV & Security Surveillance systems	Analytics	Video Analytic	The Virtual Fence/Tripwire detection is based on a background model and a tracking technology. According to this approach, a background model (BM) describes the scene when it is empty (without foreground pixels).
CIO- VA-1.32	CCTV & Security Surveillance systems	Analytics	Video Analytic	The background model is learned and maintained online. In each frame, the deviation of the current frame from the BM is measured. This deviation is analyzed the tracker, which is a higher-level process that searches and tracks foreground objects.
CIO- S-1.0	CCTV & Security Surveillance systems	Storage	Storage	The storage solution proposed is that the video feeds must be available for 7 days as primary storage and 90 days on secondary storage. After 90 days, the video feeds would be overwritten unless it is flagged or marked by the Police for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police deem it good for deletion.
CIO- VMS-1.0	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Openness	VMS must be open to any ONVIF compliant IP and Analog CCTV cameras integration.
CIO- VMS-1.1	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Openness	In that respect, VMS must already support IP cameras from various major vendors.. As such, it is mandatory for VMS to have ONVIF Profile S & G compliance.
CIO- VMS-1.2	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Openness	VMS must be open to any standard storage technologies integration. It should support Local HDD, DAS, and Network Storages (NAS, SAN)
CIO- VMS-1.3	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Openness	VMS shall be open to any video wall system integration.
CIO- VMS-1.4	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Openness	VMS should support Remote access for Live viewing and Archive search using any standard Browsers, e.g., Mozilla Firefox, Chrome, Internet Explorer, Safari, etc.
CIO- VMS-1.5	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Openness	VMS must have Open Interface to send Analytics event alerts and other Maintenance alerts (Camera disconnection, Storage Full, DBMS disconnection, etc.) over HTTP protocol to any external application running in a different machine in the same LAN. This is required for integration with command & control software or any other 3rd party incident management system.
CIO- VMS-1.6	CCTV & Security	Network Video Management	VMS Architecture	VMS must be designed to offer a full IP based centralized architecture.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
	Surveillance systems	Software (NVMS)		
CIO-VMS-1.7	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Architecture	VMS must have the capability to support multiple client (operators) from different physical locations spread geographically apart, and connected through WAN/MAN connectivity.
CIO-VMS-1.8	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Architecture	VMS must have scalable architecture, without problem with running system.
CIO-VMS-1.9	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Architecture	It must support virtual environment.
CIO-VMS-1.10	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	VMS must allow managing initial client logon, system configurations, logging, remote administration of recording servers, devices, security, rules, alerts and logging.
CIO-VMS-1.11	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	VMS must support 3 or more levels of users with various privileges to access the system functionality. Each category of users shall have selectable rights to perform various operations like Camera add/delete, Change camera settings, Configure storage, Control PTZ cameras, User management, etc.
CIO-VMS-1.12	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	The System health status like Server failure, Camera disconnection, Storage full, etc. should always be displayed at the Client UI.
CIO-VMS-1.13	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	VMS must maintain a continuous log of server status messages, Camera connectivity, Storage status, Recording ON/OFF, User activity logs , etc. which shall be accessed from the Workstations using different filters.
CIO-VMS-1.14	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	VMS must be able to detect IP camera devices hooked in employer network automatically.
CIO-VMS-1.15	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	VMS must store all configuration data of Servers, Analytics application settings, Camera recording Schedules, User login credentials, Archived video files etc. in a single Database.
CIO-VMS-1.16	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Management	VMS must support multi-layer hyperlinked maps (open source digital/ google map or any other maps). Cameras can be dragged and dropped from directory on the map for click-n-view on Client viewer. The system should be able to plot the camera location on the city map (open source digital/Google Map or the maps provided by employer)
CIO-VMS-1.17	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Failover Support	The system must support automatic failover for recording servers. The allocation of Cameras to recording servers shall be done automatically by the VMS. On failure or any particular Recording server, the cameras associated with the failed server should be automatically run on active servers without any human intervention. When the failed server becomes active, the cameras will be automatically allocated to the server again without any human intervention. The system design should support N+0, N+1 and N+N configuration for such failover.
CIO-VMS-1.18	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Failover Support	Once configured, the Video Management System must not require reconfiguration of any kind when any server passes through a power Off-On cycle.
CIO-VMS-1.19	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Failover Support	The system must provide seamless access to recordings on the failover server for all clients through the same client views once the services are fully started.
CIO-VMS-1.20	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Failover Support	The VMS server must have capacity to fail over and failback of database/management server, recordings shall not be stop when data base/management server is down or database disconnection.
CIO-VMS-1.21	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must be able to operate in multicast & unicast protocol to minimize the network bandwidth

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-VMS-1.22	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must have the capability of managing the camera throughput on per camera basis.
CIO-VMS-1.23	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must support H.265, H.264 and MJPEG stream for both live view and Recording independently. Compression rate shall be manageable
CIO-VMS-1.24	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must manage, display and record min 2 or multiple video streams from a single IP camera.
CIO-VMS-1.25	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	Each video streams must be individually and independently configurable in term of resolution, frames and bandwidth
CIO-VMS-1.26	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must support video streams up to at least 50/60fps per camera.
CIO-VMS-1.27	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must support at least CIF, 2CIF, 4CIF/D1 and HD/Megapixel resolution
CIO-VMS-1.28	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	VMS must include automatic camera discovery function and intuitive configuration wizards
CIO-VMS-1.29	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	While in Unicast streaming, the VMS must support flow control independently for each client.
CIO-VMS-1.30	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	The VMS must be able to stream standard H.264, H.265, Mpeg4 camera video streams to any external software on demand basis.
CIO-VMS-1.31	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	SNMP Support: - The system must support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system.
CIO-VMS-1.32	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Multicasting and Multi-streaming	a)To ensure security and ease of Firewall deployment, only one Server must be allowed to be exposed to Internet for delivering services to all the remote clients sitting on the Internet. The remote clients shall access only that server to access the system for all the functionality. b) The VMS should provide viewing capabilities by browsing, supporting laptops, smartphones and tablets for remote viewing without any installation on the viewing device.
CIO-VMS-1.33	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Health monitoring	Detailed listing of all active or incoming alarms with available filters for time period, alarm source, operator and alarm state. - Ability to preview, view live or playback recorded images. - Automatically close an alarm based on a corresponding event. - Generate audit trail reports by incident.
CIO-VMS-1.34	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Cameras:-	VMS must be open standard and must be able to support multiple brand of camera. VMS shall be open to do any customization in order to integrate any make of IP camera.
CIO-VMS-1.35	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Cameras:-	VMS must allow camera clustering based on Locations as well as Groups independently.
CIO-VMS-1.36	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Cameras:-	Each operator must be able to monitor one or several camera

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-VMS-1.37	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Cameras:-	It shall be able to prevent an operator from viewing/managing one or many camera. At any given time it shall be possible to block sensitive video from being viewed by some non-authorized users
CIO-VMS-1.38	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Cameras:-	Following typical camera parameters shall be manageable: - Brightness, compression, contrast, include date and time, resolution, rotation - Frame per second, bit rate control mode, maximum bit rate, bit rate control priority, target bit rate - Camera's Name, Description, Hardware name and Part number - Storage and recording settings, maximum storage limits and database configuration. The total hard drive space used to store the camera's recorded data shall be displayed.
CIO-VMS-1.39	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Cameras:-	Archiving settings - Pre-set positions (if the selected camera is a PTZ camera) - Patrolling profiles (if the selected camera is a PTZ camera) - Hardware configurable events
CIO-VMS-1.40	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Logs	The system log must be searchable by Level, Source and Event Type.
CIO-VMS-1.41	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Logs	The Audit Log records remote user activity (searchable by User name, Audit ID, Source and Location)
CIO-VMS-1.42	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Logs	The Event Log records event-related information (searchable by Service name, Source and Event type)
CIO-VMS-1.43	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	VMS must provide feature-rich administration client for system configuration and day-to-day administration of the system
CIO-VMS-1.44	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must provide a Graphical User Interface (GUI) for the convenient access of live and recorded video as well as camera properties and display quality
CIO-VMS-1.45	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must support real time simultaneously view of 1, 2x2, 3x3, 4x4, , or customized view plan.
CIO-VMS-1.46	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	It must be possible to drag and drop cameras from the camera directory to the display screen.
CIO-VMS-1.47	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must offer the capability of browsing recordings from cameras on the same panel where other cameras are displayed live. There shall be provision to replay multiple such cameras from various timestamps, independent to one another.
CIO-VMS-1.48	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client viewer must have the feature to synchronize replay of selected cameras/all cameras in the view panel.
CIO-VMS-1.49	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	VMS must select the appropriate video stream from camera for display depending on the display resolution to optimize the network bandwidth.
CIO-VMS-1.50	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	Digital zooming must be possible both on live view as well as on Replay view on Fixed as well as PTZ Cameras.
CIO-VMS-1.51	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must support the use of standard PTZ controller or 3-axis USB joysticks for control of pan, tilt, zoom and auxiliary camera functions.
CIO-VMS-1.52	CCTV & Security	Network Video Management	VMS Client Viewer	The Client Viewer must support the use of keyboard shortcuts for control of standard features.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
	Surveillance systems	Software (NVMS)	(Operator) features	
CIO-VMS-1.53	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must have the following two-way audio functions: - The Client Viewer must allow an operator to play live audio from a camera's microphone and play back recorded audio. - The Client Viewer must allow an operator to export audio together with video in the AVI format.
CIO-VMS-1.54	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	From the Client Viewer it must be possible to - Run instant replay of any camera on display - Bookmark of any important event to facilitate search and retrieval - Bookmark the display layout with selected distribution of cameras across the panel - Activate manually triggered events. - Use sound notifications for attracting attention to detected motion or events. - Get quick overview of sequences with detected motion. - Get quick overviews of detected alerts or events. - Quickly search selected areas of video recording for motion - Skip gaps during playback of recordings. - Configure and use several different joysticks. - Print images, with optional comments. - Copy images for subsequent pasting into word processors, email, etc. - Export recording (e.g. for use as evidence) in AVI or JPEG formats
CIO-VMS-1.55	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must have the capability to receive multicast streams if a present number of clients are requesting the same live view camera. The Operator shall have the option to configure the system to always receive unicast streams at the discretion of the system administrator. .
CIO-VMS-1.56	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The operator must have the ability to use digital zoom where the zooming is performed in the image & video on any number of cameras simultaneously. This functionality shall be the default for fixed cameras. The use of digital zoom shall not affect recording or other users.
CIO-VMS-1.57	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Client Viewer (Operator) features	The Client Viewer must integrate the following viewing capabilities: - Matrix Switching: The Client viewer must allow switching amongst multiple selected bookmarked display layouts with pre-determined time duration for each matrix view. - Matrix Window – A window that is used to display cameras on demand or by an external event - Client viewer must allow the same camera to be viewed on multiple display tiles; one may be digitally zoomed, or on high resolution stream. - An overview image in the view must display the normal field-of-view and the digital zoom area in a highlighted box to provide the user with spatial awareness. - The PTZ control window must allow the user to select pre-defined presets for PTZ cameras and drive the selected camera to the preset. - The current camera state must be displayed and shall indicate whether the camera is in live mode, in recording mode or in stopped mode. - The Client Viewer must display Alerts defined as bookmarked events. - The Client Viewer must display a time line for each camera to represent recorded video sequences. The time line band shall be highlighted based on the camera view selected in the display. The Client Viewer shall allow video sequences for the displayed cameras to be reviewed simultaneously. - The Client Viewer must allow an area of interest in an image to be searched for motion by time. - The Client Viewer must allow a surveillance report to be printed from the image with specific information including the camera name, capture time, print time, user and user notes. The surveillance report shall be printed to any network connected printer. - The Client Viewer must allow the start and stop time and camera source for the export to be set and provide two format options for exporting video clips. - AVI/JPEG format – VMS must provide options for export format type (AVI/JPEG), timestamp, frame rate (full/half), digital zoom export, and AVI CODEC. Video clip may be exported to desktop/CD/DVD/flash drive or a specific file path. All audio associated with the video being exported shall automatically be included in the AVI export. - Watermarking & Encryption – VMS must watermark each and every frame of the Video files with Watermarks to authenticate the source of the video. While exporting video segments to external media (CD/DVD/flash drive) or to any

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				folder in workstations, the VMS shall allow encryption of the video files with at least 256-bit encryption technique. - The Client Viewer must allow the digital zoom feature to be used in recordings. - VMS must allow seamless integration into an external Geographical Information System - From the GIS console Operators must get an overview of the system and access to all system components. - Map function can use standard graphical file formats including jpg, gif, png, tif, etc. - The Map should be a part of the Client viewer application and VMS must allow detaching the map and showing it separately on another monitor connected to the Client viewer machine (in case of Multi-monitor workstation). - System performance data for cameras and servers including camera resolution, FPS, network usage, disk space, etc.
CIO-VMS-1.58	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	VMS must comply with any conventional storage technologies (IDE, SCSI, RAID, SAN, CAS, NAS, etc.) to accommodate future potential expansion.
CIO-VMS-1.59	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	VMS must be able to use server installed HDD as well as NAS/SAN in the same system for recording purpose.
CIO-VMS-1.60	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	It must be possible to create Recording Schedules on the fly, and assign any schedule to any camera, any group of camera or to all the cameras any time. The recording shall be controlled on need basis. It shall be possible to manage recording on per camera basis, each with different video settings (format, frame rate and resolution).
CIO-VMS-1.61	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	VMS must allow users to mark any specific segment of the video as Critical video segment, so that those particular segments of video do not get deleted on the default scheme (FIFO, Retention period, etc.).
CIO-VMS-1.62	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	Archive retention period must be configurable on per camera basis. The system shall allow both retention based as well as file based deletion policy.
CIO-VMS-1.63	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	Because of the large quantity of cameras and their locations, it is foreseen that numerous alarms and alerts could be triggered off. Appropriate and accurate VCA selection shall help decreasing those errors hence ease the operator's mission.
CIO-VMS-1.64	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	VMS must be delivered along with a set of Video Content Analytics features
CIO-VMS-1.65	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	Video Content Analytics systems should be native to the VMS.
CIO-VMS-1.66	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	NVMS, Video Analytics and Video summarization system should be preferable from the same manufacture, if not MSI to ensure seamless integration between systems.
CIO-VMS-1.67	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	The VMS and VCA must have tight integration, so that there is no need to add cameras to VMS and VCA servers separately.
CIO-VMS-1.68	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	Multiple video analytics rules should run on a single camera.
CIO-VMS-1.69	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VMS Storage	VCA shall handle analytics both at the edge (in the camera) and at the server.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-VMS-1.70	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VCA Architecture	The propose VCA can be server based or camera based.
CIO-VMS-1.71	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VCA Architecture	The system must support multiple Video Content Analytics servers running on different machines.
CIO-VMS-1.72	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VCA Architecture	Once one or more VCA server fails, the other servers should share the load of the failed server(s) to provide a failover support for VCA applications.
CIO-VMS-1.73	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VCA Architecture	The solution must run on computer networks using industry-standard equipment.
CIO-VMS-1.74	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	VCA Architecture	The analytics software must be compatible with common Latest generation operating systems such as Linux, Microsoft Windows server, Windows, Mac OS, Unix, etc.
CIO-VMS-1.75	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Event Generation and Receipt	The solution must provide real-time generation of events to alert operators.
CIO-VMS-1.76	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Event Generation and Receipt	The VMS must show the Event messages on detection of Analytics events on the same Client live view panel instantly. On clicking on the message, relevant snap of the scene should appear on screen.
CIO-VMS-1.77	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Rules Capabilities	The solution must enable any combination of analytics rules to run on the same camera simultaneously, without limitations.
CIO-VMS-1.78	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Rules Capabilities	The solution must enable the operator to define minimum 3 or more number of detection regions per camera.
CIO-VMS-1.79	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Viewing Search Results Capabilities	The solution must provide a fundamental capability to display video playback for any search result around the time that the search target / behavior was found
CIO-VMS-1.80	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Viewing Search Results Capabilities	The solution must continuously display a bounding box over the target (target tracking)
CIO-VMS-1.81	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Viewing Search Results Capabilities	The solution must display the video playback related to alarm.
CIO-VMS-1.82	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Viewing Search Results Capabilities	The solution must present a progress bar, including a graphic indication showing the time at which the search criteria were met
CIO-VMS-1.83	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Viewing Search Results Capabilities	The solution must enable the user to Pause and Re-Play the video playback
CIO-VMS-1.84	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Viewing Search Results Capabilities	Event lists: After searching cameras for a particular Event, the solution must be capable of displaying list of all the events in a tabular form. On clicking any entry in the table, a snap with the event detail shall be displayed. It shall be possible to play back the video of each event simply by a single click of mouse.
CIO-VMS-1.85	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Investigation and Forensic Analysis	The solution must provide the following process and investigation capabilities:
CIO-VMS-1.86	CCTV & Security	Network Video Management	Investigation and	Bookmarking: The solution must allow the user to bookmark any Event clip for ready reference at any later point of time.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
	Surveillance systems	Software (NVMS)	Forensic Analysis	
CIO-VMS-1.87	CCTV & Security Surveillance systems	Network Video Management Software (NVMS)	Investigation and Forensic Analysis	Critical event Tagging: The solution must allow the user to tag critical Event clips so that they do not get removed from the storage based on FIFO/Retention period settings.

3.3.4. CIOC - AV Hardware & Software

The following usage scenarios will be available in all rooms and areas to greater or lesser degree depending on room type and function:

- Display of content to room occupants, sources to be both within the room (local PC applications, user laptop or BYOD) and from information / data available on the network
- Participation in audio conferencing sessions, using the installed sound system from individual to group calls
- Participation in audio conferencing sessions with data sharing using Communication Soft client.
- Participation in video conferencing sessions and data sharing to all participants (local / remote)
- Annotation to PC content available to local personnel and during conferencing sessions (shared)
- Digital signage for display of visual management data / corporate branding.

Functional and Technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-AV 1.1	CIO	EUC / Meeting	Audio / Video	User can make an audio call to one or more internal party
CIO-AV 1.2	CIO	EUC / Meeting	Audio / Video	User can make an audio call to one or more external party
CIO-AV 1.3	CIO	EUC / Meeting	Audio / Video	Users can control outgoing and local audio and video
CIO-AV 1.4	CIO	EUC / Meeting	Audio / Video	Users can conduct a video or audio conference through Video Conferencing unit.
CIO-AV 1.5	CIO	EUC / Meeting	Audio / Video	Users are able to share content locally securely
CIO-AV 1.6	CIO	EUC / Meeting	Audio / Video	Users can record presence camera feeds
CIO-AV 1.7	CIO	EUC / Meeting	Audio / Video	Users can record Visual Management feeds
CIO-AV 1.8	CIO	EUC / Meeting	Audio / Video	Users can share their laptop content (video and audio)
CIO-AV 1.9	CIO	EUC / Meeting	Audio / Video	Users and Guests can share their laptop content and BYO device content (video and audio)
CIO-AV 1.10	CIO	EUC / Meeting	Audio / Video	There will be a rack mounted video-conferencing codec 1080p with H265 support
CIO-AV 1.11	CIO	EUC / Meeting	Audio / Video	A video conferencing camera system will be 4K resolution with auto tracking
CIO-AV 1.12	CIO	EUC / Meeting	Audio / Video	A built-in microphone array for speaker tracking and camera switching
CIO-AV 1.13	CIO	EUC / Meeting	Audio / Video	The audio system will have built in AEC, AGC & NR capabilities

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-AV 1.14	CIO	EUC / Meeting	Audio / Video	Table mounted microphone system
CIO-AV 1.15	CIO	EUC / Meeting	Audio / Video	There will be two ceiling mounted microphone systems.
CIO-AV 1.16	CIO	EUC / Meeting	Audio / Video	There will be ceiling mounted speakers driven by a networked ceiling mounted amplifier.
CIO-AV 1.17	CIO	EUC / Meeting	Audio / Video	There will be a ceiling mounted document camera
CIO-AV 1.18	CIO	EUC / Meeting	Audio / Video	The audio visual room system will be controlled by a desk mounted touch panel
CIO-AV 1.19	CIO	EUC / Meeting	Audio / Video	A built-in microphone array for speaker tracking auto camera switching
CIO-AV 1.20	CIO	EUC / Meeting	Annotate	Users can annotate shared content
CIO-AV 1.21	CIO	EUC / Meeting	Annotate	Users can annotate far end content
CIO-AV 1.22	CIO	EUC / Meeting	Annotate	Users can allow far end annotation of their content
CIO-AV 1.23	CIO	EUC / Meeting	Annotate	Users can annotate on a shared interactive display
CIO-AV 1.24	CIO	EUC / Meeting	meeting room	Users can record a meeting

Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR-AV 1.1	AV Control Software	Non Functional requirement	Availability	AV control is required citywide. Admin access should be from any location with an AV device and any point on the AV VLAN (WAN/LAN)
NFR-AV 1.2	AV and General Meeting Hardware / Firmware	Non Functional requirement	Availability	Hardware duty cycle: 12/365 (h/d)
NFR-AV 1.3	AV Hardware / Firmware	Non Functional requirement	Availability	Hardware will be physically located in IOC areas, meeting rooms and general areas, communication rooms and hosting infrastructure at Server room. Login access to networked equipment will be available on the VLANs as part of the LAN/WAN
NFR-AV 1.4	AV and General Meeting Hardware / Firmware	Non Functional requirement	Availability	Planned maintenance must be carried out to minimize periods of unavailability i.e. out of office hours. General AV and meeting rooms are not mission critical and multiples of each room type exist as redundancy. Planned maintenance must be carried out on parts of the systems, without effecting the whole system i.e. LED walls can be maintained in part while maintaining display. Maintenance must be carried out during non-peak times
NFR-AV 1.5	AV Control Software	Non Functional requirement	Availability	Software duty cycle: 24/365 (h/d)
NFR-AV 2.0	AV Control Software	Non Functional requirement	Documentation	Full documentation is required to be handed over. This includes specification of every application used, its maintenance, its revision version and IP address table(s). Operations and Maintenance manual must be provided including back-up frequency, updates calendar (where known), original installation files and license keys. Configuration data book is required for all application and configuration of software, back-up and recovery data must be provided.
NFR-AV 2.1	AV Hardware / Firmware	Non Functional requirement	Documentation	Full documentation is required to be handed over. This includes specification of every device used, its maintenance, its firmware version and IP address table. Operations and Maintenance manual must be provided including asset tag register with serial numbers, cabling schematics with cable numbers and types, schedule of

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
				maintenance intervals, and actual power and heat loading figures. Physical arrangements in plan and elevation showing the location of every device, in floors, wall mounted, under desks, and ceiling mounted. Rack cabling diagrams and loading drawings must be provided. Configuration data book is required for all devices and configuration of software, back-up and recovery data must be provided.
NFR-AV 2.2	AV Control Software	Non Functional requirement	Documentation	In addition to knowledge base, manufacturers operations manuals must be provided
NFR-AV 2.3	AV Hardware / Firmware	Non Functional requirement	Documentation	In addition to user guides and quick start manuals, manufacturers' operations manuals must be provided. Train the trainer materials will be required
NFR-AV 3.1	AV and General Meeting Hardware / Firmware	Non Functional requirement	Reliability	24 hours break fix, or better
NFR-AV 3.2	AV Control Software	Non Functional requirement	Reliability	AV control software must be fully redundant to enable 99.74% availability. AV control impacts IOCs, which are mission critical
NFR-AV 3.3	AV Hardware / Firmware	Non Functional requirement	Reliability	IOC systems must be designed to be high availability 24/365 (h/d), and have field replaceable units to minimize the fault to fix time. The systems must have redundancy built in to ensure they remain operable at all times. A total failure of the systems is unacceptable in any case except for the entire CIOC being compromised.
NFR-AV 3.4	AV Control Software	Non Functional requirement	Reliability	Maximum 1 hour for break fix during operational times, for partial loss of availability in general AV rooms. Fastest possible break fix time for IOCs, alternative control must be available.
NFR-AV 3.5	AV Hardware / Firmware	Non Functional requirement	Reliability	Maximum 4 hours for break fix during operational times, for partial loss of availability.
NFR-AV 3.6	AV and General Meeting Hardware / Firmware	Non Functional requirement	Reliability	Systems must be designed to be reliable and should have field replaceable units to minimize the fault to fix time. Redundancy is provided by multiple rooms of each specification.
NFR-AV 4.1	AV and General Meeting Hardware / Firmware	Non Functional requirement	Security	Access permissions for application data may only be changed by the system's data administrator
NFR-AV 4.2	AV Hardware / Firmware	Non Functional requirement	Security	128-bit AES encryption or HDCP 2.0 is required on all data passed between devices
NFR-AV 4.3	AV Control Software	Non Functional requirement	Security	Access permissions changed by administrators on instruction of applications owner(s) / the system's data administrator
NFR-AV 4.4	AV Control Software	Non Functional requirement	Security	Administrator: Full admin access to all components and functionality. Programmer / Debugger: access to create new control code and run diagnostics, access to reprogram faulty code and to add new hardware to be controlled in to program. Access to run reports and export data. User: access to operate control system in each area where control is deployed, no change or reporting rights of any kind.
NFR-AV 4.5	AV Control Software	Non Functional requirement	Security	AV control logging must be backed up every 24 hrs. System configuration must be backed up before and after every configuration change. All backups to be stored securely as per IT / Data security policy
NFR-AV 4.6	AV Hardware / Firmware	Non Functional requirement	Security	Copies of Firmware updates and device configuration must be recorded at each update / change and stored in knowledge management database. Central IP config data book required for all non-DHCP devices. IP address range / VLAN / MAC Address must be recorded for all devices
NFR-AV 4.7	AV Hardware / Firmware	Non Functional requirement	Security	Device passwords must be eight characters long and contain only numerals and letters (upper and lower case). Passwords must be unique to each device. No user passwords required.
NFR-AV 4.8	AV Control Software	Non Functional requirement	Security	If passwords are not managed through active directory - User Passwords must be eight characters long and contain numerals, special characters and letters (upper and lower case). Passwords must be unique to each user. Admin passwords must be unique to each administrator. All passwords must be changed every 90 days.
NFR-AV 4.9	AV Control Software	Non Functional requirement	Security	Must comply with enterprise-wide IT application security.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR-AV 4.10	AV Hardware / Firmware	Non Functional requirement	Security	Password timeouts will be dependent on each device and pre-set by hardware manufacturer. No audit for hardware login required.
NFR-AV 4.11	AV Control Software	Non Functional requirement	Security	Required levels, Administrator, Programmer / Debugger, and User
NFR-AV 4.12	AV Hardware / Firmware	Non Functional requirement	Security	Two user levels are required: User - this requires no user credentials for user operation of systems, Admin - password protected access for firmware revisions, configuration updates or Program updates
NFR-AVS 5.1	AV Control Software	Non Functional requirement	Usability	Control platform must support multi-lingual content with different character sets - language must be user selectable on every control page at time of operation
NFR-AVS 5.2	AV Control Software	Non Functional requirement	Usability	Control platform, must be available in multiple languages, must support accessibility features such as high or low contrast graphics, be color-blindness aware, and have a big type version. Audible and voice command are not required.
NFR-AV 6.1	AV Control Software	Non Functional requirement	Audit	All user and admin interactions are required to be logged for audit
NFR-AV 6.2	AV Control Software	Non Functional requirement	Audit	Audit trail for user interactions, which room, what time, which function requested, number of button presses.
NFR-AV 6.3	AV Control Software	Non Functional requirement	Audit	Control platform should be segregated from other systems as much as possible
NFR-AV 6.4	AV Control Software	Non Functional requirement	Audit	Storage capacity should be adequate for logging, reports and audit data.

3.3.5. CIOC - Collaboration Solution for Helpdesk

Collaboration Solution would include Video conferencing, IP Telephony and Helpdesk solution for utilities. The whole collaboration solution for DSIR is divided into 3 sections:

- Video conferencing
- IP telephony
- Help desk

Core infrastructure

IP telephony refers to the technology for transmitting voice communications over a network using IP standards. This leads to creating a single, converged network - that can handle data, voice and video traffic simultaneously, while maintaining a high level of availability, QoS and Security for your network. IP telephony solution delivers high-quality IP voice and fully integrated communications by allowing the transmission of voice, video and data over a single network infrastructure.

Leveraging the framework provided in WAN, IP telephony solutions deliver unparalleled performance and capabilities to address current and emerging communications needs in the enterprise environment. IP telephony solutions are designed to optimize feature functionality, reduce configuration and maintenance requirements, and provide interoperability with a wide variety of applications.

Helpdesk Solution for Utility

The proposed Video conference, IP Telephony and Helpdesk solution for a utility help desk gets integrated for a seamless communication. The contact center solution can reside on the recommended redundant IPPBX for inbound, outbound calls, Email, Chat, redundant compliance voice recording and screen recording, Self Service IVR, integration with CRM and external Database and blended agents for inbound and outbound calls, Agent desktop, Integration with 3rd party gadgets, integration with knowledge base and Web based reporting.

IP Telephony:

IP telephony solution is required at various floors in the building. The following is recommended:

- 1:1 Redundant Centralized call managers in the building in server room
- 1:1 Redundant centralized 4 PRI ISDN Gateway in server room
- Voice Gateways to connect analog PTT Phones
- PoE IP Phones distributed across the building across different floors for the various users
- Solution for soft clients for multiple users

VC Soft Clients

- The solution helps the guest users such as prospective employees of various utilities to join a video call without having to install any client software/app on their windows/Mac PC or laptop. Guests simply click a URL, website link, or mobile application to start the interaction.
- The solution delivers HD720p resolution on the desktop along with the ability for instant messaging, chat, file transfer or group chat.
- The solution enables users to interact on Video both on Intranet and internet
- The solution works on Windows, Mac, android and IOS devices.

Functional, Technical and Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.1	Communications	Communication System	General	A comprehensive IP based solutions based on a Server Gateway Architecture.
CM-CMS-1.2	Communications	Communication System	General	Support for integrated telephony solution for Video conferencing devices, Analog & IP Phones, PSTN gateways over IP architecture.
CM-CMS-1.3	Communications	Communication System	System Architecture	The call control system should support IPv4 and IPv6 from day one.
CM-CMS-1.4	Communications	Communication System	System Architecture	The system should natively support tenant partitioning so as to comply with TRAI regulations for not allowing VoIP (CUG calls) and PSTN calls to be bridged.
CM-CMS-1.5	Communications	Communication System	System Architecture	The proposed call control server should provide support for standards based SIP IP Phones (Wired & Wireless), Analog Phones, Video Conferencing endpoints and soft clients to provide centralized management and unified dial plan.
CM-CMS-1.6	Communications	Communication System	System Architecture	Conference Bridge—provides software conference bridge resources that can be used by IP EPABX.
CM-CMS-1.7	Communications	Communication System	System Architecture	The system should support an inbuilt/external reporting tool for calls. Reports that are provided include Calls on a user basis, Calls through gateways, Simplified Call Quality
CM-CMS-1.8	Communications	Communication System	System Architecture	Should support signalling standards/Protocols – SIP, H.323, Q.Sig.
CM-CMS-1.9	Communications	Communication System	System Architecture	CODEC support - G.711, G.729, G.729ab, g.722
CM-CMS-1.10	Communications	Communication System	System Architecture	Call preservation – redundancy and automated failure – on call-processing failure. In progress PSTN calls at each of the locations should not be interrupted in the event of any WAN failure or call control server failure.
CM-CMS-1.11	Communications	Communication System	System Architecture	All the appliances in the call control system should have dual redundant and hot swappable power supply and fans for high availability.
CM-CMS-1.12	Communications	Communication System	System Architecture	Support for configuration database (contains system and device configuration information, including dial plan)

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.13	Communications	Communication System	System Architecture	Access to the system should be secure for the purpose of access over IP network. The protection of signaling connection over IP by means of authentication, Integrity and encryption should be carried out using TLS.
CM-CMS-1.14	Communications	Communication System	System Architecture	There should be provision of defining password aging, one time passwords. Provision shall be available to bar unauthorized user to connect to the system. The system should monitor and report the following types of security \ violation login Violations, authorization code violation Station security code violations etc.
CM-CMS-1.15	Communications	Communication System	System Architecture	IP Phones should not support direct, external initiated, connections via HTTP, telnet, FTP, TFTP or any other protocol as means to prevent distributed Denial of Service attack exploitation, except those required for routine firmware upgrades.
CM-CMS-1.16	Communications	Communication System	System Architecture	All Hardware & Software with license required for providing above Security measures must be incorporated.
CM-CMS-1.17	Communications	Communication System	System Capabilities	The System should have IP capability for interfacing & Communicating with Voice, Video and Data infrastructure
CM-CMS-1.18	Communications	Communication System	System Capabilities	The architecture should support a minimum of 60 IP phones and more than one Video Conferencing systems.
CM-CMS-1.19	Communications	Communication System	System Capabilities	The System should support Audio message-waiting indicator (AMWI)
CM-CMS-1.20	Communications	Communication System	System Capabilities	The System should have Automated bandwidth selection
CM-CMS-1.21	Communications	Communication System	System Capabilities	It should be possible to monitor the call control system i.e. system performance, device status, device discovery, voice messaging ports etc.
CM-CMS-1.22	Communications	Communication System	End User Features	Extension mobility
CM-CMS-1.23	Communications	Communication System	End User Features	Call forward all
CM-CMS-1.24	Communications	Communication System	End User Features	Device mobility
CM-CMS-1.25	Communications	Communication System	End User Features	Hunt groups
CM-CMS-1.26	Communications	Communication System	End User Features	Dial-plan partitioning
CM-CMS-1.27	Communications	Communication System	End User Features	Distributed call processing
CM-CMS-1.28	Communications	Communication System	End User Features	Deployment of devices and applications across an IP network
CM-CMS-1.29	Communications	Communication System	End User Features	Call-Servers in proposed solution should be able to support high volume of concurrent call (in multiple of ten thousand's) and there should not be a single point of failure. Each call processing server at different locations must support equivalent capacity.
CM-CMS-1.30	Communications	Communication System	End User Features	Solution should have scalability to 100+ sites through gateway
CM-CMS-1.31	Communications	Communication System	End User Features	Fax over IP—G.711 pass-through and Fax Relay
CM-CMS-1.32	Communications	Communication System	End User Features	Forced authorization codes and client matter codes (account codes)
CM-CMS-1.33	Communications	Communication System	End User Features	H.323 interface to selected devices
CM-CMS-1.34	Communications	Communication System	End User Features	Hotline
CM-CMS-1.35	Communications	Communication System	End User Features	Interface to H.323 gatekeeper for scalability, CAC, and redundancy

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.36	Communications	Communication System	End User Features	Language support for client user interfaces (languages specified separately)
CM-CMS-1.37	Communications	Communication System	End User Features	Multi-Level Precedence and Preemption (MLPP)
CM-CMS-1.38	Communications	Communication System	End User Features	Multilocation—dial-plan partition
CM-CMS-1.39	Communications	Communication System	End User Features	Multiple ISDN protocol support
CM-CMS-1.40	Communications	Communication System	End User Features	Multiple remote CallServer platform administration and debug utilities
CM-CMS-1.41	Communications	Communication System	End User Features	Prepackaged alerts, monitor views, and historical reports
CM-CMS-1.42	Communications	Communication System	End User Features	Real-time and historical application performance monitoring through operating system tools and Simple Network Management Protocol (SNMP)
CM-CMS-1.43	Communications	Communication System	End User Features	Remote terminal service for off-net system monitoring and alerting
CM-CMS-1.44	Communications	Communication System	End User Features	Real-time event monitoring and presentation to common syslog
CM-CMS-1.45	Communications	Communication System	End User Features	Should have the facility to monitor device status, trace, monitor Remote access service, registration messages, etc.
CM-CMS-1.46	Communications	Communication System	End User Features	Trace Collection tool.
CM-CMS-1.47	Communications	Communication System	End User Features	Multisite (cross-WAN) capability with intersite CAC
CM-CMS-1.48	Communications	Communication System	End User Features	Q.SIG (International Organization for Standardization [ISO])
CM-CMS-1.49	Communications	Communication System	End User Features	Call-Server should support new video end points.
CM-CMS-1.50	Communications	Communication System	End User Features	SIP Video endpoints which should inherit the functionality of audio calls which gives the user the same call model for both video and audio calls.
CM-CMS-1.51	Communications	Communication System	End User Features	Call-Server/Collaboration solution should have the infrastructure to handle codec and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place, single point of administration, management of media devices such as gateways and MCUs.
CM-CMS-1.52	Communications	Communication System	End User Features	Call server/collaboration solution should provide control agents for signaling, configuration and serviceability for voice/video end points.
CM-CMS-1.53	Communications	Communication System	Multipoint control Unit	The MCU should be running on standard intel servers on standard Virtualized platforms. The hardware, software and virtualization software should be supplied and supported by a single MSI.
CM-CMS-1.54	Communications	Communication System	Multipoint control Unit	All necessary hardware to support the required capacity needs to be supplied from day one. Each of the server supplied for the MCU must have a redundant power supply from day1.
CM-CMS-1.55	Communications	Communication System	Multipoint control Unit	The MCU must have minimum 20 HD ports @1080p 30 fps with H.264 AVC and Continuous presence from day1.
CM-CMS-1.56	Communications	Communication System	Multipoint control Unit	All the 20 ports must be able to connect different sites at different bandwidths and protocols. H.264 AVC standard must be supported at the minimum to connect all the 20 sites.
CM-CMS-1.57	Communications	Communication System	Multipoint control Unit	The MCU must be able to host at least 4 simultaneous conferences each having different capacities restricted by the maximum port capacity of the MCU
CM-CMS-1.58	Communications	Communication System	Multipoint control Unit	The MCU must also support Full HD mode and it must provide a capacity of connecting at least 10 sites @1080p30 fps

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.59	Communications	Communication System	Multipoint control Unit	MCU should be capable of supporting participants using various means i.e. via video enabled phones, room based video endpoints, soft clients on mobile/tablet or via the browser using WebRTC compatible browsers in a single conference. The meeting quality has to be consistent and of high quality. The end points can be present on the WAN network or on the internet. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution
CM-CMS-1.60	Communications	Communication System	Multipoint control Unit	The MCU should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies
CM-CMS-1.61	Communications	Communication System	Multipoint control Unit	The MCU should support H323 and SIP protocols.
CM-CMS-1.62	Communications	Communication System	Multipoint control Unit	The MCU should support geographical redundancy, so that MCU could be placed in DC/DR setup in case future expansion is needed.
CM-CMS-1.63	Communications	Communication System	Multipoint control Unit	The MCU must support the concept of virtual meeting rooms to users who Hosts meeting frequently. Such meeting rooms should support dialing in from standard based video end points, internal and external users and browser based clients. The system should allow one Virtual meeting room per employee, however it should not consume resources when not in use.
CM-CMS-1.64	Communications	Communication System	Multipoint control Unit	The MCU should be able to maintain the dynamic resource allocation capacity for 1080p, 720p and SD participants simultaneously without having to reboot or change any configuration.
CM-CMS-1.65	Communications	Communication System	Multipoint control Unit	The MCU should support 20 ports or more at HD 720p (transmit and receive) up to 4Mbps on IP in continuous presence mode with 30fps, 100 audio ports, 50 WebRTC connections and H.264 resolution and AES encryption on the same MCU.
CM-CMS-1.66	Communications	Communication System	Multipoint control Unit	The MCU should display a security icon on the endpoint if the conference is secure.
CM-CMS-1.67	Communications	Communication System	Multipoint control Unit	The administrator should be able to specify maximum resolution for main video and content.
CM-CMS-1.68	Communications	Communication System	Multipoint control Unit	Video conferencing endpoints deployed at other organization must be able to take part in video conferencing. The endpoints can be of various makes with using open standards.
CM-CMS-1.69	Communications	Communication System	Multipoint control Unit	Interoperability with all organization must be possible using standards based dialing methodology using the Internet.
CM-CMS-1.70	Communications	Communication System	Multipoint control Unit	The MCU should support on-screen text messaging on video endpoints, so that if there's a delay in starting a meeting, participants can be informed.
CM-CMS-1.71	Communications	Communication System	Multipoint control Unit	The MCU should be able to integrate with existing IP PBX to provide audio conferencing ports to phones.
CM-CMS-1.72	Communications	Communication System	Multipoint control Unit	The MCU should be able to integrate with Call Control system using SIP.
CM-CMS-1.73	Communications	Communication System	Video Standards	Should support H.263, H.263+, H.263++, H.264, H.264 SVC/H.264 High Profile video algorithms
CM-CMS-1.74	Communications	Communication System	Video Resolution	Should support video resolution from SD to Full HD to join into a conference
CM-CMS-1.75	Communications	Communication System	Video Resolution	The proposed MCU should be able to combine HD and SD in the same conference without degrading the HD resolution from and to the HD endpoints. The MCU shall interoperate with multiple vendors' endpoints. The supported mediums should be IPv4 and IPv6.
CM-CMS-1.76	Communications	Communication System	Audio Standards	Along with the support for basic algorithms like G.711 and G.722.1 the MCU should also support wideband Audio protocols like MPEG 4 AAC - LC / MPEG 4 AAC - LD or better
CM-CMS-1.77	Communications	Communication System	Transcoding & Rate Matching	The MCU should support transcoding of different Audio/video Protocols.

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.78	Communications	Communication System	Transcoding & Rate Matching	MCU should be able to combine HD and SD in the same conference without degrading the HD resolution from and to the HD endpoints.
CM-CMS-1.79	Communications	Communication System	Dual Video	The MCU should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).
CM-CMS-1.80	Communications	Communication System	Dual Video	At least 10 sites to be seen simultaneously on the screen in traditional Continuous Presence mode.
CM-CMS-1.81	Communications	Communication System	Dual Video	The MCU must also support advanced continuous presence such that the site that is "on-air" to be seen on a larger window and the other sites are seen in smaller quadrants.
CM-CMS-1.82	Communications	Communication System	Security	The MCU must be a secure Non-PC Hardware with a strong operating system. The Hardware and software must be from the same OEM.
CM-CMS-1.83	Communications	Communication System	Security	The MCU should support 128 Bit strong AES encryption for calls and H.235 for authentication
CM-CMS-1.84	Communications	Communication System	Security	The MCU must support encryption for calls on SIP.
CM-CMS-1.85	Communications	Communication System	Network /USB Interface	At least 1 LAN /Ethernet--10/100/1000 Mbps full duplex and dedicated serial/USB connection for maintenance/upgrade.
CM-CMS-1.86	Communications	Communication System	Conference Layout	MCU Solution should support minimum of 10 layouts
CM-CMS-1.87	Communications	Communication System	Firewall Traversal	Should support firewall traversal solution for Business to Business (B2B) Video Calling.
CM-CMS-1.88	Communications	Communication System	Video Conferencing	Should be an integrated system with at least 23 and above size LCD/TFT screen, 1080P resolution (16:9), HD camera and with speakers for wide band audio output. The Codec should be a part of the unit. No separate Codec's are preferred. The LCD/TFT screen should be a touch/non-touch screen to provide an easier interface to the user through remote control/PC/Laptop keyboards.
CM-CMS-1.89	Communications	Communication System	Video Conferencing	Must support IPv4 and IPv6 from day one.
CM-CMS-1.90	Communications	Communication System	Video Conferencing	Must have the following physical buttons for ease of use 1. Mute/ Unmute 2. Volume Increase/ decrease
CM-CMS-1.91	Communications	Communication System	Video Standards	Minimum H.264 and above
CM-CMS-1.92	Communications	Communication System	Video Standards	The system should support SIP protocol.
CM-CMS-1.93	Communications	Communication System	Video Standards	Must support desktop sharing SIP calls
CM-CMS-1.94	Communications	Communication System	Video Frame Rate	Must support 1080p 30 fps
CM-CMS-1.95	Communications	Communication System	Video Features	Ability to send and receive two live simultaneous video sources in a single call.
CM-CMS-1.96	Communications	Communication System	Video Features	The unit must support layout control for video and presentation on a single LCD / LED screen.
CM-CMS-1.97	Communications	Communication System	Video Input	Should have HDMI or DVI (Digital Video Interface) input to connect PC/ Laptop directly to the Video conferencing system and display a resolution of XGA/SXGA.
CM-CMS-1.98	Communications	Communication System	Video Input	The user must be able to toggle between the Laptop/PC mode and the Video conferencing mode at a push of button/icon.
CM-CMS-1.99	Communications	Communication System	Video Output	Must have a HD output via a HDMI/DVI output port to display the VC screen onto an external display.
CM-CMS-1.100	Communications	Communication System	Video Resolution	CIF (352 x 288 pixels) VGA, 240p, 360p, 480p 720p (1280 x 720 pixels) 1080p (1920x1080 pixels)

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.101	Communications	Communication System	Dual Stream	Must support H.239 and BFCP for resolutions up to 1080p
CM-CMS-1.102	Communications	Communication System	Firewall Traversal	Should support firewall traversal solution using the H.460.18 and H.460.19 protocol.
CM-CMS-1.103	Communications	Communication System	Audio Standards	Audio System: The system should have two stereo front speakers with inbuilt/external microphones, wideband speakers.
CM-CMS-1.104	Communications	Communication System	Audio Standards	G.722, G.711, MPEG 4 AAC or better - which supports 20 KHz audio must be supported
CM-CMS-1.105	Communications	Communication System	Other Features	Noise Reduction/Echo Cancellation, Automatic Gain control, Automatic Audio mixer
CM-CMS-1.106	Communications	Communication System	LAN	1 x LAN /Ethernet--10/100/1000
CM-CMS-1.107	Communications	Communication System	LAN	1 x LAN /Ethernet--10/100/1000 to connect a PC (i.e. built in switch)
CM-CMS-1.108	Communications	Communication System	Wi-Fi	Must support 802.11a/b/g/n
CM-CMS-1.109	Communications	Communication System	Bluetooth	Must support Bluetooth 3.0 for connecting Bluetooth headsets
CM-CMS-1.110	Communications	Communication System	SIP/H.323/ IP Features	Must support Standard based Packet loss recovery algorithm to handle packet loss.
CM-CMS-1.111	Communications	Communication System	SIP/H.323/ IP Features	QOS
CM-CMS-1.112	Communications	Communication System	SIP/H.323/ IP Features	Should support URI Dialing
CM-CMS-1.113	Communications	Communication System	SIP/H.323/ IP Features	Must support SIP and H.323
CM-CMS-1.114	Communications	Communication System	SIP/H.323/ IP Features	Presentation through presence of DVI/HDMI Input port
CM-CMS-1.115	Communications	Communication System	SIP/H.323/ IP Features	The system must have the ability to pair mobile devices such as Tablets and Smartphones based on iOS or Android platforms so that these devices can be used for: 1) View the Presentation that is being shown in the VC call. 2) Add and disconnect call, move the call from mobile device to/ from video unit The system must have the ability to pair with laptop for sending content without any wires to the video unit. In case the above feature is not available natively, then additional components can be provided to achieve this functionality.
CM-CMS-1.116	Communications	Communication System	Security	Password protected system menu
CM-CMS-1.117	Communications	Communication System	Security	Meetings both point to point and multipoint, should be password protected and the same should be possible for SIP networks
CM-CMS-1.118	Communications	Communication System	Security	Encryption of video call: ITU-T standards based Encryption of the video call using Advanced Encryption Standard (AES)
CM-CMS-1.119	Communications	Communication System	Security	Call should be encrypted end-to-end on IP calls
CM-CMS-1.120	Communications	Communication System	Security	The unit must support the option of disabling the secondary network port if not in use.
CM-CMS-1.121	Communications	Communication System	Camera	Should be HD at least 6 megapixel camera, with privacy shutter
CM-CMS-1.122	Communications	Communication System	Camera	Must support 1080p resolution.

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.123	Communications	Communication System	Camera	60 degrees horizontal Field of View
CM-CMS-1.124	Communications	Communication System	Camera	35 degrees vertical field of view
CM-CMS-1.125	Communications	Communication System	Camera	Must have a privacy shutter
CM-CMS-1.126	Communications	Communication System	Camera	The VC unit must allow the camera to be used as a document camera to capture hard copies and transmit it to the far end site.
CM-CMS-1.127	Communications	Communication System	Directory Services	Should support Local and Global directories
CM-CMS-1.128	Communications	Communication System	Directory Services	Should support LDAP and H.350 protocols for directory transfer.
CM-CMS-1.129	Communications	Communication System	System	The system should be an integrated system, HD 1080p camera with automatic speaker tracking cameras or with pre-set setting, total zoom or higher, Mic, remote control, cables and power supply, 55" LCD/LED and a floor mount kit. The system should not be a locally fabricated unit. The system should be capable giving HD 1080p @60fps. The system should deliver 1080p@60fps in motion and in sharpness video mode day one.
CM-CMS-1.130	Communications	Communication System	Contact Centre	Should be highly available with hot standby and seamless failover in case of main server failure. There should not be any downtime of Contact Center in case of single server failure.
CM-CMS-1.131	Communications	Communication System	Contact Centre	Should support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups
CM-CMS-1.132	Communications	Communication System	Contact Centre	ACD support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc.
CM-CMS-1.133	Communications	Communication System	Contact Centre	ACD should support call routing based on longest available agent, circular agent selection algorithms
CM-CMS-1.134	Communications	Communication System	Contact Centre	ACD should support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay.
CM-CMS-1.135	Communications	Communication System	Contact Centre	Agents should be able to chat with other Agents or supervisor from the Agent desktop software or any soft client
CM-CMS-1.136	Communications	Communication System	Contact Centre	Supervisor should be able to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop
CM-CMS-1.137	Communications	Communication System	Contact Centre	Should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.
CM-CMS-1.138	Communications	Communication System	Contact Centre	It is required the ACD should support active and standby server mode, where the server can be put in DC and DR. In case of Main server in the Data Centre fail the standby server in DR should take over seamlessly. ACD solution should support placing of Main and Stand by server in DC and DR respectively
CM-CMS-1.139	Communications	Communication System	Interactive Voice Response	IVR should play welcome messages to callers Prompts to press and collect DTMF digits
CM-CMS-1.140	Communications	Communication System	Interactive Voice Response	IVR should be able to integrate with backend database for self-service, as and when required.
CM-CMS-1.141	Communications	Communication System	Interactive Voice Response	GUI based tool to be provided for designing the IVR and ACD call flow.
CM-CMS-1.142	Communications	Communication System	Interactive Voice Response	IVR should support VoiceXML for ASR, TTS, and DTMF call flows
CM-CMS-1.143	Communications	Communication System	Interactive Voice Response	IVR should be able to Read data from HTTP and XML Pages
CM-CMS-1.144	Communications	Communication System	Interactive Voice Response	IVR should be able to run outbound campaigns.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CM-CMS-1.145	Communications	Communication System	Reporting	System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.
CM-CMS-1.146	Communications	Communication System	Reporting	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes
CM-CMS-1.147	Communications	Communication System	Reporting	Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.
CM-CMS-1.148	Communications	Communication System	Reporting	Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures.
CM-CMS-1.149	Communications	Communication System	Reporting	Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV.
CM-CMS-1.150	Communications	Communication System	Emails	Administrator should be able to assign one or more email addresses to a single Queue.
CM-CMS-1.151	Communications	Communication System	Emails	Email routing support integration with Microsoft Exchange 2003/2007/2010/above versions.
CM-CMS-1.152	Communications	Communication System	Emails	Agents should be able to automatically resume of e-mail processing on voice disconnect.
CM-CMS-1.153	Communications	Communication System	Emails	Agent should be able to save email draft response and resume at a later time.
CM-CMS-1.154	Communications	Communication System	Emails	Agent should be able to re-queue email.
CM-CMS-1.155	Communications	Communication System	Emails	Supervisor should be able to access real-time reporting for Agent E-Mail mail volume by Queue

Note: MSI needs to provision 25 audio and 10 audio-video licenses for IP phones/IPBX

3.3.6. CIOC – Dashboards & Reporting

Dholera will be a smart city, managed and monitored by personnel in Integrated Operations Centers (IOCs) within interim CIOC building. The centers will be equipped with tools and technologies to aid operators conduct their roles. A key component of the technical deployments in the IOCs are large electronic screens. These screens will be used to display information pertinent to the role(s) of the people in each IOC. This type of display of information has come to be known as a dashboard.

The objectives, as mentioned above, can be wide-ranging. Examples of the types of dashboard in Dholera would be;

Three Types of Dashboard

- Operational dashboards tell you what is happening now
 - Events – planned and unplanned; to provide up to the minute information and monitoring of events such as public festivals and crisis response
 - Operations; dashboards will be used in areas such as the SCADA floor to monitor city-wide utilities
- Strategic dashboards track key performance indicators
 - Oversight; there will be a dashboard for the mayor displaying an overview of the city's performance
 - Marketing; a large dashboard has been specified in CIOC/ABCD building for the purpose of displaying information designed to attract investment in to the new city
- Analytical dashboards process data to identify trends
 - Utilities; forward planning of availability and demand for power and water etc. based on past usage and demand

- Emergency response heat maps showing historical trends of ambulance demand at different times of day, can be overlaid with real-time locations of ambulances

Note: Above is an indicative list of dashboards, further details would be shared with the MSI at the time of implementation phase.

Data will be drawn-in from all aspects of the city's operations and will be displayed graphically so as to be "human readable" and insightful.

The data sets will include, but not be limited to, functions such as traffic and parking, environmental measurement, power availability, water requirements, key performance indicators (KPIs), crime statistics, finance, weather and weather warnings, etc.. Some data will be displayed as 'actuals' and other data will be compared to metrics or trends, and could have thresholds indicated. Each type of dataset will have to be carefully considered so as to provide the most insightful information to the observer.

It is important to understand that dashboards are a 'display' of information only. While many dashboards can be interacted with, users can select what to view, and the data can be drilled down, this can only be done in predefined ways; i.e. the data cannot be queried. Nor is a dashboard a method for data entry of any kind.

Initially, Dholera's main focus on dashboards will be for internal use and will display confidential information not available to the public domain.

These dashboards contain all three types of visualization: strategic, analytic and operational.

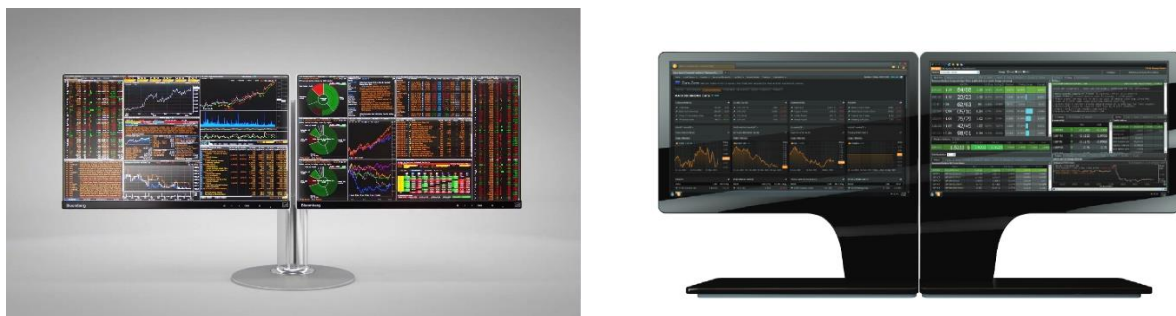


Figure - 35 Analytics dashboards showcasing various parameters

Purpose

The purpose of the Dholera dashboards is to provide situational awareness of the city's current state, in some cases historical data will also be shown. Situational awareness is not intended for focused work. Any focused work will be conducted by the users on their own workstations.

Visual Information Archetypes

Dholera will make use of a number of different visual information display archetypes, these are described below in the context of Dholera CIOC.

In dashboards, for the sake of disambiguation it is necessary to discuss the other information display archetypes. There is a necessary blurring of the lines between the different archetypes, this is also discussed and highlighted in some of the requirements.

- Dashboards; A dashboard is a data visualization tool that displays data, metrics and key performance indicators (KPIs) for an enterprise, department, team, or community of interest. Dashboards consolidate and arrange information, metrics and performance scorecards on a single screen.

They may be tailored for a specific role and display metrics targeted for a single point of view or department, or can provide an oversight of a number of different, or even disparate, data sets.

The dashboards for Dholera will be built on an open framework and be user / administrator configurable to suit the needs of the viewers. These dashboards will be custom views of information as necessitated by purpose and business processes for each display location.

- City Dashboards (internal / confidential)
- Citizen Dashboard (external / public facing)

- Visual Management; is a term used to describe the display of multiple sources each on a single screen as part of a display wall. It is anticipated that numerous data / video sources will be available with the CIOC. These should be made available on the network and 'policed' by policy so only personnel or teams who need to have access to the information can view it.
- Applications; there will be applications which are used to monitor certain functions; indicative examples of this would be:
 - Surveillance / CCTV
 - NOC network performance
 - Call center statistics

The data / screens displayed by these applications can be used standalone or in conjunction with visual management or a dashboard to provide the information that the users require.

- KPI; In the Dholera CIOC there are a number of single displays which are co-located with certain teams or workgroups. These screens will display a simplified information dataset such as number of calls answered, calls waiting, and calls missed in a call center. The content of the KPI screens could come from any archetype mentioned previously.
- Digital Signage; Dholera will have an advanced digital signage platform. The digital signage platform is not a one of the Digital Information Archetypes per se, but is the infrastructure over which the archetypes above will be distributed around the buildings as well as city-wide.

Description of dashboards

The following list shows the expected dashboards based on interim CIOC building design and teams. The information displays listed are examples of what might be required, it not an exhaustive list, any other available information or data may be required also.

- VIP Briefing Room / Situation Room
 - Context sensitive, user selected data; based on briefing requirements or incident being managed
 - Access required to all available data
- Application upkeep center + KPI
 - Application metrics
- City Advertising and Kiosk (KPI)
 - Display of real time advertising content
 - Revenue metrics
 - Display of kiosks in use and trending search
- KPI Screen upkeep
 - Display of all KPI screens usage data
- Utility Integrated management
 - Display of overview of all SCADA / utility systems
 - Display of SCADA systems in entirety
- NOC

- Network performance application
 - Tickets open / known faults / resolution time
- End user technical help desk (KPI)
 - Call center application
- Integrated emergency call center + KPI
 - Emergency Response call center application and KPIs
 - GIS mapping showing asset location
 - Heat map showing predicted / historical demand
- Operations control center
 - All city data needs to be available
 - Mapping
 - Emergency response information
 - CCTV application
 - City performance data
 - Incident management plans
 - Web resources
- Operations control center support team
 - As Operations control center
- Integrated Surveillance center
 - CCTV application
 - CCTV / surveillance related data
 - Emergency response information
 - Incident management information
- City Investment
 - City performance
 - Mapping
 - Development plan
 - Marketing material
- Mayor's Office
 - City performance
 - Mapping
 - Development plan
 - Marketing material
 - All city KPIs
 - Police data / crime statistics
- CIOC Reception
 - City performance
 - City events calendar
 - Marketing materials
- Citizen Dashboard
 - Transport information (bus / train / roads)
 - News and Weather
 - City events calendar
 - Link to e-Govt portal / services

Dashboard Design

The dashboards for the CIOC will develop over time. This development will be predicated by the expansion of the city, and as more services are moved in to the city's control, providing more data sets. The city's data repository will be gradually populated by sensors and IoT devices, and will start to offer meaningful historical data which can be analyzed and displayed.

All of the insight which can be extracted from the data available to the city will go to build dashboards which provide valuable information, and support the city's operation through better informed decision-making.

Not all of the data sets will be available from day one, but will be required as and when they become available. It is not desirable to re-engineer the dashboards each and every time a new data set is made available. It is therefore necessary to deploy a framework and to develop standards which will enable a flexible dashboarding environment.

Anatomy

The recommended approach for a dashboard is to develop a framework, which supports 'drag and drop' elements from a list of available data. This list can be populated through the use of 'widgets' as more data becomes available. The framework will support different sizes and types of widget, these widgets might be simple such as; graphically represented KPIs, data such as temperature, or status of carparks around the city. The more complex widgets would include traffic data shown on a map, or data from SCADA systems. Each widget will be a standardized report, which will be created by a dashboard administrator and made available to users to select.

There are many off-the-shelf dashboard applications, which can be used to generate reports. These applications provide a user interface, which requires no coding.

Framework

The dashboard's framework is a simple application, which enables different widgets to be selected and laid-out on screen, in a structured way, by the users by means of a drag and drop mechanism. Its primary function is to define the form of the widgets. The layouts will be able to be saved and recalled.

The dashboard framework will support different sized widgets and will be user configurable.

Widgets

The widgets for the dashboards will each display a single report. This report will be created by an admin and could use any number of available data sources. The admin will need to select which of the following widget formats is most appropriate to the report being displayed.

Widget ratios:

- 1/1 Full Screen: 16x9 ratio at full HD (1920 x 1080 px) or 4K resolution (3840 x 2160 px)
- 1/2 Half Screen: 8x9 ratio at 960 x 1080 px (or 1920 x 2160 px for 4K displays)
- 1/8 Eighth Screen: 4x4.5 ratio at 480 x 540 px (or 960 x 1080 px for 4K displays)

It will be possible to create 1/4 Quarter Screen widgets in either a landscape or portrait format by using two adjacent 1/8 widgets.

Theses widgets are shown diagrammatically below as is a couple of indicative layouts:

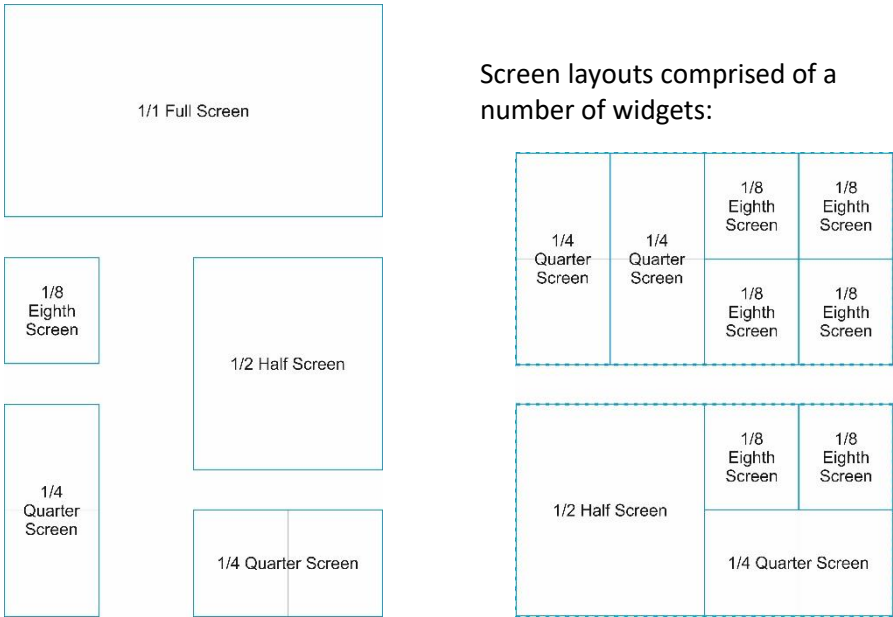


Figure - 36 Screen layout with widgets (indicative)

When selecting the size and resolution of a new widget, care should be taken to consider the type of content, the amount of data to be displayed, the total available screen area in the case of video walls, and the viewing distance of the user.

Using this dashboard approach information-rich displays can be produced and can include many different types of media, from mapping to simple graphical KPIs.

This wall is shown diagrammatically below. Each of the 16x9 ratio rectangles represents an HD resolution display area.

Surveillance / CCTV Display Wall - Physical Screen Diagram:

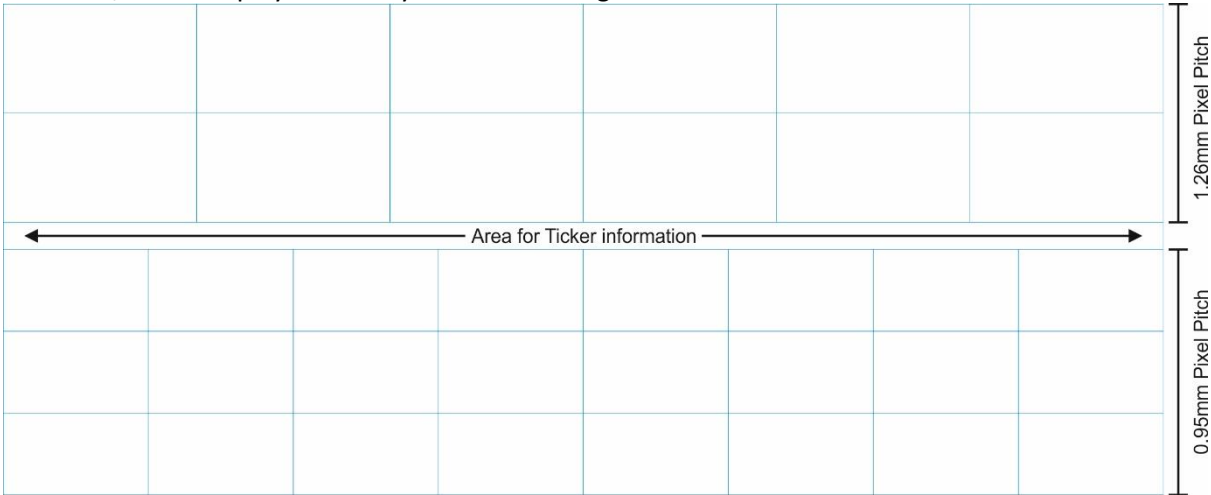
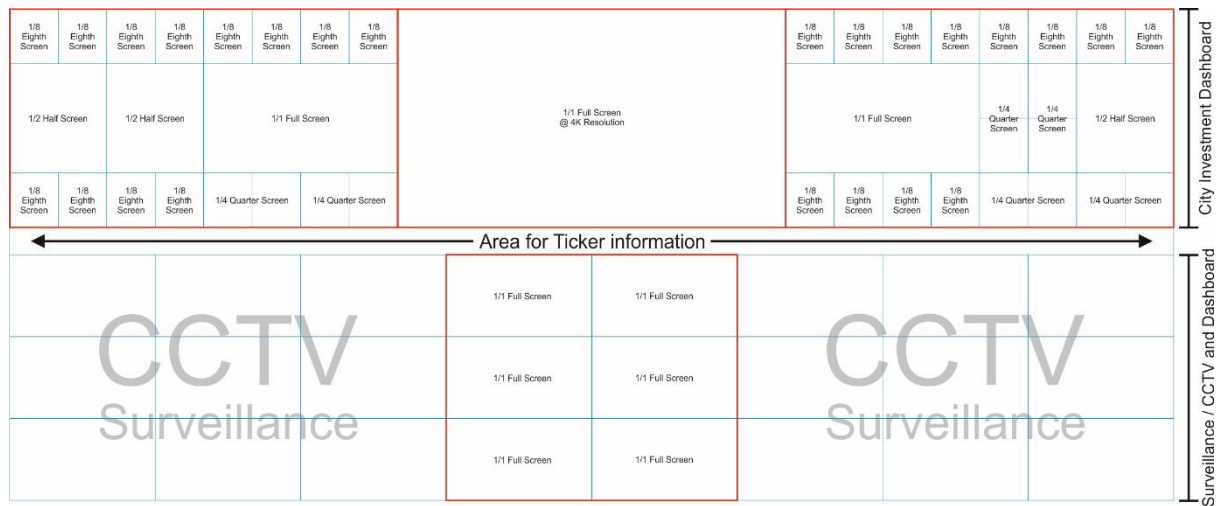


Figure - 37 Video Wall for Surveillance (indicative)

Surveillance / CCTV Display Wall – Dashboard and CCTV Application Layout:
Red bounding boxes show dashboard display area.

RfQ cum RfP for Appointment of Master System Integrator (MSI) for Design, Supply, Install, Test, Integrate, Commissioning, Operation & Maintenance of ICT Components in Cluster A1 of Activation Area at Dholera Special Investment Region, Gujarat



Surveillance / CCTV related Dashboard
Figure – 38 CCTV Display wall

Functional and Technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DAS 1.1	CIO	Dashboards	Dashboards	Users can select a dashboard framework which matches the screen size and resolution of the intended physical display site / screen
CIO-DAS 1.2	CIO	Dashboards	Dashboards	Dashboard frameworks for each screen type and resolution are pre-configured and available
CIO-DAS 1.3	CIO	Dashboards	Dashboards	Users can configure their own dashboard by dragging and dropping widgets in to a framework
CIO-DAS 1.4	CIO	Dashboards	Dashboards	Access to widgets must be controlled by user credentials
CIO-DAS 1.5	CIO	Dashboards	Dashboards	Window with pallet of all available widgets displayed in dashboard configuration application
CIO-DAS 1.6	CIO	Dashboards	Dashboards	Users can request access to widgets from owner / admin
CIO-DAS 1.7	CIO	Dashboards	Dashboards	Users can make a request for a custom widget
CIO-DAS 1.8	CIO	Dashboards	Dashboards	Incident management account with access to all widgets
CIO-DAS 1.9	CIO	Dashboards	Dashboards	Users can save configured dashboards and recall them
CIO-DAS 1.10	CIO	Dashboards	Dashboards	Dashboards can be accessed / configured by multiple users concurrently
CIO-DAS 1.11	CIO	Dashboards	Dashboards	Dashboard framework supports child applications to be windowed within framework
CIO-DAS 1.12	CIO	Dashboards	Dashboards	All data can be accessed by dashboard application
CIO-DAS 1.13	CIO	Dashboards	Dashboards	Dashboard application allows different levels of user access
CIO-DAS 1.14	CIO	Dashboards	Dashboards	Dashboard application can access data from common database repository
CIO-DAS 1.15	CIO	Dashboards	Dashboards	Dashboard application can access data from analytics application
CIO-DAS 1.16	CIO	Dashboards	Dashboards	Dashboard application can access data from specialist applications (incident management, emergency response, mapping, etc.)

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DAS 1.17	CIO	Dashboards	Dashboards	Dashboard application can access data from standard user applications (spreadsheet, etc.)
CIO-DAS 1.18	CIO	Dashboards	Dashboards	Dashboard application can access data from internet (weather, CSS, news, maps, etc.)
CIO-DAS 1.19	CIO	Dashboards	Dashboards	External applications expose required data to Dashboard application
CIO-DAS 1.20	CIO	Dashboards	Dashboards	Dashboard application is interactive
CIO-DAS 1.21	CIO	Dashboards	Dashboards	Users can use touch to interact with dashboard
CIO-DAS 1.22	CIO	Dashboards	Dashboards	Dashboard can contain links to external processes, applications, web pages, etc.
CIO-DAS 1.23	CIO	Dashboards	Dashboards	Multiple instances of same widgets can be displayed
CIO-DAS 1.24	CIO	Dashboards	Dashboards	Widgets can be interacted with without effecting other instances of the same widget (each instance is a separate report)
CIO-DAS 1.25	CIO	Dashboards	Dashboards	Widgets can be real-time reports
CIO-DAS 1.26	CIO	Dashboards	Dashboards	Widgets can be near-real time reports
CIO-DAS 1.27	CIO	Dashboards	Dashboards	Widgets can be historical reports
CIO-DAS 1.28	CIO	Dashboards	Dashboards	Widgets can be simple KPI-type reports
CIO-DAS 1.29	CIO	Dashboards	Dashboards	Widgets can display complex mapping and historical data
CIO-DAS 1.30	CIO	Dashboards	Dashboards	Widgets can be graphically data
CIO-DAS 1.31	CIO	Dashboards	Dashboards	Widgets can be child process windows
CIO-DAS 1.32	CIO	Dashboards	Dashboards	Widgets can be a photo / video
CIO-DAS 1.33	CIO	Dashboards	Dashboards	Widgets are based on standard size formats
CIO-DAS 1.34	CIO	Dashboards	Dashboards	Widgets are designed to have the same look / feel / design
CIO-DAS 1.35	CIO	Dashboards	Dashboards	Style sheets should be developed and used
CIO-DAS 1.36	CIO	Dashboards	Dashboards	Standardized colors must be used for design
CIO-DAS 1.37	CIO	Dashboards	Dashboards	Standardized colors must be used for notifications
CIO-DAS 1.38	CIO	Dashboards	Dashboards	Standardized colors must be used for status (i.e. red / amber / green / blue)
CIO-DAS 1.39	CIO	Dashboards	Dashboards	Admins can make new widgets based on user requests
CIO-DAS 1.40	CIO	Dashboards	Dashboards	Admins can assign widget permissions
CIO-DAS 1.41	CIO	Dashboards	Dashboards	Admins can create new dashboards on behalf of users

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
CIO-DAS 1.42	CIO	Dashboards	Dashboards	Admins can modify dashboards remotely on behalf of users
CIO-DAS 1.43	CIO	Dashboards	Dashboards	Widgets can access calendar information
CIO-DAS 1.44	CIO	Dashboards	Dashboards	Widgets can respond to data changes (i.e. status change / thresholds)

Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR-DAS 1.0	Dashboards	Non Functional requirement	Security	Required levels, Administrator, Content creator, content manager, view.
NFR-DAS 1.1	Dashboards	Non Functional requirement	Security	Administrator: Full admin access to all components and functionality. Content Creator: access to create new dashboard components, framework, widget, data connections, layouts, dashboard (visual management) groups, css feeds, etc., no hardware or firmware or system config changes. Content Manager: access to schedule and select dashboard views across all displays. View user: view only access to content.
NFR-DAS 1.2	Dashboards	Non Functional requirement	Security	Access permissions changed by administrators on instruction of application owner(s)
NFR-DAS 1.3	Dashboards	Non Functional requirement	Security	If passwords are not managed through active directory - User Passwords must be eight characters long and contain numerals, special characters and letters (upper and lower case). Passwords must be unique to each user. Admin passwords must be unique to each administrator. All passwords must be changed every 90 days.
NFR-DAS 1.4	Dashboards	Non Functional requirement	Security	Must comply with enterprise-wide IT application security. No special requirements
NFR-DAS 1.5	Dashboards	Non Functional requirement	Security	Dashboard layouts and content must be backed up every 24 hrs. System configuration must be backed up before and after every configuration change. All backups to be stored securely as per IT / Data security policy
NFR-DAS 1.6	Dashboards	Non Functional requirement	Security	128-bit AES encryption or HDCP 2.0 is required on all data passed between devices
NFR-DAS 2.0	Dashboards	Non Functional requirement	Audit	Audit trail for login, who, when and changes made. Display changes (which dashboard on which display)
NFR-DAS 2.1	Dashboards	Non Functional requirement	Audit	Storage capacity should be adequate for, dashboard layouts, three times the content, logging, reports and audit data.
NFR-DAS 2.2	Dashboards	Non Functional requirement	Audit	Dashboard software must be exposed to all available data, either through ESB or data historian, direct application connection is not desirable.
NFR-DAS 3.0	Dashboards	Non Functional requirement	Availability	Software duty cycle: 24/365 (h/d)
NFR-DAS 3.1	Dashboards	Non Functional requirement	Availability	Planned maintenance must be carried out to minimize periods of unavailability i.e. out of office hours. Dashboards are for situational awareness, not focused effort and therefore short planned outages is acceptable.
NFR-DAS 3.2	Dashboards	Non Functional requirement	Availability	Signage content is required citywide. Admin access should be from any display point and any point on the signage VLAN (WAN/LAN)
NFR-DAS 4.0	Dashboards	Non Functional requirement	Reliability	Dashboard software should be fully redundant / clustered to ensure high availability
NFR-DAS 4.1	Dashboards	Non Functional requirement	Reliability	Maximum 1 hour for break fix during operational times, for partial loss of availability.
NFR-DAS 5.0	Dashboards	Non Functional requirement	Usability	Look and Feel to be defined by dashboard admins / designers / content creation users - this is a highly subjective topic. Framework must be flexible to allow users to leverage the system without unnecessary design constraints.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR-DAS 5.1	Dashboards	Non Functional requirement	Usability	Signage platform must support multi-lingual content with different character sets
NFR-DAS 6.0	Dashboards	Non Functional requirement	Documentation	Full documentation is required to be handed over. This includes specification of every application used, its maintenance, its revision version and IP address table(s). Operations and Maintenance manual must be provided including back-up frequency, updates calendar (where known), original installation files and license keys. Configuration data book is required for all application and configuration of software, back-up and recovery data must be provided.
NFR-DAS 6.1	Dashboards	Non Functional requirement	Documentation	In addition to knowledge base, manufacturers operations manuals must be provided
NFR-DAS 6.2	Dashboards	Non Functional requirement	Documentation	In addition to user guides and quick start manuals, manufacturers' operations manuals must be provided. Train the trainer materials will be required

3.3.7. Integrated Building Management System

Objective of IBMS:

As a part of Smart City initiative and order to carry out the Safety, Security and automation functions, the Administrative and Business Centre for Dholera (ABCD) complex is planned to support for 153 sq. km of Dholera Special Investment Region (DSIR).

ABCD complex was designed along with the overall master plan of the area covering 9 HA of land. – ABCD complex will house the offices of the proposed Node/ City level SPV, Exhibition Cum Auditorium Centre, Data Centre/Server Room and City Integrated Operations Centre.

The proposed IBMS Solution across various facilities shall comply to standards, integral, expandable / scalable from a long-term perspective as per the requirements of Dholera Special Investment region. Effort shall be made to conceal all services and still provide access to these for accommodating changes in requirement in future. Conservation of energy, optimization of resources, eco-friendliness, modular construction of support infrastructure and state of the art technology shall be the key factors in the design concept to ensure least downtime and reduce maintenance hassles.

The proposed Designs, Solutions, Specifications & BOQ along with draft drawings are enclosed in the tender document and are meant for reference and for purpose of bidding. The MSI so finalized would be required to make all the necessary shop drawings within the layouts enclosed and the BOQ in consultation with the DICDL/ICT Consultant to arrive at the final scheme in line with the requirements of the DSIR. The final scheme so submitted should be in accordance with Guidelines, Indian Standards, ISO and Green IT requirements, BIS and National Building codes, ASHRAE, TIA provisions if any.

The proposed Safety, Security and automation systems will remain under comprehensive warranty for 5 Years from date of Go-Live and the MSI has to ensure systems availability to 99.74%. The Scope also includes the Operation and Maintenance of the for 5 years along with any hardware/software upgrade and replace as the case may be.

Scope of Work:

The scope of the work is to provide Turnkey solution of IBMS with required Infrastructure, which shall include the Supply, Installation, Testing & Commissioning (SITC) of various facilities and its operations and Maintenance.

- The solution shall comprise of supply, installation, testing, commissioning, training and handing over of all materials, equipment, hardware, software, appliances and necessary toolkits, all complete with all the required components & documentation strictly as per the enclosed tender specifications, design details.
- The scope includes the supply, installation & commissioning of any material or equipment including civil/interior works and works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project
- The successful MSI shall provide documentation including user, system and operation manuals as well as the necessary diagrams and design drawings;
- MSI shall be responsible for providing complete IBMS for Service Area Buildings as Turnkey project. Technical details and BoQ are mentioned as part of this document itself.
- MSI shall be responsible for performing verification tests (FAT or any other respective tests) at manufacturing site & installation site to ensure all proposed software and hardware are functioning properly as designed. MSI should share the FAT as well as test certificate for all required tests performed during project implementation and O&M phase to DICDL on timely manner.
- MSI shall be responsible for providing support and maintenance for all equipment and systems installed on site on 24 x 7 x 365 basis and the systems availability must be 99.74%.
- In case of any planned maintenance to be carried out over the system then the MSI needs to get a prior approval from DICDL as well as the ICT Consultant before starting off the maintenance activity. Also it should be taken care that the maintenance activity is planned mainly on non-office hours.
- MSI shall be responsible for providing acceptance checklists for the project.
- The Designed IBMS solutions in various facilities should completely integrate to central location (integrated operations center or any other central location as finalized by DICDL) in all respect and handover the same to DICDL for to be use in 240 days from date of issue of work order to the successful MSI.
- MSI shall be responsible for providing and configuring, commissioning overall IBMS integration software with unlimited licenses and should have scalable licenses to meet future integrations.

Any extra item / works arising out of the changes in the scheme shall be first notified to the Site Project Engineer and the ICT Consultant/, who shall take a review of the same and if convinced notify the DICDL officials about the execution of that item / work.

The IBMS activity will include the following, but not limited to;

- Cabling and Conduiting
- Installation of Controllers, devices
- Power cabling for controllers, devices
- Integrated Building Management Software deployment and Integration to central location.
- Operation and Maintenance of the system as per scope mentioned in the tender.

Submittals/Deliverables:

- Product data for IBMS system components including dimensioned plans, sections, and elevations showing minimum clearances, installed features and devices, and list of materials.
- Wiring diagrams for equipment, devices and for system with all terminals and interconnections identified. Include drawings indicating components of field wiring.
- Shop drawings shall be subject to approval of project stakeholders.
- System operation description including method of operation and supervision and sequence of operations for all IBMS system. Description shall cover this specific project. Manufacturer's standard descriptions for generic systems are not acceptable.
- Product certification signed by the manufacturer of the fire alarm system components certifying that their products comply with the referenced standards and specifications.
- All As-Built drawings for all IBMS Systems at completion and handing over the project.

Quality Assurance:

- **Manufacturer's Qualifications:** Firms regularly engaged in manufacture of IBMS systems and components, whose products have been in satisfactory use in similar services for not less than 5 years period.
- **Installer Qualifications:** An experienced specialist sub-contractor who is authorized by the system manufacturer.
- All the components and installations shall comply with the requirements of IEC, BS, IS, NFPA and NEMA standards.
- **Single Source Responsibility:** All components and accessories shall be product of single manufacturer.

MSI shall provide qualified and experienced senior IBMS expert on site for execution of the Project Work & during operations and should submit the name, experience, qualification and role during execution, installation & operations of the project work and will be responsible for all the installation work under the scope of contract.

Design Criteria: Master System Integration

MSI shall adopt Safety, Security system Industry Standards for implementation of IBMS. MSI to ensure Captive infrastructure required to support complete IBMS solution to integrate all installed systems at various facilities to seamlessly communicate with Central location (Integrated Operation Center) to monitor, configure, operate, view all alarms and events. The monitoring & control software shall be based on the generic Building Operating System (BOS) software platform that contains the full set of features and functionalities to serve as the Monitoring & Control Software for the fully featured IBMS system, and supports integration and interoperability of various building systems.

The BOS software platform shall consist of the BOS Server and User Interface applications. The BOS Server shall be a scalable solution, based on modern software architecture and technologies, and its core applications shall be implemented using industry standard technology. The software shall be capable of running on both Windows and Linux operating systems.

The BOS Server shall support industry standard operating systems, networks and protocols. The system shall support industry standard protocols, including at least BACnet, Lon Works, Modbus, M-Bus, OPC, Ethernet TCP/IP technologies. These protocols shall be supported on software level without need for external gateways. Web UI application and Client UI application shall both be supported as User Interface applications.

The BOS platform shall support a true Client-Server architecture, enabling the server application to be run separately from the client application. Whenever required, it shall also be possible to run both applications on the same computer. Client connections to the server must utilize TCP/IP network (e.g. LAN, Internet). The server application shall be able to handle many simultaneous client connections from a number of workstations. The BOS platform shall allow for usage through a standard Internet browser.

BOS Server application shall be a software product allowed to have a project specific application, The BOS Server shall offer an application framework consisting of core services and network interface driver services. It shall also be possible to develop new services to the framework according to the manufacturer's development API specifications. The BOS Server shall include a RDBMS database for centralized storage of system events, trends and logs. The RDBMS database shall be able to run on the same server or in a separate computer. The system shall include centralized alarm dispatching features

for all connected systems, using e.g. SMS, mobile app and email. The system shall support triggering of functions based on the events from the other connected systems. The BOS Server shall be configurable using a dedicated application, e.g. a Server Manager Tool. It shall be possible to configure the Server Application, which is installed on the same computer, or remotely accessed server using SSH connection. The Server Manager application shall allow for configuration of the services, users and user rights based on the structured data model of the server. It shall be possible to take a backup of the configurations of the server application using the Server Manager Tool. All configuration must be done using the Server Manager application. No manual editing or manipulation of the server application's configuration files is allowed, in order to prevent unwanted error situations.

Integrated Monitoring & Control Software Features

The BOS platform shall include the following features: -

- The systems connected to the BOS shall be monitored with a Graphical User Interface. Web usage and a client application shall be both supported.
- The BOS shall support receiving of real time values, trends, alarms and event logs from the connected systems. Different levels of logs (e.g. warning, error, info) shall be available.
- The BOS shall support modification of set points, time schedules and manual (override) controls in the connected systems.
- The BOS shall support an event mapping mechanism for triggering of functions, e.g. starting video recording and turning on lights from events like unauthorized access attempt, or turning 'ON' the Air Conditioning Unit of the room while the employee/person is granted access to the building.
- The BOS shall be modular in structure, consisting of services, which are flexible to add, configure and to update. - The functionalities of the BOS shall run on the server level autonomously of the user interfaces.
- The BOS shall support multiple operating systems, including UNIX, Linux and Windows.
- The BOS shall contain an RDBMS database for storing data.
- The BOS shall contain drivers to industry standard field buses and shall support third party device integrations.
- The BOS shall contain a Data Model describing the structure of the building and the control systems.
- The BOS shall support high-availability systems with a failover server.
- The BOS shall use dedicated storage server for video alarms.
- The BOS support shall support unlimited user licenses.

Integration Interfaces

The BOS Server shall comprise defined interfaces for systems and applications to be connected with the platform. The interfaces shall include interfaces as follows:

- A System Interface to allow different systems to be connected with the BOS Server using Network Interface Drivers and Device Drivers.
- An Enterprise Interface to allow a variety of applications and services to be produced and connected with the BOS platform and accessing all connected systems. The Enterprise Interface shall enable value-adding services that require accessing the connected building systems.

IBMS Integrated Software Performance Efficiency

Sr. No.	Service Level Requirement	Performance Efficiency
1	Definition	Application Performance refers to the maximum time for IBMS Application(s) initialization, login screen, response time. Application availability refers to the total time when the Application is available to the users for performing all activities and tasks.
2	Measurement of Service Level Parameter	$[(\text{Total Uptime of the Application in a quarter}) / (\text{Total Time in a quarter})] * 100$
	a. Overall application(s) availability	$\geq 98\%$
	b. Response Times application being used at CIOC	$< 5 \text{ Sec}$
	c. Maximum time for User Login	$< 4 \text{ Sec}$
	d. Menu Navigation, Window/Screen Opening, Screen Navigation (Average)	$< 4 \text{ Sec}$
	e. Change of Screen from one camera source to another	$< 4 \text{ Sec}$
	f. Video Feed Query Retrieval Response Time	$< 5 \text{ Sec}$
	Simple query - Report generation of more than 10 days data	Simple query - $< 5 \text{ Sec}$
	Medium complexity query - Report generation of more than 20 days data	Medium complexity query - $< 10 \text{ Sec}$
	High Complexity query - Report generation of more than 30 days data	High Complexity query - $< 15 \text{ Sec}$
	g. Reports Generation Response Time (Alerts/MIS/Logs)	Medium complexity query - $< 30 \text{ Sec}$ High Complexity query - $< 60 \text{ Sec}$
	h. PTZ Lag time (movement at keyboard/joystick and actual moving indication through video feed viewed)	$< 3 \text{ Sec}$
	i. Maximum time for successful camera settings modification	$< 4 \text{ Sec}$
3	Measurement Method	Automated system tools
4	Responsibility for Measurement	System Integrator

Client User Interface Application

The system shall enable a client-based User Interface for central monitoring of systems. The User Interface client shall allow for the following:

- **Alarm monitoring and alarm handling by multiple operators**
 - Access Control alarms
 - Fire alarms
 - Alarms from electrical and BMS systems
 - System maintenance alarms
 - Video monitoring
- **Remote diagnostics, energy optimization and trending**
 - Set point adjustment
 - Control optimization
 - Trending
 - Remote diagnostics of system/devices
 - Preventive maintenance schedule

- Consumption reports for energy management and billing
 - Logs and reporting
 - User profile and role management
 - Access rights management

Web User Interface Application

The User Interface shall also be available as a Web Application, having the same main features as the Client Applications.

Alarms Handling

The BOS platform shall include an alarm handling mechanism for connected systems. Alarms shall be displayed in chronological order on the Alarm lists. In addition, it shall be possible to define an optional audible annunciation with user selectable audio file. Alarming points can also include operator instructions as free-form text. Operator can acknowledge alarms either one by one or several at one time. Alarm lists shall be shown as separate tabs, including Active Alarms, Handled by Me, Handled by Others and Acknowledged Alarms. The operator can accept an alarm into his/her handling process, and the alarm is then removed from the main list of Active Alarms.

The status of alarms shall be indicated with the following colors.

- RED - alarm is activated, unacknowledged
- YELLOW - alarm is inactivated, unacknowledged
- GREEN - alarm is activated, acknowledged
- GREY - alarm is inactivated, acknowledged

Alarm list shall include also the Alarm History Browser feature, which enables queries to system wide alarm database covering all present and past alarms. This feature can be used for trouble-shooting and auditing.

The Alarm list shall include an advanced linking feature. Each alarming point shall be automatically equipped with a link to guide the operator straight into the alarming point in any of the graphical views. The alarming point shall be temporarily highlighted to guide the user to the correct point on the graphical view.

Event Logs

Event log shall store all control events that are initiated from the graphical User Interface by the operator. Each log event shall include event time, user name, controlled point and value.

System should facilitate to export event logs as CSV file for utilization by external applications.

The log shall also include a link to the controlled point to guide the operator straight into the point in any of the graphical views.

Functional Requirements

Sr. No	Description

1	IBMS Integration Software: Graphical User Interface Software meeting the scope mentioned in the document for overall integration of Safety, Security, automation systems including configuration and facility to create and provide the graphic mapping of all alarms, events integrated to central location for monitoring and controlling. The software should support animate the Graphics, Navigation between pages, display of logs, popup alarms, configurable password protection. Software shall be able to communicate with Lon works, BACnet, Modbus and open protocol simultaneously, with unlimited user license capacity. The integration software seamlessly supports multiple client workstation for viewing /acknowledging, monitoring of all events and alarms generated by all controllers.

The proposed Safety, Security and automation systems will remain under comprehensive warranty for 5 Years from date of Handing Over of the Project and the MSI has to ensure systems availability up to 99.74%. The Scope also includes the Operation and Maintenance for 5 years.

Technical Annexures (IBMS)

The scope of the work is to provide Turnkey solution of IBMS with required Infrastructure which shall include the Supply, Installation, Testing & Commissioning (SITC) of various facilities and its operations and Maintenance.

- The solution shall comprise of supply, installation, testing, commissioning, training and handing over of all materials, equipment, hardware, software, appliances and necessary toolkits, all complete with all the required components & documentation strictly as per the enclosed tender specifications, design details.
- The scope includes the supply, installation & commissioning of any material or equipment including civil/interior works and works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project
- The successful MSI shall provide documentation including user, system and operation manuals as well as the necessary diagrams and design drawings;
- The successful MSI shall be responsible for providing complete IBMS for Service Area Buildings as Turnkey project. Technical details would be shared by DICDL to the successive MSI at the time of design and implementation phase.
- The successful MSI shall be responsible for performing verification tests at manufacturing site & installation site to ensure all proposed software and hardware are functioning properly as designed.
- The successful MSI shall be responsible for providing support and maintenance for all equipment and systems installed on site on 24 x 7 x 365 basis and the systems availability must be 99.74%.
- The successful MSI shall be responsible for providing acceptance checklists for the project.
- The Designed IBMS solutions in various facilities should completely integrate to central location in all respect and handover to DSIR for to be use in 180days from date of issue of work order to the successful MSI.
- The successful MSI shall be responsible for providing and configuring, commissioning overall IBMS integration software with unlimited licenses and should have 30% spare licenses to meet future integrations.

3.3.8. Variable message Signboards

Variable Message Sign Board is a system by which information can be centrally authored, controlled, and most importantly distributed throughout a building, across the campus, or across the whole city. This is done on a network of digital displays that are centrally managed and addressable for targeted information, entertainment, merchandising and advertisement.

Signage can provide traveler information, at bus and train stations, airports along with pedestrian guidance

within buildings and cafeteria menus, in addition to revenue generating advertising.

Dholera will require major broad types of content such as:

- Display only – this is content which is pushed to screens with no user control or interaction. It would be used for:
 - Advertising – revenue generating; requires audit trail and billing capabilities. The content displayed can follow pre-arranged playlists shown at defined time slots or dynamic playlists that evolve according to criteria including user interaction, environmental sensors, event triggers in response to local activities.
 - Information – display of information within buildings or citywide. This could be VMS (Variable Message Signage) at bus stops or for notifications with office areas.
- Visual Management (user selectable) – the CIOC has many meeting rooms and dashboard displays, in these cases the users / room occupants will need to select what content is displayed. The content could be from a local source i.e. their own laptop or from central data historian i.e. a dashboard, or a collection of different dashboards, applications, browsers, etc. to provide situational awareness to users.

VMS shall be generally used for:

- Public information – news, weather, traffic and local (location specific) information, such as building directory with map, fire exits and traveler information.
- Internal information - corporate messages, such as health & safety items, news, and so forth.
- Advertising and Promotion – promoting products or services, may be related to the location of the sign or using the screen's audience reach for general advertising.
- Influencing behavior – directing people to different areas, providing wayfinding services, and a wide range of other uses in service of such influence.
- Enhancing customer experience – applications include the reduction of perceived wait time in the waiting areas, as well as demonstrations, such as those of recipes in food stores, among other examples.
- Navigation – with interactive screens / kiosks or with other means of dynamic wayfinding to guide staff and visitors to the area they need to go.
- City information – citizen dashboards, events and outages.
- Variable message service – Roadside displays can be controlled and monitored by a signage platform.

Important considerations are:

- Scalability - Using industry standard and well understood technologies to ensure signage solutions scale - while remaining cost effective - from a single standalone solution to a network of tens of thousands.
- Complete Solution - To not only deliver rich functionality for all scenarios in a single solution, but to do so using an appliance model where the solution comes ready to run out of the box, and run for years without user intervention.
- Reliability - To deliver reliability using high quality hardware and a stable operating system for digital signage. This assures 24h/365d uptime and minimal maintenance downtime
- Multi-Zone and Layout capability - Provide absolute control over what appears on your signage. Overlapping videos, images, text and flash, to simple full screen video, the Player provides rich capabilities to make it easy to get your message across.
- Easy access to external content - Use external content on your signage making it more engaging. Bring live TV, Video, Web pages, RSS feeds, and even captured HD content from set top boxes, PCs and Blu-ray™ players and display it on your signage.
- Role and Permission control - Multi-level control of content, play listing and publishing can be applied to meet the global and local needs of an Enterprise network.
- Easy to Update - Up to date content is much more effective in attracting attention, content updates

are quick and easy. Overall layout design can be controlled centrally while content in specific zones can be updated by local staff.

- Considerations of Structure Design for mounting VMS:
 - The minimum vertical clearance between the finished road surface and the bottom of the support structure/bottom of the VMS (whichever is lower) shall be 5.5 m as per IRC/MORTH guidelines.
 - The structure for VMS mounting shall be designed for wind speeds as per IS-875 part 3
 - Should have suitable walkway for maintenance access

VMS will be used to provide many levels of information. That is:

- Specific and relevant to the buildings or rooms within buildings
- General Notifications – both Public and Internal, both inside and outside of buildings
- Advertising – Targeted dependent on location and time of day
- Within the buildings information can be displayed directly on a screen or overlaid on current live presentation to alert participants of an event, without stopping their presentation.
- Broadcast and advertising content can be displayed
- In an emergency evacuation, ‘what to do next information’ can be ‘pushed’ that is relevant to the display’s location.
- The same signage system, virtually segregated, will be used to display information citywide.

VMS will be used to provide a number of levels of information such as:

- Specific and relevant to the building within the ABCD campus,
- General Notifications – both public and confidential, Internal or external of buildings
- Advertising – Targeted dependent and according to displays physical location

Within the ABCD campus buildings information can be displayed directly on a screen or overlaid on current live presentation to alert participants of an event, without stopping their presentation.

Broadcast and advertising content can be displayed full screen or within windows, to suit the displays usage at the time the information is transmitted and the level of urgency applied to the content.

In an emergency evacuation, what to do next information can be ‘pushed’ that is relevant to the display’s location, this content would be designed to be clearly visible and unambiguous.

In many locations the content will include audio that will be relayed through the displays internal speakers, however in dedicated areas or rooms this audio may have additional sound reinforcement.

The same signage system within the ABCD campus, will be used to display information citywide however all external areas will be ‘virtually separated’ on the networks.

Signage Areas

There are three distinct geographic signage areas that will be addressed and handled by the main signage platform:

- ABCD Campus
- City Wide Information systems
- General Advertising

Functional and Technical requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
VMS-1.1	Variable Message Signboard	VMS	Content management	Content Management software will allow authorized users to edit, create and display templates / content
VMS-1.2	Variable Message Signboard	VMS	Content management	Management software will allow regulation of relevant content to relevant areas
VMS-1.3	Variable Message Signboard	VMS	Media	Will have the ability to upload Images (multi-format)
VMS-1.4	Variable Message Signboard	VMS	Media	Will have the ability to upload video (multi-format)
VMS-1.5	Variable Message Signboard	VMS	Functionality	Can display Calendars
VMS-1.6	Variable Message Signboard	VMS	Functionality	Can display Clocks
VMS-1.7	Variable Message Signboard	VMS	Functionality	Can display RSS feeds, Rich media and HTML
VMS-1.8	Variable Message Signboard	VMS	Functionality	Will allow Scheduling
VMS-1.9	Variable Message Signboard	VMS	Functionality	Will allow creation of Playlists
VMS-1.10	Variable Message Signboard	VMS	Technical capability	Will allow Zoning
VMS-1.11	Variable Message Signboard	VMS	Technical capability	Change Channels within IPTV
VMS-1.12	Variable Message Signboard	VMS	Technical capability	The system shall be 4k Compatibility
VMS-1.13	Variable Message Signboard	VMS	Technical capability	Multi video windows
VMS-1.14	Variable Message Signboard	VMS	Technical capability	Will integrate LDAP/ Active directory
VMS-1.15	Variable Message Signboard	VMS	Technical capability	Will support SAML Integration
VMS-1.16	Variable Message Signboard	VMS	Technical capability	Will have redundancy and auto failover
VMS-1.17	Variable Message Signboard	VMS	User management	User management
VMS-1.18	Variable Message Signboard	VMS	Audio support	The system will support audio
VMS-1.19	Variable Message Signboard	VMS	Audio support	The Audio will be routable to external audio systems
VMS-1.20	Variable Message Signboard	VMS	Displaying	Content can be displayed on multiple displays simultaneously
VMS-1.21	Variable Message Signboard	VMS	Displaying	Different content can be displayed on multiple different displays simultaneously

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
VMS-1.22	Variable Message Signboard	VMS	UX	Users will be able to interact / select the content where appropriate
VMS-1.23	Variable Message Signboard	VMS	UX	All senses experience
VMS-1.24	Variable Message Signboard	VMS	Integration	Information content can be collected from 3rd party traffic systems and displayed on standard screens, LED Pixel boards and full matrix signs (MS4) on overhead gantries.
VMS-1.25	Variable Message Signboard	VMS	Integration	The system will be able to collect data from many different external data sources and using pre-designed layout templates, display the information in a manner useful to the user
VMS-1.26	Variable Message Signboard	VMS	Event triggers	Will support external event triggers
VMS-1.27	Variable Message Signboard	VMS	Event triggers	The system will respond to event triggers, either software, closed contact, serial or fire (or other emergency) alarm input
VMS-1.28	Variable Message Signboard	VMS	Event triggers	On receipt of an event trigger the appropriate message for the display location will be displayed
VMS-1.29	Variable Message Signboard	VMS	Event triggers	The event triggered display will either be an overlay, a windowed screen or a full screen 'take over' depending on the severity of the trigger event
VMS-1.30	Variable Message Signboard	VMS	Advertisement management	Software Management of advertising content
VMS-1.31	Variable Message Signboard	VMS	Advertisement management	Scheduling and Tracking of "Paid for" advertising
VMS-1.32	Variable Message Signboard	VMS	Advertisement management	Software mechanism to auto-generate invoices for advertising content
VMS-1.33	Variable Message Signboard	VMS	Administrator	Administrator settable user credentials for control of signage display segments
VMS-1.34	Variable Message Signboard	VMS	Administrator	Administrator settable user credentials for creation of signage content

Technical Requirements

Sr. No.	Description
Content Designing tool	
1	Content Creation/Composer, Presentation/Layout Maker & Designer Software
2	Capability to drag and drop to any layer/Plug-in on the presentation area
3	Plug-in Based Architecture / API for allowing easy custom development of new plug-ins
4	Allow to create unlimited overlapping layers with full transparency control.
5	Capability to encrypt presentations & capability to Preview your final layout/presentations before publishing it to Player
6	Should have Unlimited History to go back to any previous state of the presentation while working on
7	Capability for Masking Support: Apply mask on every element (including videos) to show only the required portion of the element.
8	Should have capability for RSS Integration: Display RSS feeds intelligently by merging different content with the data received from the feeds.

9	Capability for Rich Text Support: Create documents with full flexibility with an option use RSS Feeds as well.
10	Should have the capability for Professional Alpha Key: Ability to specify the alpha key in videos and display on top of any other zone.
11	Show preview of media created
12	Choice of Layout Design in landscape-mode or portrait mode and playback in same mode.
13	Should have External file support: import Power-Point / PPT as WMV video or Adobe (.pdf),
14	External plugins for Countdown timer in digital clock: Add countdown timer to a particular date and time or for a particular duration in customizable digital format.
15	External Database Support for XML, Oracle, Google Spreadsheet, Google Calendar, Microsoft Exchange, SQL Server, Excel, CSV, etc.
16	Synchronization of elements in different zones
17	Display any kind of textual data from any database source in the form of crawls/scrawl or tabular form.
18	Should be Capable of Change the live data (from databases) using predefined set of rules/layouts before they are displayed.
19	Content creator to create layouts and preview the output in real time before transferring/publishing the content.
20	Multi language input and display support.
21	Animations capability for layers (including transition animations, movements, effects and time)
22	Should be Capable to create QR codes.
23	Database support for Scrolls/tickers.
24	Separator/image support for Scrolls/tickers.
25	Capability to add overlays, (picture in picture)
26	Option to add vertical scrolls with text and pictures.
27	Should have capability to Show content from Live camera (without using streaming)
28	Should have capability of creating gradient/Color animations
29	Background animations
30	Should have capability on layer transparency control
31	Should have capability on timeline for layer time control
32	Should have capability on stopwatch and timer capability.
33	Should have digital clock with customization for display format. (DD/MM/YY or MM/DD/YY or MM/DD/YYYY HH:MM:SS)
34	Capability to show world time (analogue/digital) in regional cultures.
35	Capability to show World weather with support for current conditions, forecast; in regional cultures.
36	Should have the capability of edit the media files added in layout.
37	Should have the capability undo or redo any performed activity
38	Should have the capability to play two or more different contents with single media designing layout
39	Should have the capability crop videos/web links/ images as per the requirements
40	Should have the capability combine the multiple layouts and publish them at once rather than individually scheduling different layouts
41	Should have the capability on supporting following file formats - All Standard Images - Tiff/ Jpeg/ BMP etc. - Shockwave / Flash/ RSS Feeds - Live Analogue Television - DVB Format Digital TV - Live Video Capture (DVD, Web Cams, CCTV etc. - Advanced Systems Format/ DivX - XML/ Web Pages

42	Windows Media Formats - MPEG-1 (.mpeg, .mpg, .m1v) - MPEG Audio Layer II (.mp2, .mpa)/ M3U (.m3u)/ MP4 (.mp4)/ QuickTime Content (.avi, .mov, .qt) - MPEG Audio Layer III (.mp3)
Content Manager/Scheduler/Publisher Software	
1	Should be password protected so as to keep the entire network secure.
2	Should have Email Alerts capability: Get Notified as soon as the player goes out of reach and get the support team started on recovery process.
3	Should allow to Create and manage schedules in visual Timeline and playlist.
4	Lock the players and secure them using your own passwords to prevent unauthorized access.
5	Should have strong Encrypted and secure communication between content scheduler and players.
6	Should allow seeing what's playing: Check the status of current playback and next items in the playlist.
7	Should allow grouping/division of the network in groups for ease of publishing: If you want to play the same content on 50 different locations, assign them to a group and schedule the whole group together, no need to add the schedule for 50 locations individually.
8	Should support pulling content from FTP server.
9	Capability for Multiple Scheduling Options: Playlist and Time-Based Scheduling - Control what to play when.
10	Playback status/proof of playback of any player (as Reports).
11	Should have Built-in database for easy back-end management of content & player databases and exporting them.
12	Should allow Smart publishing of content. The already sent content needs not to be transferred again, only the changes will be transferred automatically.
13	Should allow for addition of Multiple Players: Add multiple players of his network in one go.
14	Should have an Administrative panel for Password management and e-mail triggering.
15	Should show live Machine Health: Be aware of how much system is being used Hard Disk space/Memory and other critical Hardware and Software Statistics.
16	Should allow to Pre-Transfer Content: Files used for designing the layout can be transferred in the background while the layout is being designed hence saving your time.
17	Should have the capability for Intelligent File Transfer technology: Automatic resume of downloads from the point where it was disconnected. If the content files are reused in multiple presentations, they will be transferred only once.
18	Complete Player Control: Remotely control when to sleep/hibernate/switch on/off the system or monitor at specific time of day.
19	Remotely execute RS232 commands on the media players to manage hardware.
20	Add files to the playlist that are in the player but not on the server.
21	Alerts on content scheduler on Showing emergency/ alert messages, overriding the playback schedule.
22	Should have capability on Filter Campaign View for quick overview of player activity
23	Manage and specify shutdown/sleep/hibernate/wake-up time for the media players remotely.
24	Servers Watchdog reporting
25	Centralized control center for all the systems and content.
26	Control Panel Dashboard: View live screenshot of all the installed sites in one go.
27	Different content should be targeted to individual screens
28	Content should be targeted to category or group of screens
29	Proof of playback reports
30	Should have the software allow customized proof of playback repots as per playlist

31	Should have the Proof-of-Playback Reporting available in XML/pdf Format
32	Should have capability to be scalable and be able to support a large network of screens which can increase with time
33	Should have capability scheduler software have a proven track record in digital signage for at least 5 years or more.
34	Should have capability support standard UDP (Universal Data Protocol)/ TCP (Transmission Control Protocol)/ IP (Internet Protocol)/ FTP (File Transfer Protocol) protocols.
35	Should have capability to work the given software work on Internet / LAN/WAN/ Broad bands
36	Should have capability to allow creation of a pattern based on week days or month
37	Should allow option to schedule distribution of playlist at user defined time schedule (for example - from 9 p.m. to 6 a.m. so that the content will be distributed at defined time only)
38	Should allow advanced scheduling (Content scheduled to be played on the screen up to years/months/weeks in advance.)
39	Should have capability to send remote commands should be targeted to individual screens or group of screens or all the screens as per user choice
Digital Signage Player	
1	Should have logging of different types like hardware Health and log views
2	Capability for Internal Caching of Data: If the internet gets down, all the external data requests will be fulfilled by the internal Cache. The internal cache is updated every time new data is found.
3	Capability for Live TV Playback: Player needs to fetch internal/local Live TV feeds and needs to be played as per the schedule given by CM along with local signage content.
4	Should have Self-healing mechanism: Player keeps on monitoring the network status of the system, and automatically updates itself on any change in the network or recover from any software level fault
5	Secure and Encrypted communication: All the communication with the scheduler is done on a secure channel.
6	Password Protected access: The access to player (schedules, content and logs) is password protected. If the scheduler doesn't have the right password for the player, the player is completed locked from access.
7	Smart download: Content can be transferred to the player remotely by scheduler or it can be uploaded to an online ftp server. The player automatically checks if the required content necessary to play the presentation is available locally, or else downloads the content from the internet at the background.
8	Should have the capability for Real-time rendering of output at time of playback.
9	Should have the capability for all sizes of resolution and content Scaling: Players can render in any standard aspect ratio or custom defined aspect ratio.
10	Should be able to receive remote commands from server including custom serial commands.
11	Should be able to remotely control the devices attached to players via RS 232.
12	Should be able to act as a local content repository/FTP In case of Multiple Players at one site.
13	Should be able to play the content during content Downloading /distribution from server.
14	Should automatically adjust the display according to the resolution of content.
15	Should allow the authorized and encrypted server to interrupt and remove live running campaigns on players within seconds.
16	Should support multiple Display options: VGA, DVI, HDMI, Display Port
17	Capability to avoid re-download of existing asset/media file
18	Multi language input and display support.
19	Clearing of Old unused files after a pre-defined time period from the clients (Digital Media Player).
20	Media player should be capable of playing multiple videos /live videos/ images/text crawls/ webpages, etc.

21	Media Player Technical specification: Windows 10 IoT Enterprise LTSB ("Windows 10 Embedded") CPU: Intel Celeron N3160 1.60GHz (quad-core) Graphics: Intel HD Graphics 400 Video: One HDMI 1.4b port with cable retention screw, Display Continuity button Memory: 4GB DDR3L RAM (dual-channel) Storage: 64GB SSD storage Network: One gigabit Ethernet port, wireless 802.11 a/b/g/n/ac Wi-Fi USB: Four USB 3.0 Type A ports Serial: One DB9 port Housing: Anodized aluminum, fanless Minimum Dimensions: 190 mm x 160 mm x 25 mm Operating Temp: 0°C to +40°C Storage Temp: -55°C to +75°C Mean Time Between Failures (MTBF): > 50,000 hours

Non-Functional requirements

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR-VMS 1.0	Variable Message Signboard	Non Functional requirement	Security	Required levels: Administrator, Content creator, content manager, billing, view.
NFR-VMS 1.1	Variable Message Signboard	Non Functional requirement	Security	Administrator: Full admin access to all components and functionality. Content Creator: access to create new digital signage layouts, signage groups, channels, upload new advertiser content, create city content, css feeds, etc., no hardware or firmware or system configuration changes. Content Manager: access to schedule advertiser and city content across all channels. Billing user: access to run advertiser reports for billing purposes. View user: view only access to content (i.e. signage / advertising end-point)
NFR-VMS 1.2	Variable Message Signboard	Non Functional requirement	Security	Access permissions changed by administrators on instruction of applications owner(s)
NFR-VMS 1.3	Variable Message Signboard	Non Functional requirement	Security	If passwords are not managed through active directory - User Passwords must be eight characters long and contain numerals, special characters and letters (upper and lower case). Passwords must be unique to each user. Admin passwords must be unique to each administrator. All passwords must be changed every 90 days.
NFR-VMS 1.4	Variable Message Signboard	Non Functional requirement	Security	Must comply with enterprise-wide IT application security. No special requirements
NFR-VMS 1.5	Variable Message Signboard	Non Functional requirement	Security	Billing content must be backed up every 24 hrs. Advertiser and city content must be backed up at the start of each campaign cycle or every 24hrs unless no changes have been made. System configuration must be backed up before and after every configuration change. All backups to be stored securely as per IT / Data security policy
NFR-VMS 1.6	Variable Message Signboard	Non Functional requirement	Security	128-bit AES encryption or HDCP 2.0 is required on all data passed between devices
NFR-VMS 1.7	Variable Message Signboard	Non Functional requirement	Audit	Advertising data for billing purposes must maintain full audit trail, number of displays, no of times content shown, time of day content shown, time content shown for - for each advert / advertiser
NFR-VMS 1.8	Variable Message Signboard	Non Functional requirement	Audit	Audit trail for static and time-based (video) advertising content
NFR-VMS 1.9	Variable Message Signboard	Non Functional requirement	Audit	Storage capacity should be four times contemporaneous requirement. This allows for the previous content, current content and the next content to be queued up, as well as billing and audit data.
NFR-VMS 1.10	Variable Message Signboard	Non Functional requirement	Audit	Signage software must be exposed to data from all required sources, i.e. IPTV, broadcast video, VOD, IIS, CSS, web.

Requirement ID	Domain	Business Topic / Application / Module Name	Sub-Module / Functionality	Short Description
NFR-VMS 1.11	Variable Message Signboard	Non Functional requirement	Availability	Software duty cycle: 24/365 (h/d)
NFR-VMS 1.12	Variable Message Signboard	Non Functional requirement	Availability	Planned maintenance must be carried out to minimize periods of unavailability i.e. during periods where the fewest advertising viewers are present. Systems must be segregated so for maintenance in to different areas so the whole platform is not taken down for maintenance
NFR-VMS 1.13	Variable Message Signboard	Non Functional requirement	Availability	Signage content is required citywide. Admin access should be from any display point and any point on the signage VLAN (WAN/LAN)
NFR-VMS 1.14	Variable Message Signboard	Non Functional requirement	Reliability	Signage software should be fully redundant / clustered to ensure high availability
NFR-VMS 1.15	Variable Message Signboard	Non Functional requirement	Reliability	Maximum 4 hours for break fix during operational times, for partial loss of availability.
NFR-VMS 1.16	Variable Message Signboard	Non Functional requirement	Usability	Look and Feel to be defined by dashboard admins / designers / content creation users / advertising content providers - this is a highly subjective topic. Framework must be flexible to allow advertisers to leverage the system without unnecessary design constraints
NFR-VMS 1.17	Variable Message Signboard	Non Functional requirement	Usability	Signage platform must support multi-lingual content with different character sets
NFR-VMS 1.18	Variable Message Signboard	Non Functional requirement	Documentation	Full documentation is required to be handed over. This includes specification of every application used, its maintenance, its revision version and IP address table(s). Operations and Maintenance manual must be provided including back-up frequency, updates calendar (where known), original installation files and license keys. Configuration data book is required for all application and configuration of software, back-up and recovery data must be provided.
NFR-VMS 1.19	Variable Message Signboard	Non Functional requirement	Documentation	In addition to knowledge base, manufacturers operations manuals must be provided
NFR-VMS 1.20	Variable Message Signboard	Non Functional requirement	Documentation	In addition to user guides and quick start manuals, manufacturers' operations manuals must be provided. Train the trainer materials will be required

3.4. Project deliverables / Documentation

MSI needs to prepare and share system/user documents, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents includes:

Sr. No.	Key Activities	Deliverables
1	Project Kick-Off	- Project Plan - Risk Management & Mitigation plan template - Project progress report template
2	Team mobilization	
3	Assess the requirement of IT and Non-IT infrastructure	
4	Assessment of Business process	- Functional Requirement Specification document (FRS-updated) - System Requirement Specification document (SRS) - Requirements Traceability Matrix (RTM) - RACI Matrix
5	Assessment of Functional as well as Software requirements	
6	Assess the Integration requirement	
7	Assess the connectivity requirement for all locations (including internal requirements for all relevant/DICDL buildings)	Site Survey report
8	Assessment of Network laying requirement	
9	Assessment of Training requirement	
10	Solution Architecture	- Bill of Quantity/Material (BoQ & BoM) - HLD documents - LLD documents - Solution/Application architecture documents - Technical Architecture documents. - Network Architecture documents. - ER diagrams and other data modeling documents. - Database design documents (Logical & physical database design) - Data dictionary and data definitions - GUI design (screen layout, workflow, navigation, etc.) - Test Plans, test cases, etc. - Standard operating Procedures (SoPs) - Change management Plan
11	Detail drawings (technical)	
12	Detailed design of Smart City components/solutions	
13	Prepare and sharing of test cases (Unit, System Integration and User Acceptance)	
14	Preparation of Bill of Quantity and material (BoQ & BoM)	
15	Standard operating Procedures (SoP) for system design and implementation	
16	Helpdesk setup	
17	Physical Infrastructure setup	
18	Supply of proposed hardware/equipment's, edge devices, COTS software (if any), Licenses, etc.	
19	Installation and commissioning of IT & Non-IT Infrastructure	
20	Development, Testing/Staging and Production environment setup	- Installation & Commissioning report for IT & Non-IT Infrastructure - Setting up of IT application on development as well as staging/testing environment for demo/testing purpose - System Manual - Installation manual for hardware/software installation and commissioning - Test cases - Test reports (Unit testing, regression testing, UAT, etc.) 3rd party Auditor/Testing reports and certification (STQC/Cert-In) - System design documents (SDD's) - Data flow diagrams (DFD)
21	Design and development of software application (customization)	
22	Design and development of bespoke application (if any)	
23	Data digitization (if any) & Data migration	

Sr. No.	Key Activities	Deliverables
24	Integration with Third party services/application	• UAT and closure of UAT observations report • Training completion report (department wise) • Application deployment and configuration report • STQC/Cert-In Certificate for application as well as security testing by 3rd party auditor • Inspection and testing procedures manual including QA Policy as per STQC framework and procedures for the software/hardware equipment's
25	Testing (Unit, System, Integration, User acceptance testing, etc.)	
26	Implementation/deployment of solution	
27	Prepare and sharing of User manuals, training curriculum & training materials	
28	Generic as well as role based training for various Smart city solutions to be deployed across the city	
29	SoP Implementations	
30	Integration with smart city components (SCADA, GIS, Smart meters, sensors, etc.)	• Integration Testing report
31	Integration with Command and control center	
32	System Go-Live	• Go-Live report
33	Operations and Maintenance phase	• Detailed plan for monitoring of SLAs and performance of the overall system • Fortnightly/Monthly Project Progress Report • Monthly SLA Monitoring Report and Exception Report (EMS) • Quarterly security Report from EMS along with detailed analysis • Issues logging and resolution report from CRM system as well as from EMS. • Source code versioning document
34	SLA & performance monitoring	
35	Logging, tracking and resolution of issues in timely manner	
36	Application enhancement	
37	Patch deployment & version upgrades	

- MSI also need to prepare and share a process document in accordance with the ISO 9001 standard; containing all the process being carried out during the entire tenure of the project and share the same with authorized officials at DSIR.
- Any other document(s) deemed necessary for implementation, operation and maintenance of the overall system.
- MSI needs to ensure upkeep & updating all documentation and manuals on periodic basis and should be shared with DSIR as and when requested by the authorized officials.
- In addition to the training to the operations staff during acceptance stage, the MSI shall conduct half-yearly training refreshment sessions to train the new staff inducted by DICDL and to enhance the knowledge of the DICDL's staff operating the DSIR smart city ICT components by adopting the "Train the trainer" approach.

3.5. Training and capacity building

To strengthen the DICDL staff which will be deployed at DSIR, structured capacity building programs shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to be given to the staff for pre-defined period. Additionally, refresher trainings for various domain activities related to the operations of Command Control Centre, City Operations, Data center and Disaster recovery site, MIS, dashboards, ERP as well as other utility systems, etc. shall be a part of Capacity Building for DSIR staff.

Considering the criticality of the work being carried out by staff deployed at CCC, utility systems, emergency response center, etc. it becomes important for DSIR as well as the MSI to understand their training needs and design a training plan as well as training material to be provided to each staff personnel at DSIR. These officers shall be handling emergency situations with very minimal turnaround time. Following are the indicative guidelines, which may be expanded and designed as per the requirement of the DSIR smart city project in future as and when required.

- Train the trainer: Training for all the courses on learning management system/platform needs to be provided by the MSI.
- MSI shall prepare and submit detailed Training Plan and Training Manuals to the authorized officials for review and approval.
- Appropriate training shall be carried out as per the User Training Plan prepared in detail for 48 nos. participants of batch size 16 and 3 nos training per quarter needs to be carried out over the period of 2 years post implementation, including but not limited to course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
- MSI shall be responsible for setting up of necessary demonstration environment including setup of required infrastructure, classrooms, internet connectivity to connect to staging/training server, Kiosk, etc. to conduct end user training. End user training shall be conducted at a centralized location or any other location as identified by MSI and being agreed/approved by authorized officials at DSIR.
- MSI shall conduct end user training and ensure that the training module holistically covers all the details around system applications (ERP system, Workflow process, CIOC, Surveillance, etc.) which is expected to be used by various DICDL officials day-to-day to run the system.
- MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the comprehensive system designed and implemented at DSIR.
- MSI needs to have a dedicated trainer for various modules rather than a generalist/functional analyst to provide module/application specific training to all the users at DSIR.
- Training needs to be imparted in English as well as regional language (Gujarati/Hindi) as per the requirement of the trainees/users and as agreed by authorized officials of DSIR.
- MSI needs to prepare solution/domain/application specific training manuals and submit the same to authorized officials at DSIR for their review and approvals. Training Manuals, standard operation procedures, etc. needs to be provided in English/other language as requested by DSIR officials.
- MSI needs to provide Computer based training (CBT) materials for all the applications/modules being developed and implemented from their end on the intranet for reference of the departmental users. CBT should be prepared in languages (English & Gujarati/Hindi) agreed between DSIR & MSI team.
- MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
- MSI needs to chalk out an annual training calendar and shared with authorized officials of DSIR along with complete details of content of training, target audience for each year, training locations, etc. The said training calendar needs to be agreed and approved by authorized officials at DSIR.
- MSI needs to update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments carried out in the system.
- In addition to the above, while designing the training courses and manuals, MSI needs to take due care in imparting training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.

- Types of Trainings: Following training needs is identified for all the project stakeholders:
 - Functional Training: This training should focus on the usage of application software so that the users are aware of all the operations of the application systems, ensuring a smooth run of Citizen Services or Departmental Operations. It should be covered for each of the functional module/application.
 - Administrative Training: This training should focus on the administration of Application Software and Server Infrastructure and should be imparted to the IT Department staff. The said training should be chalked for;
 - System Administration Helpdesk, FMS, BMS Administration etc.
 - Master trainer assistance and handling helpdesk requests etc.
 - Senior Management Training:
 - Usage of all the proposed systems for monitoring, tracking and reporting,
 - MIS reports, accessing various exception reports,
 - Dashboards, Analytics, etc.
- Post-Implementation Training: MSI needs to provide refresher training to a particular percentage of resources/users which will be deployed at different departments (personnel movement via different means) over a period of time. For them various training which needs to be provisioned are;
 - Refresher Trainings for the Junior/Senior Management
 - Functional/Operational training for new clerks/operators
 - Refresher courses on System Administration
 - Change Management programs

3.6. Standards

The MSI shall ensure adherence to the reference standards as well as applicable international standards during all the stages. (indicative list but not limited to)

Sr. No.	Standard Name	Standard Reference / Information
1	ISO/IEC 20000-1:2011	Information Technology - Service Management System (SMS) Standard
2	SOAP	Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured Information in the implementation of web services in computer networks.
3	REST	REST: (Representational State Transfer) is a software architecture style consisting of guidelines and best practices for creating scalable web services.
4	ISO/IEC 27000	Information Security Management Systems (ISMS)
5	ITIL	Information Technology Infrastructure Library
6	ISO/IEC Telecom Room 8802-1.43125	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 1: Overview of Local Area Network Standards
7	ISO/IEC 8802-2:1998	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks –Specific requirements – Part 2: Logical link control
8	ISO/IEC/IEEE FDIS 8802-1X	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks –Part 1X: Port-based network access control

Sr. No.	Standard Name	Standard Reference / Information
9	ISO/IEC 13236:1998	Information technology – Quality of Service (QoS): Framework
10	IEEE 802.1ad	Virtual Local Area Network (VLAN) Stacking
11	IEEE 802.1D-1998 STP	Bridging (Media Access Control Bridges)
12	IEEE 802.1p	Class of Service (CoS)/QoS
13	IEEE 802.1Q VLANs	Virtual Bridged Local Area Networks
14	IEEE 802.1s MSTP	Multiple VLAN Spanning Tree
15	IEEE 802.1x	Port-Based Authentication
16	Extended 802.1x	Authenticated VLAN (multiple MAC, multiple VLANs per port)
17	IEEE 802.1v	Protocol VLANs
18	IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
19	IEEE 802.3ab The IEEE 802.3ab Standard	Specifications for the 1000BASE-T twisted-pair Giga Ethernet
20	IEEE 802.3ac	VLAN tagging
21	IEEE 802.3ad	Link Aggregation (Dynamic)
22	IEEE 802.3ae	10-Gigabit Ethernet
23	IEEE 802.3ba	40-Gigabit Ethernet
24	IEEE 802.3af	Power over Ethernet (PoE)
25	IEEE 802.3x	Ethernet flow control
26	IEEE 802.3u The IEEE 802.3u	Standard describes the specification 100BASE-TX, and 100BASE-FX Ethernet
27	IEEE 802.3z The IEEE 802.3z	Standard describes the specifications for the 1000BASE-X fiber optic Gigabit Ethernet
28	UL	Fixed Camera, PTZ Camera, Fixed Dome Camera
29	FCC	Fixed Camera, PTZ Camera, Fixed Dome Camera, PTZ Camera Housing
30	IEEE 802.3	RJ45 Ports
31	ONVIF/PSIA	Video Management Software, All CCTV Cameras
32	IP-66	Fixed Camera, PTZ Camera, Housing
33	IP-65	Field Junction Box, Industrial Switches, etc.
34	International Electro-technical Commission (IEC)	Power Cables
35	Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA) 568	Category 7 Ethernet Cable
36	RFC 3261	SIP: Session Initiation Protocol
37	RFC 3262	Reliability of Provisional Responses in SIP
38	RFC 3264	An Offer/Answer Model with SDP
39	RFC 3311	UPDATE method
40	RFC 2976	The SIP INFO Method
41	RFC 3711	The Secure Real-time Transport Protocol(SRTP)
42	RFC 4568	SDP: Security Descriptions for Media Streams
43	G.711	G.711 is a narrowband audio codec that provides toll quality audio at 64 Kbit/s
44	G.728	G.728 is an ITU-T standard for speech coding operating at 16 Kbit/s.
45	G.729	The G.729 codec compresses the payload to 8kbit/s
46	H.264	Advanced video coding for generic audiovisual services
47	H.263	H.263 is a video compression standard originally designed as a low-bit-rate compressed format for videoconferencing.

Sr. No.	Standard Name	Standard Reference / Information
48	H.235	H.235 covers security and encryption for H.323
49	H.239	H.239 is the ITU standard for a second video channel
50	H.460	H.460 is a firewall traversal recommendation that accompanies the H.323 set of ITU standards for multimedia communication over packet networks.
51	H.323	H.323 is a recommendation from the ITU that defines the protocols to provide audio-visual communication sessions on any packet network.
52	SIP	Signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks
53	LTE	Long-Term Evolution (LTE)
54	Air Interface	TETRA according EN 300 392-2
55	RF Specifications	TETRA according EN 300 394-1
56	ISO 27001:2013	Information technology — Security techniques — Information security management systems
57	ISO 27002:2013	Implementation of related Code of practice for Information Security controls need to be referenced for ISO 27002: 2013 certification standard.
58	NIST	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4
59	CIS Benchmarks	A set of configuration guidelines for various technologies

3.7. Bill of Quantity

The Bidder should provide the proposed bill of Quantity (BoQ) here. Bidders are required to mention the details of the make/brand and model against each line item, wherever applicable. The bid can be considered non-responsive in the absence of such details. Once the bidder provides this information in the submitted bid, the bidder cannot change it with any other component / equipment etc. of lower specifications/ performance; it can only be upgraded at the time of actual deployment/ installation. The Bidder may add any additional line item (with adequate details) in the proposed BoM table below (towards the end of the table) in each work package, that may be required to fulfill the RFP and project requirements in totality.

The Bidder shall quote only one specific make and model from only one specific OEM, for each of the goods.

Mentioned below is the indicative Bill of Quantity work package wise for each proposed solution; however, MSI is required to assess the exact requirement based on entire scope mentioned in the RFQ cum RFP and the draft form of contract, location wise, for all the proposed solution components and shall accordingly provide requisite quantities and size the hardware and software infrastructure requirement within the total bid price, without any additional cost to employer. **Bidder shall submit the Financial Bid only on the online portal i.e. www.nprocure.com**

Sr. No.	Line Item	Unit of measurement	Indicative Qty	Proposed Qty	Make	Model	Full Compliance with RFP requirements (Y/N)
Work Package - 1 Basic Infrastructure							
Network passive- Back-bone							
1	Supply of 144 core armored FO cable, single mode, G652 D with FO splice closures with complete accessories along with supply and Laying of warning tape, pull thru chambers, splice chambers, protection materials, Electronic route locators, earthing of armored FO cable, etc.	Mtr.	14000				
2	Supply and Laying of 12 way (40 mm OD) ducts along with survey, excavation and resurfacing Up to 1.5 Mtr. in all kind of soil and surface (open cut /HDD) as per standards with required accessories	Mtr.	14000				
3	Supply of rack in server room and Primary POP (42U)	Nos.	12				
Network passive- Distribution							

4	Supply of Unarmored 144 F FO cable, single mode, G652 D along with LIU and FO splice closures with complete accessories.	Mtr.	12000				
5	Supply of racks in service areas (42U)	Nos.	6				
Network passive - Access: CCTV							
6	Supply of Fiber patch panel (fully loaded), with complete accessories	Lump sum	As per requirement				
7	Supply of 144 F Fiber with complete accessories (FTTx)	Mtr.	45000				
8	Supply of cat 6 patch cable	Nos.	As per requirement				
9	Supply of Splice closure (fully loaded)	Nos.	As per requirement				
10	Patch chords, 1 Mtr length	Nos.	As per requirement				
11	Patch chords, 5 Mtr length	Nos.	As per requirement				
Network passive - Accesses: VMS, poles, sensors, etc.							
12	Supply of Fiber patch panel (fully loaded), with complete accessories	Lump sum	As per requirement				
13	Supply of cat 6 patch cable	Nos.	As per requirement				
14	Supply of Splice closure (fully loaded)	Nos.	As per requirement				
15	Patch chords, 1 Mtr length	Nos.	As per requirement				
16	Patch chords, 5 Mtr length	Nos.	As per requirement				
Network Active							
17	Server Room Core Router	Nos.	2				
18	Internet Router	Nos.	2				
19	Server Room WAN Switch	Nos.	2				
20	Network Firewall (NGFW)	Nos.	2				
21	Server Room Core Switch	Nos.	2				

22	Server Room Access Switch	Nos.	6				
23	SA Distribution Device/Switch	Nos.	14				
24	SA Access Switches (PoE+)	Nos.	21				
25	Blade Chassis and management	Nos.	As per requirement				
26	Blade Servers	Nos.	As per requirement				
27	Network Access Control & Authentication System	Nos.	2				
28	Backup Solution	Nos.	1				
29	SAN Switch	Nos.	2				
30	Unified NAS with NL-SAS (1 PB)	Nos.	1				
31	Unified Backup Storage (250 TB)	Nos.	1				
32	Industrial Ethernet Switch (Industrial Grade)	Nos.	20				
33	Database licenses	Nos.	As per requirement				
34	OS licenses	Nos.	As per Requirement				
35	UPS (sizing as per proposed solution)	Nos.	2				
36	Rodent Repellent system	Nos.	1				
37	Variable Message Signboard server	Nos.	1				
38	End Point Security Solution (Enterprise)	Nos.	1				
39	Air Conditioning (as per proposed solution)	Nos.	As per requirement				
Enterprise Management System & Network Management System							
40	Enterprise Management System & Network Management System	Lot	1				
City Wide Sensors							
41	Gas level Monitoring	Nos.	1				
42	Wind Speed Monitoring	Nos.	1				
43	Environmental Sensor (Rainfall & Noise Pollution & Air Quality Monitoring)	Nos.	1				
44	Metrological data sensor	Nos.	1				

City Integrated Operations Platform							
45	Integration Platform: SCADA, CEPT, WTP, Gas, Utilities, etc. - Integration services, - Data Normalization/IoT Software, - City Mobile application, - Analytics Engine with visualizations (BI/Analytics) - Reporting tool, - Video integration module - City Operation software - Notifications, Alerts & Alarms - Standard Operating Procedure - Social Media - Intelligence Support - Policies & Events - Dashboard & Reporting - Monitoring & Control	Lot	1				
46	Any Other Item						
Work Package - 2 City Applications							
ERP System							
1	HR Management	Lot	1				
2	Payroll Management						
3	Finance Management						
4	Projects & Works Management						
5	Asset Management						
6	Contracts & Inventory Management						
7	Industry specific solutions for utilities						
8	CRM						
9	Process workflow						
10	Master Data Governance						
Multi Service Kiosk							
11	Multiservice Kiosk	Nos.	2				
Common applications							
12	Web Portal	Nos	1				

13	Mobile Application/platform	Nos.	1				
14	Any other item						
Work Package - 3 Integrated Operations							
Surveillance							
1	Box Camera with required accessories (e.g. Power supply, IR illuminator, cables etc.)	Nos.	24				
2	PTZ cameras	Nos.	17				
3	Video Management Software + Analytics	Nos.	1				
4	Recording Server	Nos.	As per requirement				
5	Database/Management Server	Nos.	As per requirement				
CIOC Setup							
4	Site Preparation (furniture) covering Cubicles with Table and Chair for operators, Partitioning, Enclosures, Earthing, Power Cabling, Interiors, etc. for 50 Seating capacity	Nos.	50				
5	2 Screen –Operators Client Workstations for Command Control Centre.	Nos.	15				
6	Video Wall Solution with 70 inch or more display Cubes (4x2 – 1 nos. & 6x3 – 1 nos.) with Controller and required Software	Nos.	2				
7	Indoor LED display for public (3000 mm x 1700 mm or higher)	Nos.	1				
8	Camera Type 3 - Dome Camera mounting arrangements/accessories for Command Center & DC	Nos.	10				
9	Command Centre Site Preparation covering Partitioning, False flooring, cooling, access control system, etc.	Nos.	1				
10	Codec based VC System	Nos.	2				

11	Helpdesk Solution, IPBX System	Nos.	1				
12	Video Conference System with collaborative display	Nos.	1				
13	IP Phones	Nos.	25				
14	IP Phones with Display	Nos.	10				
15	Headsets for operators with built in mic	Nos.	20				
16	Multifunctional keyboard with touchscreen panel screen	Nos.	2				
Integrated Building Management System (IBMS)							
17	IBMS Integration Software	Nos.	1				
Variable Message sign boards							
18	Variable Message Sign Application	Nos.	1				
19	Variable Message Sign Boards on Road (Minimum Display size: 25 Feet x 9 Feet)	Nos.	4				
20	Any other item						
21	ISO 27001 and ISO 20000 certification during O&M Phase	Lot	As per requirement				

3.8. Technical Specifications:

Unarmored Fiber Optic Cable:

Mechanical Characteristics of cable:		
Sr. No.	Parameters	Nominal Values
1	Min. Bending Radius (short term)	20D
2	Min. Bending Radius (long term)	10D
3	Max. Tensile Strength-Short Term	1000N
4	Max. Crush Resistance-Short Term	1000N/10 cm
5	Sheath	HD Polyethylene (UV Stabilised) 1.8mm thickness
6	Impact Load	4.4 Nm
7	Flex Cycles	25 cycles of mechanical flexing (as per FOTP -104)
8	Armoring	Yes
9	Outer Jacket Material	UV Proof High Density Polyethylene (HDPE), Anti-Rodent
10	Water Blocking material	Water blocking yarn and Water-blocking tape

11	Central Element	Dielectric
12	Fiber per cable	48 / 96 / 144
12.1	Fiber Count per Tube	48 OFC : 4 cores per tube 96 OFC: 12 cores per tube 144 OFC: 12 cores per tube
13	Installation Temperature	0° to +60° C
14	Operating Temperature	-40° to +60° C
15	Cable OD	Max 16mm
16	Weight kg/km	Approx. 162± 10 kg/km
17	Jacket thickness nominal	1.8 mm minimum
18	Armouring	Copolymer Laminated Steel
19	Fibre Core diameter@1310nm	9+/- 0.4 µm
20	Fibre Category	OS2 G652D (meet ITU G.657.A1 requirements) (ECCS Tape)
21	Cladding Non-Circularity	≤ 0.7%
21.1	Cladding diameter	125 ± 1.0 µm
21.2	Coating Diameter	242 ± 5mm
22	Effective Group Index of refraction	1.4676 @ 1310nm ; 1.4682 @ 1550 nm
23	Core/Cladding Concentricity	≤0.5 µm
24	Mode Field Diameter	8.6 ± 0.4 mm @ 1310 nm
25	Minimum Proof Strength	> 100Kpsi
26	Max. Attenuation	0.34 dB/km @ 1310 nm; 0.20 dB/km @ 1550 nm
27	Max. Average Attenuation	0.33 dB/km @ 1310 nm; 0.20 dB/km @ 1550 nm
28	Attenuation Discontinuity	Both Windows <0.10dB
29	Numerical Aperture	0.14
30	Approvals	ISO.IEC 11801 - 2nd Edition, type OS1/OS2; AS/ACIF S008; AS/NZS 3080; ITU-T REC G 652D spec for Low Water Peak fibre
31	Strength Member	Single sheath Wet tube & Dry core type FRP as Central strength member

Armoured Fiber Optic Cable

Mechanical Characteristics of cable:		
Sr. No.	Parameters	Nominal Values
1	Maximum pulling tension (MPT)	2700 N
2	Maximum Tensile Loads	Short Term : 2700 N ; Long Term : 890N
3	Minimum bend radius, no load	10 times the cable outside diameter
4	Min bend at max pulling tension	15 times the cable outside diameter
5	Crush Resistance	3000 N / 10cm
6	Impact Load	4.4 Nm
7	Flex Cycles	25 cycles of mechanical flexing (as per FOTP -104)
8	Armoring	Corrugated steel tape armor
9	Outer Jacket Material	Medium Density Polyethylene (MDPE)
10	Water Blocking material	Water-swell able tape/ jelly
11	Central Element	Dielectric

12	Fibers per cable	144
13	Installation Temperature	0° to +55° C
14	Operating Temperature	0° to +55° C
15	Cable OD	Max 17.5 mm (144F)
16	Weight kg/km	Approx. 250± 10 kg/km
17	Jacket thickness nominal	1.3 mm
18	Aarmor thickness nominal	0.25 mm

Optical Characteristics of fiber:		
Sr. No.	Parameters	Nominal Values
1	Fiber Core diameter	8.2µm
2	Fiber Category	OS2 G652D
3	Cladding Non-Circularity	≤ 0.7%
4.1	Cladding diameter	125 ± 5µm
4.2	Coating Diameter	242 ± 5µm
5	Effective Group Index of refraction	1.4676 @ 1310nm ; 1.4682 @ 1550 nm
6	Core/Cladding Concentricity	≤0.5 µm
7	Mode Field Diameter	8.6 ± 0.4 µm @ 1310 nm
8	Minimum Proof Strength	> 100Kpsi
9	Attenuation	< 0.34 dB/km @ 1310 nm <0.22 dB/km @ 1550 nm
10	Maximum Dispersion	<3.5 ps/nm-km;1285-1330 nm < 18 ps/nm-km ; 1550 nm
11	Cable Cut-off Wavelength	λ _{ccf} ≤1260 nm
12	Fiber Macro bend (1 turn @ 7.5 mm diameter)	< 0.10 dB @ 1550 nm
13	Coating Strip Force	Dry: 0.6 lbs. (3N)
14	Optical Skew	≤0.75 ns
15	PMD Coefficient	≤0.06 ps /√Km
16	Serial 1 Gigabit Ethernet	≥ 5000 m (@1310 nm)

Double Walled Corrugated DWC HDPE Pipe

Sr. No.	Parameters	Technical Details
A	General	
1	Type	HDPE
2	Construction	Double Wall Corrugated & as per IS 14930-Part II
3	Outer Diameter	40mm (+0.8 mm)

4	Inner Diameter	32mm (Min 30.0 mm)
B	Technical Details	
1	Impact Test	After the test, at 5Kg striker weight, 300 mm fall height and -5 C +/- 1 C conditioning for 2hours in cold chamber, there shall be no crack allowing ingress of light or water between inside and outside
2	Compression Test	Observed load shall be at least 450N at 5% deflection of inside Diameter
3	Bending Test	Pipe Shall not flatten at a minimum bending radius of 1100 mm. A Sphere of Diameter 95% of declared ID of pipe should pass through it smoothly.

Server Room Core Router:

Sr. No.	Detailed Specifications
A	Solution Requirement
A1	The router architecture should be based on hardware based forwarding and switching. System should be multi-processor based architecture for enhanced performance
A2	The router should support traffic detection and management using QoS features and should prioritize the traffic based on L3 & L4 and apply the QOS policies
A3	Router should support the complete STACK of IP V4 and IP V6 services
A4	The Router Should provide the Redundant supervisor/Control Plane Redundancy for High Availability , There should not be any impact on the performance in the event of failure of active Control plane
A5	The router should support on line hot insertion and removal of connected modules. Any insertion line card should not require for router rebooting nor should disrupt the functionality of the system
B	Hardware and Interface Requirement
B1	Each Router should have at least 10 x 10GbE with single Mode Fiber Interfaces(SFP)
B2	Router should have management interface for Out of Band Management/ Console port/ Management port over and above ports asked in B1 above
B3	Router should be rack mountable and support side rails if required
B4	Router should have redundant power supplies
B5	Router should have hardware health monitoring capabilities and should provide different parameters through SNMP
B6	Router should support VLAN tagging (IEEE 802.1q)
B7	Router should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy(IEEE 802.3ad)
B8	Router should support for different logical interface types like loopback, GRE and IP tunnel, VLAN etc.
C	Performance Requirement
C1	The router should support minimum 100000 IPv4 and IPv6 routes entries including multicast routes
C2	The router should support should support multiple VRF instances
C3	Router should support restart for OSPF, BGP, MP-BGP etc.
C4	c. IP Routing (Static/Dynamic)
C5	d. IP Forwarding
C6	g. QoS
C7	h. ACL and Other IP Services
C8	i. MPLS with VRF Edge Routing
C9	j. IP V.6 host and IP V.6 routing
C10	The router should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
C11	System should provide basic Layer 2 WAN protocols as:
C11.1	a. GRE

C11.2	b. Ethernet
D	Layer3 Features
D1	Solution should provide basic routing feature i.e. IP Classless and default routing. Router should provide static and dynamic routing using:
D1.1	a. Static routing
D1.2	b. RIP V.2 with MD5 Authentication
D1.3	d. OSPF V.2 using MD5 Authentication
D1.4	e. ISIS using MD5 Authentication
D1.5	f. BGP V.4 using MD5 Authentication
D1.6	g. Should support route redistribution between these protocols
D1.7	h. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)
D2	Router should support for policy based routing for providing different path selection for different applications
D3	The router should reconverge all dynamic routing protocol at the time of routing update changes
D4	Router should connecting multiple MPLS service provider using multi instance routing using VRF
D5	Router should be capable to work as DHCP server and relay
D6	Router should provide multicast traffic reachable using:
D6.1	PIM-SM
D6.2	PIM-SSM
D6.3	MBGP, DVMRP or equivalent
D6.4	IGMP V.1, V.2 and V.3
D6.5	Multicast Source Discovery Protocol (MSDP)
E	Availability
E1	Router should have provisioning for connecting to dual power system
E2	Router should automatically failover of primary interface status change or remote network not reachable to the secondary link connectivity using real time parameters (IP SLA)
E3	Router should provide gateway level of redundancy in IPV4 and IPV6 using HSRP/VRRP & NHRP/equivalent for VPN
E4	Router should support information, which identifies current and trending congestion, resource utilization, traffic volume, latency, and delay.
F	Quality of Service
F1	Router system should support 802.1P classification and marking of packet using:
F1.1	a. CoS (Class of Service)
F1.2	b. DSCP (Differentiated Services Code Point)
F1.3	c. Source physical interfaces
F1.4	d. Source/destination IP subnet
F1.5	e. Protocol types (IP/TCP/UDP)
F1.6	f. Source/destination TCP/UDP ports
F2	Router should support methods for identifying different types of traffic for better management and resilience under network attacks
F3	Router should support for different type of QoS features for real time traffic differential treatment using
F3.1	Weighted fair queuing or equivalent
F3.2	Weighted Random Early Detection
F3.3	Priority queuing
F4	Router should support controlling incoming and outgoing traffic using
F4.1	a. Traffic Shaping

F4.2	b. Traffic Policing
F5	Router should support for managing congested network connectivity using:
F5.1	a. IP Precedence
F5.2	b. Ingress and Egress Rate Limiting
F6	Router should support for packet classification and fragmentation for providing end to end QoS treatment
F7	Router should support hierarchical QoS for providing granular policy per application basis for providing bandwidth provisioning and management
G	Security
G1	Router should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6
G2	Router processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
G3	Router should support for stringent security policies
G4	Router should support for external database for AAA using TACACS+ or RADIUS
G5	Router should support for multiple service provider using edge VRF
G6	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.
H	Manageability
H1	Router should support for sending logs to multiple centralized syslog server for monitoring and audit trail
H2	Router should provide remote logging for administration using:
H2.1	a. Telnet
H2.2	b. SSH V.2
H3	Solution should support for capturing packets for identifying application performance using remote port mirroring for packet captures or should support netflow/Jflow
H4	Router should support for management and monitoring status using different type of Industry standard NMS using:
H4.1	a. SNMP V1 and V.2
H4.2	b. SNMP V.3
H4.3	c. Filtration of SNMP using Access list
H4.4	d. SNMP MIB support for QoS
H5	Router should support for basic administrative tools like:
H5.1	a. Ping
H5.2	b. Traceroute
H6	Router should support central time server synchronization using Network Time Protocol NTP V3 and V.4
H7	Router should support for collecting real time traffic statistics for analysis and troubleshooting using Netflow or Ipfix or equivalent
H8	Router should support for providing MIB support for different statistics of the LAN and WAN interface
I	IPv6 features
I1	Router should support IP V.6
I2	Router should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as:
I2.1	b. OSPF V.3
I2.2	c. BGP with IP V.6
I2.3	d. IP V.6 Policy based routing
I2.4	e. IP V.6 Dual Stack etc.
I2.5	f. IP V.6 Static Route

I2.6	g. IP V.6 Default route
I2.7	h. Should support route redistribution between these protocols
I3	Solution should support different types of IPv6 tunneling mechanism, such as:
I3.1	IPv6 to IPv4 tunnels / IPv4 to IPv6 tunnels
I3.2	IPv6 over IPv4 tunneling
I4	Router should support different types of multicast routing in IP V.6 network using:
I4.1	a. PIMv2 Sparse Mode
I4.2	2. PIMv2 Source-Specific Multicast
I5	Router should support for QoS in IP V.6 network connectivity
I6	Router should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:
I6.1	a. SNMPv1, SNMPv2c, SNMPv3
I6.2	b. SNMP over IP V.6
I7	Router should support syslog for sending system log messages to centralized log server in IP V.6 environment
I8	Router should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
I9	Router should support for IP V.6 different type of application usage like:
I9.1	a. HTTP
I9.2	b. HTTPS
I9.3	c. ICMP
I9.4	d. TCP/UDP
I9.5	e. DNS lookup
I9.6	f. DHCP
I10	Router should support for IP V.6 different types of tools for administration and management such as:
I10.1	a. Ping
I10.2	b. Traceroute
I10.3	c. VTY
I10.4	d. SSH
I10.5	e. TFTP

Internet Router

Sr. No.	Detailed Specifications
A	Solution Requirement
A1	The router architecture should be based on hardware based forwarding and switching. System should be multi-processor based architecture for enhanced performance
A2	The router should support traffic detection and management using QoS features and should prioritize the traffic based on L3 & L4 and apply the QOS policies
A3	Router should have facility to work as IPsec VPN Concentrator for Site-to-Site VPN
A4	Router should support the complete STACK of IP V4 and IP V6 services
A5	The Router Should provide the Redundant Supervisor/Control Plane Redundancy for High Availability , There should not be any impact on the performance in the event of failure of active Control plane
A6	The router should support on line hot insertion and removal of connected modules. Any insertion line card should not require for router rebooting nor should disrupt the functionality of the system
B	Hardware and Interface Requirement
B1	Each Router should have at least 6 x 10GbE with SM and MM Fiber Interfaces (SFP) .

B2	Router should have management interface for Out of Band Management/ console port/ management port over and above ports asked in B1 above
B3	Router should be rack mountable and support side rails if required
B4	Router should have redundant power supplies
B5	Router should have hardware health monitoring capabilities and should provide different parameters through SNMP
B6	Router should support VLAN tagging (IEEE 802.1q)
B7	Router should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy (IEEE 802.3ad)
B8	Router should support for different logical interface types like loopback, GRE and IP tunnel, VLAN etc.
C	Performance Requirement
C1	Solution should support required IPSEC tunnels
C2	The router should support multiple VRF instances
C3	Router should support restart for OSPF, BGP, MP-BGP etc.
C4	Router should support:
C4.1	a. (IPSec VPN)
C4.2	b. IPSec Encryption
C4.3	c. IP Routing (Static/Dynamic)
C4.4	d. IP Forwarding
C4.5	e. NAT
C4.6	f. QoS
C4.7	g. ACL and Other IP Services
C4.8	h. MPLS with VRF Edge Routing
C5	IP V.6 host and IP V.6 routing
C5.1	a. IPSec Encryption
C5.2	c. IPSec Idle Timeout and Dead Peer detection
C6	e. Reverse route injection
C7	The router should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
C8	System should provide basic Layer 2 WAN protocols as:
C8.1	a. GRE
C8.2	b. Ethernet
D	Layer3 Features
D1	The router should support IPSec for Secured Data transfer
D1.1	a. IPSec Data Encapsulation AH and ESP
D1.2	b. Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509)/ RSA encrypted nonces etc.
D1.3	c. Encryption Algorithm
D1.4	d. Authentication Algorithm
D1.5	e. Group: Diffie-Hellman (DH) Group 1, 2, 5
D1.6	g. Different mode of communication: Tunnel mode and Transport mode
D1.7	h. IPSec NAT Traversal
D2	Solution should provide basic routing feature i.e. IP Classless and default routing. Router should provide static and dynamic routing using:
D2.1	a. Static routing
D2.2	b. RIP V.2 with MD5 Authentication
D2.3	d. OSPF V.2 using MD5 Authentication

D2.4	e. ISIS using MD5 Authentication
D2.5	f. BGP V.4 using MD5 Authentication
D2.6	g. Should support route redistribution between these protocols
D2.7	h. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)
D3	Router should support for policy based routing for providing different path selection for different applications
D4	The router should reconverge all dynamic routing protocol at the time of routing update changes
D5	Router should connecting multiple MPLS service provider using multi instance routing using VRF
D6	Router should be capable to work as DHCP server and relay
D7	Router should provide multicast traffic reachable using:
D7.1	PIM-SM
D7.2	PIM-SSM
D7.3	MBGP, DVMRP or equivalent
D7.4	IGMP V.1, V.2 and V.3
D7.5	Multicast Source Discovery Protocol (MSDP)
E	Availability
E1	Router should have provisioning for connecting to dual power system
E2	Router should automatically failover of primary interface status change or remote network not reachable to the secondary link connectivity using real-time parameters (IP SLA)
E3	Router should provide gateway level of redundancy in IPV4 and IPV6 using HSRP/VRRP & NHRP/equivalent for VPN
E4	Router should support information which identifies current and trending congestion, resource utilization, traffic volume, latency, and delay.
F	Quality of Service
F1	Router system should support 802.1P classification and marking of packet using:
F1.1	a. CoS (Class of Service)
F1.2	b. DSCP (Differentiated Services Code Point)
F1.3	c. Source physical interfaces
F1.4	d. Source/destination IP subnet
F1.5	e. Protocol types (IP/TCP/UDP)
F1.6	f. Source/destination TCP/UDP ports
F2	Router should support methods for identifying different types of traffic for better management and resilience under network attacks
F3	Router should support for different type of QoS features for real time traffic differential treatment using
F3.1	Weighted fair queuing or equivalent
F3.2	Weighted Random Early Detection
F3.3	Priority queuing
F4	Router should support controlling incoming and outgoing traffic using
F4.1	a. Traffic Shaping
F4.2	b. Traffic Policing
F5	Router should support for managing congested network connectivity using:
F5.1	a. IP Precedence
F5.2	b. Ingress and Egress Rate Limiting
F6	Router should support for packet classification and fragmentation before applying IPSec security encryption for providing end to end QoS treatment
F7	Router should support hierarchical QoS for providing granual policy per application basis for providing bandwidth provisioning and management

G	Security
G1	Router should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6
G2	Router processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
G3	Router should support for stringent security policies
G4	Router should support for external database for AAA using TACACS+ or RADIUS
G5	Router should support for multiple service provider using edge VRF
	Router should support GRE and IPSec WAN traffic encapsulation and encryption
G6	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.
H	Manageability
H1	Router should support for sending logs to multiple centralized syslog server for monitoring and audit trail
H2	Router should provide remote logging for administration using:
H2.1	a. Telnet
H2.2	b. SSH V.2
H3	Solution should support for capturing packets for identifying application performance using remote port mirroring for packet captures or should support netflow/Jflow
H4	Router should support for management and monitoring status using different type of Industry standard NMS using:
H4.1	a. SNMP V1 and V.2
H4.2	b. SNMP V.3
H4.3	c. Filtration of SNMP using Access list
H4.4	d. SNMP MIB support for QoS
H5	Router should support for basic administrative tools like:
H5.1	a. Ping
H5.2	b. Traceroute
H6	Router should support central time server synchronization using Network Time Protocol NTP V3 and V.4
H7	Router should support for collecting real-time traffic statistics for analysis and troubleshooting using Netflow or Ipfix or equivalent
H8	Router should support for providing MIB support for different statistics of the LAN and WAN interface
I	IPv6 features
I1	Router should support IP V.6
I2	Router should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as:
I2.1	a. OSPF V.3
I2.2	b. BGP with IP V.6
I2.3	c. IP V.6 Policy based routing
I2.4	d. IP V.6 Dual Stack etc.
I2.5	e. IP V.6 Static Route
I2.6	f. IP V.6 Default route
I2.7	g. Should support route redistribution between these protocols
I3	Solution should support different types of IPv6 tunneling mechanism, such as:
I3.1	IPv6 to IPv4 tunnels / IPv4 to IPv6 tunnels
I3.2	IPv6 over IPv4 tunneling
I4	Router should support different types of multicast routing in IP V.6 network using:
I4.1	a. PIMv2 Sparse Mode

I4.2	2. PIMv2 Source-Specific Multicast
I5	Router should support for QoS in IP V.6 network connectivity
I6	Router should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:
I6.1	a. SNMPv1, SNMPv2c, SNMPv3
I6.2	b. SNMP over IP V.6
I7	Router should support syslog for sending system log messages to centralized log server in IP V.6 environment
I8	Router should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
I9	Router should support for IP V.6 different type of application usage like:
I9.1	a. HTTP
I9.2	b. HTTPS
I9.3	c. ICMP
I9.4	d. TCP/UDP
I9.5	e. DNS lookup
I9.6	f. DHCP
I10	Router should support for IP V.6 different types of tools for administration and management such as:
I10.1	a. Ping
I10.2	b. Traceroute
I10.3	c. VTY
I10.4	d. SSH
I10.5	e. TFTP

Server Room WAN Switch:

Sr. No.	Detailed Specifications
1	Minimum 16x 10G fiber ports with SFP
2	1 U Rack mountable and should provide stacking functionality
4	Should support Non-blocking architecture
5	All interfaces should provide wire speed forwarding
6	Support for at least 4k VLANs & 16k MAC address
7	It should support IGMP snooping v1,v2 & v3
8	It should have static IP routing, RIP, RiPnG, OSPF, OSPFv3, PIM and vrf lite from day 1
9	Dynamic Host Configuration Protocol (DHCP) snooping
10	Switch should support LLDP and LLDP-MED capabilities
11	Should support IP source guard & DAI
12	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 1,2,3 (SNMP v1/v2/v3).
13	Switch needs to have console port for administration & management
14	Management using CLI, GUI using Web interface should be supported
15	FTP/TFTP for upgrading the operating System
16	IEEE 802.1x support
17	IEEE 802.1D Spanning-Tree Protocol
18	IEEE 802.1p class-of-service (CoS) prioritization
19	IEEE 802.1Q VLAN
20	IEEE 802.3 10BASE-T specification

21	IEEE 802.3u 100BASE-TX specification
22	Switch should have internal redundant power supply.
23	Switch should be manageable through both IPv4 & IPv6.
24	The Switch should be EAL3/ NDPP certified.

Network Firewall (NGFW)

Sr. No	Detailed Specifications
1.	The proposed solution must allow policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling using single dashboard.
2.	The Solution must support identification and control of all types of applications (Business, Social, Encrypted and Custom) within the Network environment. It should provide detailed analysis on sessions consumed, data transferred and threats involved through the applications
3.	The proposed solution must allow free custom application signatures for Homegrown and custom applications.
4.	The solution must provide real time traffic logs based on applications and or ports. While monitoring real time traffic logs, solution must provide detailed view of Services 's application and Users, ports and IP addresses. E.g. the solution must distinguish between telnet on port 80 and http traffic between same pair of source and destinations
5.	Solution must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must not use proprietary ASIC chips.
6.	Solution must support Full tunnel, split tunnel and application specific tunnel for client to site VPNs. Solution must allow custom policies to control VPN traffic based on users, applications. It must allow different policies for different user's groups for threat (Viruses, vulnerabilities, malware) within VPN traffic.
7.	The Firewall must support application identification from day one.
8.	The solution must support Firewall, Application visibility and control, IPS, Anti-virus, Anti-malware from day one and support for URL Filtering and should be supplied with required licences
9	The solution must have always on access to the firewall. The Firewall should have inbuilt/separate hardware/Software resources for firewall access and management at all times, and must be available irrespective of load.
10	The administrator must be able to view report on the CPU usage
11	The proposed solution must support Policy Based forwarding based on:
	- Zone
	- Source or Destination Address
	- Source or destination port
	- Services or ports
12	Firewall solution should support Active/Active and Active/Passive HA and must support synchronization of the following for HA:
	Sessions
	Certificates
	VPN Security Associations
	IPS and AV sessions
	Threat and application signatures
	FIB Tables
13	The proposed solution must support different Custom IPS and Application policies for different users and groups.

14	The proposed solution must support Customized DoS protection rules.
15	Solution should support Session based or packet based load sharing over multiple equal cost paths. It should work with both static and dynamic routing
16	Solution should be capable to identify and prevent URLs that typically arrive in emails and are established only to steal information to users (Phishing attack).
17	Solution should support Session based or packet based differentiated services code point (DSCP) classification.
18	Solution must support IPv4/IPv6 based site-to-site VPN tunnels
19	Solution must support SNMP counters for logical interfaces e.g. L2/L3 sub interfaces, tunnel interfaces, LAG (802.3ad), Loopback.
20	Solution must have at least 2 virtual systems. Every Virtual system must support individual separate configuration for separate DNS entries and other service routes for access to NTP, Syslog, SNMP, Proxy, AV, IPS etc. Every virtual system must support individual routes through virtual system specific interfaces to access all these services.
21	Solution should correlate and detect hosts that have received malware, and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.
22	Solution should correlate and detect hosts that have exhibited command-and-control (C2) network behavior corresponding to malware elsewhere on the network.
23	Solution should correlate and detect a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
24	Solution should detect probable exploit kit activity targeted at a host on the network. Exploit kits should be identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
25	Solution should correlate and detect likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
26	Solution must provide change control and baseline deviation mechanisms. It must provide visibility in traffic pattern changes in last one hour, one day and compare this with last one day, one week and one month traffic patterns.
27	Solution should support dedicated on premises sandboxing for zero day and unknown malware with real time protection from day one without any additional license and the solution shall be able to provide automated signature generation for discovered zero-day threats. The solution must be able to sandbox different sizes of files as per organization needs. Solution should support file types, including: Adobe PDF, Microsoft Word, Excel, PowerPoint, Executables (EXE, COM, SCR), JAVA (Jar) etc.
28	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware
29	The solution must support minimum four level of decompression/decoding for any combination of decoding: ZIP, gzip, base64, chunked, uuencode.
30	The solution must provide the ability to block files with multi-level-encoding e.g. office files
31	The proposed solution be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2, Transparent and Tap modes
32	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance
33	The proposed solution must support validation of policy rules before rule application
34	The proposed solution must support on appliance Per policy SSL decryption for both inbound and outbound traffic.
35	The proposed Solution must support on appliance SSL decryption policy based on IP, User, web category.

36	The proposed solution shall support block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time)
37	The proposed solution should support the ability to create QoS policy on a per rule basis:
	-by source address
	-by destination address
	-by port and services
38	The proposed solution shall support packet captures based on:
	-Applications, IP
	-any threat/port/protocol
	-data-filters
39	The solution should support Data Loss Prevention from day 1.
40	Solution must not require cloud connectivity to detect and control any application
41	Solution should allow file inspecting across all protocols
42	The solution must provide a Single View on Known Threats, Hosts/Users visiting malicious URLs, Hosts/Users resolving malicious domains, applications involved in attacks, applications using non-standard ports, and detailed view on security policies allowing applications on non-standard ports.
43	The solution must provide detailed Change monitor.
44	The solution must provide detailed view on User Activity (along with source and destination IP) with granular view on Data transferred (bytes/sessions), threats associated with a user, Content and URLs accessed by User. This information must be available in Graphical as well as tabular format.
45	OEM must provide performance, throughput and features evidence through public domains- Websites and data sheets. DICDL reserves the right for asking the bidder to do a PoC that validates all technical compliance as submitted in the tender document.
Performance Requirement	
1	The proposed solution should support at least 40 Gbps Firewall Throughput with 8 Gbps NGFW Throughput including Firewall, application control, IPS. Solution should also support Anti-Virus, Anti-malware, Geo Protections and Anti-bot with all latest signatures enabled from day 1. The OEM must publish performance claims on public domain like websites, datasheets. Letter head performance claims will not be entertained.
2	"The proposed solution should support stream based/store-and-forward Anti-Virus Prevention. Solution should provide detailed infection information per malware type and/or infected users and machine.
3	Solution should be supplied with high availability and redundant power supply from day one. The performance must be measured using Data Center Environment with all Traffic enabled (not just internet traffic).
4	The proposed solution must support at least 5,000,000 concurrent sessions. The session count must be TCP connections..
5	The proposed solution must support at least 200,000 new session per second
6	The solution must provide 8X 10/100/1000 RJ45, 8x10G with SFP /SFP+, 400GB storage for System
7	The proposed solution must have 5Gbps of VPN throughput and should support at least 100 IPSec VPN 200 SSL VPN Users from Day one.
8	OEM must be EAL4/ ICESA/ FIPS 4.0 certified.

Server Room Core Switch

Sr. No.	Detailed Specifications
A	Solution Requirement
A1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing

A2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy
A3	Switch support in-line hot insertion and removal of interface modules/ should not require switch reboot and disrupt the functionality of the system
A4	Switch should support the complete STACK of IP V4 and IP V6 services
A5	The Switch and different modules used should function in line rate
B	Hardware and Interface Requirement
B1	Switch should have the following interfaces:
B1.1	a. 24 x 10G Multi Mode Fiber Interface
B2	Switch should have console port
B3	Switch should have management interface for Out of Band Management
B4	Switch should be rack mountable and support side rails if required
B5	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
B6	Switch should support VLAN tagging (IEEE 802.1q)
B7	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy(IEEE 802.3ad)
B8	Switch should support Configuration roll-back and check point
B9	Switch should support for different logical interface types like loopback, VLAN, SVI/RBI, Port Channel/LAG, multi chassis port channel etc.
C	Performance Requirement
C1	The switch should support 50,000 IPv4 and IPv6 routes entries in the routing table and multicast routes 8,000
C2	Switch should support restart for OSPF, BGP etc.
C3	Switch should support multiple VRF instances
C4	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG
C5	All interfaces should provide wire speed forwarding for all interfaces
C5.1	a. Switching
C5.2	b. IP Routing (Static/Dynamic)
C5.3	c. IP Forwarding
C5.4	d. Policy Based Routing
C5.5	e. QoS
C5.6	f. ACL and Other IP Services
C5.7	g. IP V.6 host and IP V.6 routing
D	Layer2 Features
D1	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)
D2	Switch should support VLAN Trunking (802.1q) and should support minimum 4K VLAN
D3	Switch should support basic Multicast IGMP v1, v2, v3
D4	Switch should support minimum 90,000 no. of MAC addresses
D5	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
D6	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third-party switch or server

D7	Switch should support Jumbo Frames
D8	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
D9	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
E	Layer3 Features
E1	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
E2	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
E3	Switch should support static and dynamic routing using:
E3.1	a. Static routing
E3.2	b. OSPF V.2 using MD5 Authentication
E3.3	c. ISIS using MD5 Authentication
E3.4	d. BGP V.4 using MD5 Authentication
E3.5	e. Should support route redistribution between these protocols
E3.6	f. Should be compliant to Multiprotocol Extensions for BGP-4
E4	Switch should support fast reconvergence of protocols.
E5	Switch should support multi instance MPLS routing using VRF
E6	Switch should be capable to work as DHCP server and relay
E7	Switch should provide multicast traffic reachable using:
E7.1	a. PIM-SM
E7.2	b. PIM-SSM
E7.3	c. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)
E7.4	d. IGMP V.1, V.2 and V.3
E8	Switch should support Multicast routing
F	Availability
F1	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
F2	Switch should provide gateway level of redundancy in IPV4 and IPV6 using HSRP/VRRP or equivalent protocol
F3	Switch should support For Fast Failure Detection as per RFC 5880
G	Quality of Service
G1	Switch system should support 802.1P classification and marking of packet using:
G1.1	a. CoS (Class of Service)
G1.2	b. DSCP (Differentiated Services Code Point)
G1.3	c. Source physical interfaces
G1.4	d. Source/destination IP subnet
G1.5	e. Protocol types (IP/TCP/UDP)
G1.6	f. Source/destination TCP/UDP ports
G2	Switch should support for different type of QoS features for real time traffic differential treatment using
G2.1	a. Weighted Random Early Detection
G2.2	b. Strict Priority Queuing
G3	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x
H	Security

H1	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
H2	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
H3	Switch should support for stringent security policies
H4	Switch should support for external database for AAA using TACACS+ or RADIUS:
H5	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
H6	Switch should support DHCP Snooping
H7	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
H8	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
H9	Switch should support banner
I	Manageability
I1	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
I2	Switch should provide remote login for administration using:
I2.1	a. Telnet
I2.2	b. SSH V.2
I3	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
I4	Switch should support for management and monitoring status using different type of Industry standard NMS using:
I4.1	a. SNMP V1 and V.2
I4.2	b. SNMP V.3 with encryption
I4.3	c. Filtration of SNMP using Access list
I4.4	d. SNMP MIB support for QoS
I5	Switch should support for basic administrative tools like:
I5.1	a. Ping
I5.2	b. Traceroute
I6	Switch should support central time server synchronization using Network Time Protocol NTP V.4/PTP
I7	Switch should support for providing MIB support for different statistics of the physical and logical interfaces
I8	Switch should support Real time Packet Capture for traffic analysis and fault finding
J	IPv6 features
J1	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such
J1.1	a. OSPF V.3
J1.2	b. BGP with IP V.6
J1.3	c. IP V.6 Policy based routing
J1.4	d. IP V.6 Dual Stack etc.
J1.5	e. IP V.6 Static Route
J1.6	f. IP V.6 Default route

J1.7	g. Should support route redistribution between these protocols
J2	Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode/MLD
J3	Switch should support for QoS in IP V.6 network connectivity
J4	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:
J4.1	a. SNMPv1, SNMPv2c, SNMPv3
J4.2	b. SNMP over IP V.6 with encryption support for SNMP Version 3
J5	Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment
J6	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
J7	Switch should support for IP V.6 different types of tools for administration and management such as:
J7.1	a. Ping
J7.2	b. Traceroute
J7.3	c. VTY
J7.4	d. SSH
J7.5	e. TFTP
J7.6	f. DNS lookup

Server Room Access Switch

Sr. No.	Detailed Specifications
A	Solution Requirement
A1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
A2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy
A3	Switch support in-line hot insertion and removal interface modules/should not require switch reboot and disrupt the functionality of the system
A4	Switch should support the complete STACK of IP V4 and IP V6 services
A5	The Switch and different modules used should function in line rate
B	Hardware and Interface Requirement
B1	Switch should have the following interfaces:
B1.1	a. 24 x 10G Multi Mode Fiber Interface
B2	Switch should have console port
B3	Switch should have management interface for Out of Band Management
B4	Switch should be rack mountable and support side rails if required
B5	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
B6	Switch should support VLAN tagging (IEEE 802.1q)
B7	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy(IEEE802.3ad)
B8	Switch should support Configuration roll-back and check point
B9	Switch should support for different logical interface types like loopback, VLAN, SVI/RBI, Port Channel/LAG, multi chassis port channel etc.
C	Performance Requirement
C1	The switch should support 50,000 IPv4 and IPv6 routes entries in the routing table and multicast routes 8000.

C2	Switch should support restart for OSPF, BGP etc.
C3	Switch should support multiple VRF instances
C4	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG
C5	All interfaces should provide wire speed forwarding for all interfaces.
C5.1	a. Switching
C5.2	b. IP Routing (Static/Dynamic)
C5.3	c. IP Forwarding
C5.4	d. Policy Based Routing
C5.5	e. QoS
C5.6	f. ACL and Other IP Services
C5.7	g. IP V.6 host and IP V.6 routing
D	Layer2 Features
D1	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S
D2	Switch should support VLAN Trunking (802.1q) and should support 4K VLAN
D3	Switch should support basic Multicast IGMP v1, v2, v3
D4	Switch should support minimum 90,000 no. of MAC addresses
D5	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
D6	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server
D7	Switch should support Jumbo Frames
D8	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
D9	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
E	Layer3 Features
E1	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
E2	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
E3	Switch should support static and dynamic routing using:
E3.1	a. Static routing
E3.2	b. OSPF V.2 using MD5 Authentication
E3.3	c. ISIS using MD5 Authentication
E3.4	d. BGP V.4 using MD5 Authentication
E3.5	e. Should support route redistribution between these protocols
E3.6	f. Should be compliant to Multiprotocol Extensions for BGP-4
E4	Switch should support fast reconvergence of protocols.
E5	Switch should support multi instance MPLS routing using VRF
E6	Switch should be capable to work as DHCP server and relay
E7	Switch should provide multicast traffic reachable using:
E7.1	a. PIM-SM
E7.2	b. PIM-SSM
E7.3	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)
E7.4	e. IGMP V.1, V.2 and V.3
E8	Switch should support Multicast routing
F	Availability

F1	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
F2	Switch should provide gateway level of redundancy in IPV4 and IPV6 using HSRP/VRRP or equivalent protocol
F3	Switch should support For Fast Failure Detection as per RFC 5880
G	Quality of Service
G1	Switch system should support 802.1P classification and marking of packet using:
G1.1	a. CoS (Class of Service)
G1.2	b. DSCP (Differentiated Services Code Point)
G1.3	c. Source physical interfaces
G1.4	d. Source/destination IP subnet
G1.5	e. Protocol types (IP/TCP/UDP)
G1.6	f. Source/destination TCP/UDP ports
G2	Switch should support for different type of QoS features for ream time traffic differential treatment using
G2.1	a. Weighted Random Early Detection
G2.2	b. Strict Priority Queuing
G3	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x
H	Security
H1	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
H2	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
H3	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4
H4	Switch should support for external database for AAA using TACACS+ or RADIUS:
H5	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
H6	Switch should support DHCP Snooping
H7	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
H8	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
H9	Switch should support banner
I	Manageability
I1	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
I2	Switch should provide remote login for administration using:
I2.1	a. Telnet
I2.2	b. SSH V.2
I3	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
I4	Switch should support for management and monitoring status using different type of Industry standard NMS using:
I4.1	a. SNMP V1 and V.2
I4.2	b. SNMP V.3 with encryption
I4.3	c. Filtration of SNMP using Access list
I4.4	d. SNMP MIB support for QoS
I5	Switch should support for basic administrative tools like:
I5.1	a. Ping

I5.2	b. Traceroute
I6	Switch should support central time server synchronization using Network Time Protocol NTP V.4/PTP
I7	Switch should support for providing MIB support for different statistics of the physical and logical interfaces
I8	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
J	IPv6 features
J1	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such
J1.1	a. OSPF V.3
J1.2	b. BGP with IP V.6
J1.3	c. IP V.6 Policy based routing
J1.4	d. IP V.6 Dual Stack etc.
J1.5	e. IP V.6 Static Route
J1.6	f. IP V.6 Default route
J1.7	g. Should support route redistribution between these protocols
J2	Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode/MLD
J3	Switch should support for QoS in IP V.6 network connectivity
J4	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:
J4.1	a. SNMPv1, SNMPv2c, SNMPv3
J4.2	b. SNMP over IP V.6 with encryption support for SNMP Version 3
J5	Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment
J6	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
J7	Switch should support for IP V.6 different types of tools for administration and management such as:
J7.1	a. Ping
J7.2	b. Traceroute
J7.3	c. VTY
J7.4	d. SSH
J7.5	e. TFTP
J7.6	f. DNS lookup

SA Distribution Device/Switch

Sr. No	Detailed Specifications
A	Form Factor
A1	Rack Mountable
B	Architecture
B1	The device should be modular in architecture and should have redundant Power Supply and should support redundant supervisor
B2	The device should to support large routing tables & other memory intensive processes
B3	System throughput of minimum 160 Gbps from day 1
B4	The switch should support non blocking Layer2 switching and Layer3 routing
C	Interfaces

C1	Minimum 20 x 1 Gigabit Ethernet routing ports with copper transceivers and Ethernet Ports (SFP) from day 1
C2	All the above ports should be in compliance with 802.3 standards
C3	The Gigabit Ethernet port should support multimode and single mode fiber connectivity
C4	The device should have at least 4 x 10G ports from day 1 and scalable to 6 x 10G Ports
C5	Device should have console & 10/100 management interface
C6	The device should support QoS classification, policing and shaping
C7	The device should support ACLs/filters
C8	The device should support minimum 30,000 MAC addresses.
C9	Should support IPv4 and IPv6 routes with Multicast Routes
D	Protocol Support
D1	Should support RIPv2, OSPF, IS-IS and BGPv4, LDP, BFP, MPLS routing protocols & IP multicast routing protocols: PIM, IGMP and Layer 2 circuits
D2	The device should support multiple level of privileges and authentication for user access
D3	Should support RADIUS or TACACS+
D4	Should support source and destinations based ACLs, time based ACLs
D5	Should support MD5 authentication for routing protocols
D6	Should be capable of supporting 802.1q VLANs and VLAN trunking
D7	Should support port aggregation for higher bandwidth and redundancy
E	QoS
E1	Up to 8 Queues per interface
E2	The device should support congestion management and queuing techniques like Priority Scheduling, WRED, LLQ, etc.
F	Management
F1	Should have software Upgrades N-1
F2	Should have integrated online diagnostics features using flow monitoring
F3	It should support a simple CLI interface/out of band management for configuration
F4	Should support SNMP v 1, v2 and v3
F5	Should support Telnet client functionality
F6	Should support TFTP
F7	Should support debugging features

SA Access Switch (POE+)

Sr. No.	Detailed Specifications
1	Minimum 48 ports of 10/100/1000 Base-T PoE+ ports and 4 x 10G ports.
2	Should support Non-blocking architecture.
3	All interfaces should provide wire speed forwarding for both Fiber and copper modules
4	Support for at least 4k VLANs & 30k MAC address
5	It should support IGMP snooping v1,v2 & v3
6	It should have static IP routing, RIP, RIPv2, OSPF, OSPFv3, PIM and vrf lite from day 1
7	Switch should support 8 hardware queues per port
8	Dynamic Host Configuration Protocol (DHCP) snooping
9	Switch should support LLDP / LLDP-MED capabilities
10	Should support IP source guard

11	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).
12	Switch needs to have console port for administration & management
13	Management using CLI, GUI using Web interface should be supported
14	TFTP
15	IEEE 802.1x support
16	IEEE 802.1D,1W,1S
17	IEEE 802.1p class-of-service (CoS) prioritization
18	IEEE 802.1Q VLAN
19	IEEE 802.3at
20	Switch should have internal redundant power supply.
21	Switch should able to support management via CLI/ Web interface /out of band
22	SNMP v1, v2, v3
23	Switch should be manageable through both IPv4 & IPv6.
24	The Switch should be EAL3/ NDPP certified.

Blade Chassis and Management

Sr. No.	Detailed Specifications
Blade Chassis	
1	Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit.
Power	
2	The power subsystem should support all of the following modes of power redundancy (N+1 or N+N or grid)
Cooling	
3	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics
Chassis connectivity	
4	The chassis should support redundant modules for connectivity
5	Converged Module
6	Chassis should have sufficient number of redundant 10gb based converged modules to provide a minimum FCOE uplink bandwidth of 20Gbps per blade server and 10Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for LAN & SAN Traffic.
Management	
7	Role Based Access Control and remote management capabilities including remote KVM should be included
8	All event on server, chassis should be logged
9	Supports a server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN , FC-HBA firmware version , Adapter QoS , Management module firmware version, Server Boot Policies, KVM IP etc.
10	Must support the ability to rollback firmware from current active versions to the previous version for the Server BIOS, Adapter firmware and bootcode versions , individual server management chips from the same console.
11	It should have provision for integration with Active Directory
Licensing	
12	Should include all necessary licenses for management for a fully loaded chassis.
13	TOR Unified Port Switch

14	Vendor must quote pair of TOR FCoE enabled switch and having minimum ports to support connectivity of set of 32 Blades. FCoE TOR switch must in turn connect to existing LAN core / Aggregation switch using 10 Gig SFP+/ 40 Gig SFP+ connectivity and SAN core director switch using line rate 16 Gbps FC ports.
15	Vendor should quote dual FCoE TOR switch for every 32 servers
16	Support N+1 or N + N redundant fans
17	Should support up to 50 primary VLANs per pair of switches
18	Should support up to 1000 secondary VLANs per pair of switches
19	Should support up to 2000 active VLANs and VSANs per pair of switches
20	Supports up to 12 uplink port channels per switch module
21	Supports up to 16 member interfaces per port channel
22	Supports up to 16 interfaces per FCoE port channel
23	Supports up to 4 SAN port channels
24	Supports up to 16 port channel members per SAN port channel
25	Supports up to 16 native FC uplinks
26	Supports a maximum of 4 active SPAN session per switch
27	It should support the direct connection to FC , FCoE enabled storage arrays and NAS , iSCSI based arrays

Blade Servers

Sr. No.	Detailed Description
Processors	
1	Each blade shall have a minimum of two (2) Intel's Latest Cascade Lake Processor Series CPUs , 2.4 Ghz, 10 Cores each or higher and should supports all Intel CPUs
Storage	
2	The server should support SAS/SSD hard disk drives. Server should be configured with 2 Nos of 600 GB , 12 Gbps 10K RPM SAS HDDs in Raid 0,1
3	Must have an internal slot for SD card / Flash which supports booting hypervisors
4	The Blade should have support for Boot from SAN
Memory	
5	Should have up to 1.5 TB of DDR4 memory, should be configured with minimum 64 GB
Network	
6	The Blade server should support Converged Network Adapter , which aggregates both the Ethernet and FC connectivity on a single controller
7	It should have 40 Gb connectivity per server with a minimum of 2 ports , which is expandable to 80 Gb connectivity per server
8	It should have two adapters per server to support above for card level redundancy
9	Adapter and QoS policies can be set and defined for each of the vNICs or vHBAs created in the virtualized adapter

Network Access Control & Authentication System:

Sr. No.	Detailed Specifications

1	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture, profiling and guest management services on a single platform.
2	Solution should include all required licenses to perform above mentioned capabilities for 100 endpoints from day one and scalable to 500 in future
3	It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
4	Proposed solution should include two appliances to be configured in Active/Standby
5	Should support enforcing security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention
6	Should support improve network access control capabilities to identify, mitigate/quarantine and rapidly contain threats
7	Should utilizes standard protocol for authentication, authorization, and accounting (AAA).
8	Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Transport Layer Security (TLS).
9	Should provide a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect
10	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, IoT and tablets.
11	It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.
12	The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.
13	Should support capability to verifies endpoint posture assessment for PCs connecting to the network. Should be a persistent client-based agent to validate that an endpoint is conforming to a smart city's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispysware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications.
14	Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.
15	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.
16	Solution should support the following endpoint checks for compliance for windows endpoints: Check process, registry, file & application Check operating system/service packs/hotfixes check for Antivirus installation/Version/ Antivirus Definition Date check for Antispyware installation/Version/ Antispyware Definition Date Check for windows update running & configuration
17	Proposed solution should support TACACS+ or RADIUS to simplify device administration and enhance security through flexible, granular control of access to network devices
18	TACACS+ or RADIUS device administration should support: 1. Role-based access control 2. Per Command level authorization with detailed logs for auditing
19	Proposed solution should support capability to customize TACACS+ or RADIUS Services by specifying customer TACACS+ or RADIUS port number

20	Proposed solution should support capability to create different network device groups so that administrator can create: 1. Different policy sets for IOS/OS or wireless controller OS 2. Different for firewall 3. Differentiate base on location of device
21	Proposed solution should be able to create TACACS+ or RADIUS profile like Monitor, Privilege level, default, etc. to control the initial login session of device administrator.
22	Proposed solution should be able to create TACACS+ or RADIUS authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, (any character), * (matches any), etc. and support stacking as well
23	Proposed solution must support TACACS+ or RADIUS in IPv6 network
24	Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: •Internal Users, Internal Endpoints, Active Directory, LDAP, RSA, RADIUS Token Servers, Certificate Authentication Profiles
25	Solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors: * Profiling using MAC OUIs * Profiling using DHCP information * Profiling using RADIUS information * Profiling using HTTP information * Profiling using DNS information / Nessus * Profiling using NetFlow information / OnGuard Agent * Profiling using SPAN/Mirrored traffic
26	Should support troubleshooting & Monitoring Tools

Backup Solution Specifications:

Sr. No.	Detailed Specifications
Architecture	
1	The proposed backup software should be modular in architecture, allowing components to be added and removed without requiring the backup system to be shutdown.
Interface	
2	The software should have web based Graphical User Interface (GUI) so that all backup servers can be managed centrally, regardless of location
3	All backup/restore administration must be controlled by a centralized master system
OS Support	
4	Backup software should support Operating systems: Windows/ Linux/ Unix etc.
Protection	
5	Backup software should maintain a database for all backup/restore meta-data
6	Easy to reconstruct against in the unlikely event of corruption.
Device Support	
7	The software must provide flexibility to backup to different media. These include disk-to-tape, disk-to-disk and interoperability.
8	The proposed backup solution must be able to support raw device backup – on both Windows, Linux and Unix.
Security	
9	The proposed backup solution must have user level access control list security function. Each user has different permissions and privileges on the system

Sr. No.	Detailed Specifications
Encryption	
10	The proposed backup solution must be able to encrypt backup data at source and store with AES 256-bit or higher encryption
Scheduling	
11	Ability to configure automated backups for specific days and weeks within a month, while maintaining a simplified methodology for complex date scenarios
DB Agent	
12	Should have specific agents/API to perform “hot” backups for MS-SQL, Oracle RAC, MySQL, PostgreSQL, etc. on different platforms like Windows / Unix / Linux etc.
Reporting	
13	Full job completion report. Overview of the full backup jobs that were successful, partially successful and failed for each day
14	Full back up data volume report. Overview of the total data volumes that were backed up for each day
Capability	
15	Must support storage protocols such as NDMP (version 3 & above). Capable of providing Check Point Restart for NDMP backup
16	Must support online backup of virtual machines.
17	The software should support 32 bits and 64 bits operating systems, databases and applications.
18	The backup software should have the functionality of backing up different types of Hypervisor
19	The backup software should support Image level backup of the Virtual machine(s)
20	The backup software should allow single / granular file recovery of data from the image level backup
Management	
21	The Backup software should include / add on licenses for Enterprise wide reporting from a single dashboard.

SAN Switch Specifications:

Sr. No.	Detailed Specifications
Ports	
1	SAN switch with minimum 32 x 16 Gbps or higher FC ports with all supported Licenses from day one.
Architecture	
2	The switch should have non -blocking architecture.
Port Support	
3	The switch should have support for 8 Gbps or higher HBAs
High Availability	
4	The switch should have No Single Point of Failure (SPOF)
5	The switch should have hot swappable redundant Power Supply with separate AC inputs
Monitoring	
6	The switch should have Real time performance monitoring reporting tool
7	The switch should have support for POST & online/offline diagnostics,
Compatibility	
8	The switch should have capability to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating Systems
Cross Platform Support	
9	The switch should have support of all leading SAN / NAS disk arrays
Security	
10	The switch should have security features: • Must have hardware & Software zoning and ACL • Policy based security and centralized fabric management

Sr. No.	Detailed Specifications
	- Encryption - FC authentication - RADIUS, SSH, SNMP - port binding and Masking
Inter Switch Linking (ISL)	
11	The switch should have Inter Switch linking feature to connect two or more FC switches
Trunking	
12	The switch should have trunking capability. The required software license should be supplied with switch.
QoS	
13	The switch should Provide Adaptive Networking services such as Quality of Service (QoS)
Management	
14	Support for web based management and should also support CLI. Switch shall support alert based on threshold value for temperature, fan status, power supply status and port status
Port Type Support	
15	The switch shall support different port type such as F/E/U/EX port ; self-discovery based on switch type

Unified Storage Specifications:

Sr. No.	Detailed Specifications
Storage Size & Tiering	
1	Storage should be supplied with 1 PB of usable space upgradable upto 4 PB excluding all overhead configuration like RAID single parity, dual parity, stripping and mirroring) configuration, formatting and hot spare disk. All capacity is to be provide with SAS, SSD Disk drives. Should support latest technology SSD, SAS, NL-SAS/SATA Drives
Disk Type	
2	The supported disks should be dual ported with minimum 12Gbps or higher full-duplex data transfer capability.
RAID Support	
3	The Storage should support RAID single parity, RAID dual parity, RAID stripping, mirroring
Controller	
4	Single Micro code for SAN & NAS functionality. Minimum Dual Storage controllers/Nodes configured in Active-Active with automatic failover.
Hot Spare	
5	Storage System should have Sufficient Hot spare disk provided and should be above the usable capacity i.e. 1 PB.
Connectivity	
6	Storage should have minimum 8 FC ports (8 Gbps or higher) and 8x10 Gb SFP+ for host connectivity.
DRAM Cache Memory	
7	The storage system should have minimum 384 GB DRAM cache per controller.
Data Protection	
8	The storage should have protection of cache data during a power down either scheduled or unexpected power outage by battery backup for at least 4 hours OR by de-staging the data in cache to non-volatile Disk.
Redundancy and High Availability	
9	The storage should be with No Single Point of Failure (SPOF). All the components should be redundant and hot swappable including power supply, fans, batteries etc. The proposed storage must support non-disruptive replacement of hardware component

Sr. No.	Detailed Specifications
Provision	
10	The storage should have traditional/similar raid group provisioning for Storage allocation to hosts.
Local Copy Features	
11	The proposed storage should have point-in-time copy or snapshots
Storage Management Features	
12	Storage management software should be browser-based/web enabled accessible over IP
13	Storage management software should have access for user accounts to the storage system
14	Storage management software should provide interface/wizards to perform configuration operations like create LUNs present LUNs to host, set LUN attributes etc.
15	Storage management software should be able to monitor alerts.
16	Storage management software should provide real time monitoring and historical analysis of storage performance data such as total IOPS, read%, write %, cache-hit %, throughput, etc. for analyzing performance of the systems.
Operating System and Virtualization Support	
17	The storage solution should support all latest operating system and cluster environments. The unified storage solution should support virtual infrastructure. Should have capabilities for booting VMs from the SAN. Should be supplied with virtualization aware APIs for provisioning and managing the storage array from the virtual infrastructure.
Protocol Support	
18	SNMP, LDAP, NFS, CIFS, FC-SCSI/iSCSI, SMB and NTP Synchronization
Supported Software and licenses for the total configured capacity	
19	Compression on SSD, Snapshot, restore snapshot, Cloning and application & VM aware backup., Quality of Service, Software for IOPS/Response Time and bandwidth. Should be supplied as per solution and requirement.
Other	
20	All the required licenses, cables, passive component and connectors to be supplied as per solution and requirement.

Unified Backup Storage Specifications:

Sr. No.	Detailed Specifications
Storage Size & Tiering	
1	Storage should be supplied with 250 TB of usable space upgradable upto 1 PB excluding all overhead configuration like RAID single parity, dual parity, stripping and mirroring) configuration, formatting and hot spare disk. All capacity is to be provide with SAS, SSD Disk drives. Should support latest technology SSD, SAS, NL-SAS/SATA Drives .
Disk Type	
2	The supported disks should be dual ported with minimum 12Gbps or higher full-duplex data transfer capability
RAID Support	
3	The Storage should support RAID single parity, RAID dual parity, RAID stripping, mirroring
Controller	
4	Single Micro code for SAN & NAS functionality. Minimum Dual Storage controllers/Nodes configured in Active-Active with automatic failover.
Hot Spare	
5	Storage System should have multiple Global Hot Spares. Sufficient Hot spare disk should be provided and should be above the usable capacity i.e. 250 TB.
Connectivity	

Sr. No.	Detailed Specifications
6	Storage should have minimum 4 FC ports (8 Gbps or higher) and 4x10 Gb SFP+ for host connectivity.
DRAM Cache Memory	
7	The storage system should have minimum 64 GB DRAM cache per controller.
Data Protection	
8	The storage should have protection of cache data during a power down either scheduled or unexpected power outage by battery backup for at least 4 hours OR by de-staging the data in cache to non-volatile Disk.
Redundancy and High Availability	
9	The storage should be with No Single Point of Failure (SPOF). All the components should be redundant and hot swappable including power supply, fans, batteries etc. The proposed storage must support non-disruptive replacement of hardware component
Provision	
10	The storage should have traditional/similar raid group provisioning for Storage allocation to hosts.
Local Copy	
11	The proposed storage should have point-in-time copy or snapshots
Storage Management	
12	Storage management software should be browser-based/web enabled accessible over IP
13	Storage management software should have access for user accounts to the storage system
14	Storage management software should provide interface/wizards to perform configuration operations like create LUNs present LUNs to host, set LUN attributes etc.
15	Storage management software should be able to monitor alerts.
Operating System and Virtualization Support	
16	The storage solution should support all latest operating system and cluster environments. The unified storage solution should support virtual infrastructure. Should have capabilities for booting VMs from the SAN. Should be supplied with virtualization aware APIs for provisioning and managing the storage array from the virtual infrastructure.
Protocol Support	
17	SNMP, LDAP, NFS, CIFS, FC-SCSI/iSCSI, SMB and NTP Synchronization
Supported Software and licenses for the total configured capacity	
18	Compression on SSD, Snapshot, restore snapshot, Cloning and application & VM aware backup. Quality of Service, Software for IOPS/Response Time and bandwidth. Should be supplied as per solution and requirement.
Other	
19	All the required licenses, cables, passive component and connectors to be supplied as per solution and requirement.

Industrial Ethernet Switch (Industrial Grade)

Sr. No	Detailed Specifications
General	
1	Shall have 2 100/1000BaseSFP Single mode ports, 10 KM Support with LC connectors, 8 No's of 10/100/1000 BaseT(X) copper ports (RJ45 connectors)
2	8 IEEE 802.3at PoE+ standard ports
3	Should Support NTP
4	DHCP Option 82 for IP address assignment with different policies
5	Ethernet/IP/PROFINET and Modbus/TCP protocols for device management and monitoring

6	Should support ring redundancy protocol
7	IGMP snooping or GMRP/MVR for filtering multicast traffic from industrial Ethernet protocols
8	IEEE 802.3ad, LACP for optimum bandwidth utilization
9	QoS based policy for bandwidth management
10	Secured port to restrict access to authorized MAC addresses (802.1x)
11	Port mirroring for online debugging
12	Automatic warning by exception through email/relay output
13	Line-swap fast recovery/RSTP/ERP/Portfast/equivalent (802.1d, 802.1w, 802.1s)
14	Remote network monitoring and proactive capability
15	QoS (IEEE 802.1p/1Q) and TOS/DiffServ
16	Configurable by web browser/ RJ45 connector
17	Works with Industrial network management software
Cyber-security Features	
18	User passwords with multiple levels of security protect against unauthorized configuration
	Command Line Interface (CLI) for quickly configuring major managed functions
19	SSH/HTTPS is used to encrypt passwords and data
20	Disable one or more ports
21	Secure switch ports so that only specific devices and/or MAC addresses can access the ports
22	Radius/TACACS+ allows you to manage passwords from a central location
23	SNMPv1,2,3 provides encrypted authentication and access security
Protocols	
24	IGMPv1/v2/v3, GMRP/MVR or equivalent, GVRP/VTP or equivalent, SNMPv1/v2c/v3,
	DHCP Server/Client, DHCP Option82, BootP, TFTP, SNMP/NTP, SMTP/SNMP
	RARP, , HTTP, HTTPS, Telnet, SSH, Syslog, Ethernet/PROFINET/IP, Modbus/TCP, LLDP, IEEE 1588, IPv6, NTP
Flow Control	
25	IEEE 802.3x flow control
Switch Properties	
26	Priority Queues 4
27	IGMP/Multicast Groups 200 and above
28	MAC Table Size: 8 K
29	Jumbo Frame should be supported
30	Min. Number of Available VLANs 200
31	VLAN ID Range VID 1 to 4000 and above
32	LED indicators for various parameters should be available on the switches (viz. Power, Alarm/Fault, etc.)
33	Inputs through various components like relays, I/O ports, etc. should be supported
Environmental Features	
34	Operating Temperature: -40 to 75°C
35	Humidity 5 to 95 %(non-condensing)
36	Mounting : DIN-Rail mounting, wall mounting (with required accessories/ kit)
37	Housing: Metal, IP30 protection
Input Voltage	
38	Input Voltage: 48 VDC (46 to 57 VDC), redundant dual inputs
Standard and Certifications	

39	Safety: UL , EN
	EMI: FCC Part 15 Class A, EN 61000-6-4 (Industrial), EN 61000-6-2 (Industrial), EN 61000-4-2 (ESD), EN 61000-4-3(RS), EN 61000-4-4 (EFT), EN 61000-4-5 (Surge), EN 61000-4-6 (CS), EN 61000-4-8
	Rail Traffic: EN 50121-4
	Mechanical shock standards should be complied with (Viz. IEC 60068-2-27/IEC 60255-21-2) or equivalent
	Should comply with electrical standards IEC 60068-2-30/31/32 or equivalent
	Vibration shock standards should be complied (Viz. IEC 60068-2-6/IEC 60255-21-1/IEC 60068-2-64) or equivalent
	NEMA-TS2
40	MTBF: More than 5 years
Other	
41	OEM or their distributor should have Service /Support network in India since last 5 years and service/support network in the state where switches got installed to get better service/support.
	OEM Should have installation base of 500 Industrial Switches in India since past 10 years

End Point Security Solution (Enterprise):

Sr. No.	Detailed Specifications
1	The MSI shall propose dedicated advanced endpoint protection solution to stop APT threats and should not be subset of Antivirus or HIPS or traditional end point solution
2	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint
3	The proposed solution shall work as an independent module without relying on other endpoint and network systems for any of its functionality
4	The proposed solution shall be capable of working along with all leading endpoint AV vendors without needing to replace them
5	The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as endpoint AV
6	The proposed endpoint solution should support detecting of all malware types, both known and unknown. The movement of all known and unknown malware should be tracked and reported across the endpoints.
7	The proposed endpoint solution should be able to support continuous and root cause analysis to help in triaging of security incidents.
8	Security vendor must have a dedicated research organization that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild.
9	Software footprint should be small and must support interactive and/or silent install. Total of 100 Licenses should be factored for this End Points from day 1 and scalable upto 500.
10	Endpoint software must be easy to deploy and support (not limited to) deployment through 3rd party systems management tools
11	Root cause analysis on a suspected machines should include the following capability:
	- Sequential and chronological trace of events with details including host, username, IP, client application involved
	- Details should highlight which file/process/services that affected
12	Proposed endpoint software should support malware tracking and provide visualization at the network level: systems and users affected, patient zero, and method/point of entry.
13	Proposed system must support continuous and persistent monitoring of files to detect polymorphic and time bound malware whenever they start turning bad and shall not be only an on-demand scan mechanism

14	Proposed endpoint software must be capable to block CnC communications and dropper activity and contain the spread of malware
15	Remediation at endpoints for incident response should include (and not limited to):
	- Track and capture files on suspected machine with option for lookups on suspected devices
	- Block of files / process / services that are showing malicious behaviors
	- Dropper detection and blocking of downloads via URL / sites
	- Submit suspected malicious files for further analysis
16	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user
17	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)
18	The proposed solution shall provide details to enable forensic analysis of incidents
19	The solution shall be capable of working in Windows, Mac & Linux operating systems
20	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints
21	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition
22	Proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator
23	Proposed solution should be able to do a threat hunting across all endpoints and quarantine the specific malicious file
24	Proposed endpoint solution should run as is and not require any system changes at OS level like enabling Volume Shadow copy Service, disabling admin access or any other user level change
25	Solution must support Exploit Prevention detection engine to block exploits and memory attacks that target certain processes.
26	Solution must support System Process Protection adds protection for memory attacks against Windows system processes.
27	Solution must support Adding Process Exclusion type to support System Process Protection in AMP for Endpoints Windows Connectors.
28	Solution must support Adding Policy settings to enable Exploit Prevention and System Process Protection in AMP for Endpoints Windows Connectors.
29	Solution must allow Users to choose to preview the new Policy UI.
30	Exploit protection - for protecting certain popular applications like MS Word, Excel, PowerPoint, Internet Explorer, Firefox, Chrome, Adobe Reader and others from attacks loading malwares that directly into the memory of these processes.

Antivirus Specifications:

Sr. No.	Detailed Specifications
1	Single Agent: Should be a single agent that combines all the critical components for comprehensive security on the endpoint. (Antivirus, Antispyware, device control, desktop firewall, Desktop HIPS, application control and Endpoint Detection & Response etc.)
2	It should be managed from a single centralized management console which should provide Instant visibility into the security state and health of endpoint security products and not based on logs. Real-time actions help ensure that defenses are installed, running, correctly configured, and up to date.
Threat Prevention Module	
1	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses
2	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses

3	Scan target drives: Should specify directories and file types to scan
4	Scan exclusions: Should specify directories and file extensions not to be scanned
5	Should have Configurable Scanning. Should have the ability to control the amount of CPU resources dedicated to a scan process
6	Treatment options: Should Enable choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete
7	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware
8	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce the dependency on Daily Signature updates.
9	Should have a different protection level in cloud based intelligence. This includes Very Low, Low, Medium, High and Very High.
10	Full-system scan: Should Scans local file folders and specific file types
11	Should be able to lock down all anti-virus configurations on the system
12	User should be prevented from being able to uninstall the anti-virus software.
13	Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time
14	Should have centralized management and reporting capabilities to deliver reports like top Spywares, by category, by infected machines, by risk priority etc.
15	Real time Active protection on memory, process termination / file removal of pests in active memory
16	Should have centralized update/download mechanism which should be able to download details of latest Spywares and push the same across all the desktops
17	The solution must be able to auto-quarantine or auto-delete spyware or adware without end-user interaction
18	Browser Security : Should Support all browsers available in the market such as Internet explorer, Mozilla Firefox, Google Chrome, etc.
19	Proposed solution should have integrated URL categorization feature
20	Proposed solution should categories URLs for threats like – Spywares, Trojans, Spam, Adware etc.
21	Solution URL category module should provide end user detail threat information about the site
22	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.
23	Solution should provide real time over the web/ cloud based intelligence to detect newer threats.
24	The solution should be able to determine file-execution decisions with rule-based logic based on endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.
25	The proposed solution should be able to map the global intelligence from their own cloud with the local intelligence collected from endpoint solution proposed.
26	The proposed endpoint protection solution should be able to import threat reputation of files through file hashes into the central endpoint protection management solution.
27	The proposed endpoint protection solution should be able to integrate with Sandboxing Technology (which performs both static & dynamic code analysis) by automatically submitting samples to sandbox which have no signature, behavioral and reputation both locally and globally.
28	The proposed endpoint solution should be able to automatically prevent the execution of even unknown executable files even if the endpoint does not have the latest signatures and without heuristics or behavioral patterns.
29	Should not block just on file hashes but on certificate bases also such that only trusted certificates are allowed to execute.
30	The solution should provide an Integrated firewall which should use reputation scores based on vendor's global threat intelligence to protect endpoints from botnets, DDoS, APTs, and suspicious web connections.
31	The proposed solution should provide an option for the administrator to pick and choose the protection modules they want for their endpoints based on their system type and environment.
32	The proposed solution should not be based on point-to-point product API integrations which are subject

	to product version changes.
33	The communication over the messaging fabric should be secured via TLS version 1.2 and PKI mutual authentication.
Device Control for Desktops	
1	The solution should potentially block the end point system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug and play devices based on device classes and device definitions are used to define device rules
2	It should support device management and should allow you to Monitor, Block or make the device Read-Only along with the option of providing exceptions
3	It should support for detecting attempts to copy data to removable storage devices (e.g. USB drives, floppy, CD/DVD, etc.).
4	It should support for blocking Windows native CD writing and other CD writing software. The block must inform the user that the action is being blocked.
5	It should support for customizable notification “pop-up” messages
6	It should be able to control the access of USB devices by using their vendor ID, product ID or serial number.
7	The solution installation, policy management and reporting should be handled by an integrated endpoint agent on the client.
8	The solution should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc.), and even access evidence files as the events happen in your environment.
9	It should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users
10	It should provide the functionality of logging and audit-trail capabilities
Application Control	
1	The Solution should ensure that Only authorized software / applications / executable codes are allowed to run and provides tamper protection to them.
2	Solution should be capable of creating white list for each system dynamically and no manual intervention in creating this list.
3	Each white list created should be unique to each system and should not be a common list
4	The solution should provide the user to self-approve any new application / software with business justification. So that new application can be run successfully with notification to administrator.
5	Solution should allow administrator to approve or revoke self-approved application status so that new application can be allowed to run or ban.
6	Solution should consider executables, ActiveX, Java, Perl scripts, bat files, VBS files, com files, DLL files, and sys files while creating the white list.
7	Solution should be capable of locking down the system on the white list created above and prevent execution of non-white listed software / application / executable code.
8	Solution should prevent tampering of applications which are white listed above either on disk or on memory when running
9	The Solution should have the capability to run on observation mode post white list creation so that new applications / software's / codes are not stopped from running but are monitored only. If required administrator should be able to approve or revert back to base line.
Management Platform :	
1	Should have a single Centralized Management Console for managing Antivirus, Antispyware, device control, application control etc.
2	The solution should be managed from a single centralized console and should provide integrated management for endpoint security solution. It should be able to deploy, manage, and update agents and policies from one management platform.
3	It should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site
4	Central management console should provide actionable reports

5	Central management console should support granular role based access control
6	Should ensure security policy enforcement by integrating and centralizing installation, deployment, management & updating
7	Centralized management server should be able to automatically report about the new unprotected
8	Solution should provide for custom reports and queries along with role-based access providing different levels of dash-boarding and relevant reports to users.
9	Solutions should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc.), and even access evidence files as the events happen in your environment.
10	Solutions should support report customization and allow viewing directly using a web browser and also as a dashboard using the same management console for the endpoints.
11	Solution should supports the following formats for exporting data: CSV, HTML, XML, Acrobat PDF,
12	Solution should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users
13	Solution should provide the functionality of events being viewed, filtered, and sorted in the Management console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.
14	Solution should provide the functionality of logging and audit-trail capabilities.
15	Solution should provide the capability to log administrative activities in the Management console. Administrative activities that are logged in the Management console include, changes to policies, deployment of policies, agent override activities, agent termination, and agent uninstall key generation.

Enterprise Management System & Network Management System

Sr. No.	Technical Specification
Network Monitoring	
1	The EMS solution shall be capable of supporting multiple types of discovery like IP range discovery – including built-in support for IPv6, Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices.
2	The solution shall support exclusion of specific IP addresses or IP address ranges as per discovery requirements.
3	The solution shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.
4	The solution shall be able to identify and model the ICT asset and its properties in the solution when discovered.
5	The solution shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason as applicable.
6	The solution shall provide out of the box root cause analysis for any observed fault or outage.
7	The solution shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
8	The solution shall detect virtual server and virtual machine configuration changes and automatically update topology and shall raise a notification when VM migrations happen between hosts.
9	The solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.
10	The solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.
11	The solution shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.

12	The solution shall have all the capabilities of a Network Management System which shall provide Real time network monitoring and Measurement offer end-to-end network performance & availability to define service levels and further improve upon them.
13	The solution shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.
14	The solution shall have the capability to configure different polling speeds for different devices in the managed infrastructure.
15	The solution shall use intelligent alarm algorithms to learn the behavior of the network infrastructure components over a period of time and report in case of any unusual activity.
16	The solution shall provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. The solution shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The solution shall also intelligently determine which ports are operationally dormant.
17	The Network Performance Management console shall provide a consistent report generation interface from a single central console.
18	This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources
19	The proposed system shall enable complete customization flexibility of performance reports for network devices and monitored servers.
20	The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.
21	The proposed system shall provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out.
22	The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.
23	The solution should be made available in a High Availability setup & should be able to stably support at least 2200 network devices & switches in the DSIR environment.
Application monitoring	
24	The solution shall proactively monitor all user transactions for any web application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.
25	The solution shall determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer.
26	The solution shall be able to obtain request response times based on different call parameters.
27	The solution shall be able to correlate Application changes (code and configuration files) with change in Application performance.
28	The solution shall be able to limit access to data by user roles e.g. Data for an application should be visible only to the application's owners
29	The solution shall give visibility into end user experience for various transactions without the need to install agents on end user desktops.
30	The solution shall act as a passive listener on the network thus inducing zero overhead on the network and application layer particularly during peak loads.
31	The solution shall be able to detect user impacting defects and anomalies and reports them in real-time such as in case of a Slow Response Time, Partial response, Missing component within transaction, HTTP error codes, web application errors etc.
32	The solution shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.
33	The solution should be made available in a High Availability setup & should be able to stably support at least 12 applications with possibility for adding more apps in the future based on DSIR citizen requirements.

Service monitoring & reporting	
34	The solution shall include a service management system which shall provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
35	The MSI is obliged to regularly monitor the SLAs and KPIs as set out in "Service Level Management" documents agreed upon by the CIOC. In case of degradation in actual performance, this shall be escalated by the Supplier to the right level in the organization and follow up until resolution as per agreed SLAs. The Supplier shall keep DSIR informed about such escalations at mutually agreed time intervals and maintain a log of all escalations and messages or actions related to the escalations.
36	The solution shall provide an outage summary that gives a high-level health indication for each service as well as the details and root cause of any outage.
37	The solution shall manage IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Service definitions should be as deemed suitable for the DSIR by the CIOC team.
38	The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).
39	SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.
40	The solution shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an applicable SLA shall be available.
41	The solution shall provide reports which include service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
42	The solution shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
43	The solution shall provide for customizing service policies as per service owner definitions like Service Condition High\Low Sensitivity, service SLAs, violation conditions etc.
System monitoring	
44	The solution shall present a centralized management console & dashboard across both physical and virtual systems.
45	The solution shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents/ agentless on the servers to be monitored if needed.
46	It shall be possible to configure the operating system monitoring agents to monitor based on user-defined and thresholds for warning/critical states and escalate events to event console of enterprise management system.
47	It shall also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
48	The solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
49	System shall be able to provide process and NT service monitoring in case of critical application service/process failures using remote scripts to resolve the same by restarting the same within the event window to avoid delay in resolving such issues
50	The tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable them to take applicable actions.
51	The performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.
52	It shall be able to automate monitoring, data collection and analysis of performance from single point.

53	It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) or application owners to quickly trace and resolve performance-related bottlenecks.
54	The system shall provide Performance Management and Reporting — Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines .
55	The solution should be made available in a High Availability setup & should be able to stably support at the Datacenter/server room both Physical and Virtual.
Patch Management	
56	The system management solution should include a patch management tool which will manage the entire lifecycle of patches, hot-fixes, updates and service packs from automatic discovery, download and collection, thorough testing, conflict analysis, and vulnerability assessment, to policy-based targeting and deployment and ongoing management to ensure that patches stay applied as prescribed by policy.
57	The solution shall automatically sense and apply patches through Admin access or automated as per defined policy (install, uninstall, repair, self-healing) on the clients, eliminating the need to create lists and administrator jobs (no admin intervention). If a certain patch is deleted or un-installed from any desktop by the user, it should automatically be repaired / re-installed without the intervention of the Administrator to reduce helpdesk calls.
58	Solution should enable the administrator to generate real time patch compliance reports based on created policies, reports on failed patch deployments and rollbacks, systems pending restart etc. for streamlining the process.
Asset Management	
59	The solution shall include Service Asset and Configuration Management capabilities to fulfil the following requirements:(a) Develop, Implement and Maintain Asset Management Processes and Tools (b) Maintain Asset records relating to the Services in online asset inventory, Configuration and management system (CMDB). (c) Provide, develop, implement and maintain online Asset and Configuration Management tools that support automatic discovery and facilitate effective deployment and re-use of Assets and provide a common view of information. (d) Develop, implement and maintain forms, processes and Tools related to Asset and Configuration Management and compliance to support tracking Changes across multiprovider Environment (add/modify/delete). (e) Provide a gap analysis of in-service and out of Service Assets and resources that cannot be found using a network discovery tool and document their status and Availability for re-deployment. (f) Establish, update, and maintain CIs in the Asset and Configuration Management database (CMDB)(g) Manage every asset from requisition through retirement and the facility to track changes by maintaining history of an asset
60	The CI level of Asset information shall include at the minimum: 1. Manufacturer 2. Model 3. Serial number 4. Asset identification number 5. Asset location 6. Maintenance information and history including the age of the Asset 7. Ownership information (provider/lease /purchase) 8. Warranty information 9. End of Support Information 10. End of Life Information 11. Service tag descriptions (both on CI and CI group level), including the possibility to tag which application/usage an Asset is used for 12. Inter-relationships and dependencies between Assets and applications/Services, with necessary CI level of details to conduct Impact Assessment and analysis 13. Other information as mutually agreed. 14. Replacement History
61	The solution shall support the functionality to – 1. Add, modify, and delete access to appropriate fields within CMDB.

	2. Maintain assets and relationship, contact and escalation information to ensure Application supportability. 3. Perform monthly physical Asset audit, in accordance with the Asset Management Services, to validate that Data in the database is accurate and current and that the Information is provided as defined. Physical Asset audit shall be based on statistically significant sample size. 100% sampling is not required. 4. Establish CMDB process interfaces across all associated Cross-Functional processes and IT functions. 5. Align CMDB updates process with Service Introduction and Change Management for removal, addition or updating of CMDB data
62	Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc.
63	Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs
64	Ability to provide the facility to collect custom information from desktops and ability to recognize custom applications on desktops
65	Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned
66	Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group
67	Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc.
68	Assets must be identified and tracked location, user/department wise.
69	Server details must be managed in the System to ensure stakeholder management.
70	Proactive asset manager must be enabled to notify the stakeholder when the warranty of the asset expires as this helps the asset team to proactively manage end of life assets effectively.
71	Manage contract service levels in the system to track the End of Life Assets
72	Vendor details must be maintained in the system to map the assets.
73	The solution should be made available in a High Availability setup & should be able to stably support upward of 3500 network connected smart assets including cameras, sensors, displays etc. in the DSIR environment.
ITSM	
74	The Solution should have the complete process flow for Incident, problem and Change, Service Desk, SLM and knowledge Management etc.
75	The solution should support capability to receive, manage and respond to issues, requests, Incidents, Problems etc. communicated within the ITSM tools.
76	The solution should provision the administrator to create new or modify existing workflows.
77	For integrations with other EMS/NMS tools, various options for integration should be provided - APIs, web services, SDKs.
78	The solution should allow for, at the minimum, for the following capabilities:
79	The flexibility of logging incidents via various means - be it manual or automatic via integration within the EMS solution.
80	It should allow detailed multiple levels/tiers of categorization on the type of incident being logged.
81	It should provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels.
82	The MSI shall recommend, document (textual and graphical as appropriate) and implement best practices for Incident Management via the solution.
83	Maintain contact, escalation and notification requirements (e.g. email, phone, including Alerts) for Incidents.

84	The solution shall provide cross-functional coordination required for incidents and major incidents such as automated integration to the Event, Problem, technical and functional change, Configuration. The solution should support Incident & problem driven change-release deployment activities.
85	The solution should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.
86	The solution should deliver service level information and alerts directly to IT Operations and Service Support consoles.
87	The solution shall record, document and track all Changes regarding Equipment and Software within the CMDB maintained
88	The solution shall contain Audit trail of any and all Changes including authorization, type of Change and status
89	The solution should manage communication, coordination, Monitoring and scheduling of Changes in computing environment with the stakeholders. It should allow Involvement of CAB and change managers to provide authorization for change requests.
90	Maintain all Configuration Data of the change management system
91	Maintain Post Implementation Review for the Normal and Emergency Changes
92	The solution should support Change Impact and change collision detection based on affected CIs from CMDB.
93	The solution should provide for Change Calendar with periodical views for change tracking.
94	The solution shall provide for following Problem Management capabilities: - Record, document and track all problems - Maintain RCA and solutioning details to avoid the recurring incidents - Ability to create change request for the problem ticket - Auto Assignment of problem based on the category - Ability to create knowledge from the problem - The workflows should be able to perform notification via email to the problem managers and problem analysts
95	The solution shall allow for request management with following capabilities:- Monitor the status of Service Requests including approvals and changes to delivery dates- Maintain appropriate controls to ensure the necessary approval of requests such that only authorized individuals are able to place Service Requests.
96	The solution should support developing, supporting and update Knowledge Management (KMDB) to gather, analyze, store and share knowledge.
97	The solution should support reporting on the process flow to allow management to understand how organization is performing in terms of process adherence.
98	The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process.
99	Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time.
100	The solution should provide for best in class integration capabilities with CMDB compliant APIs.
101	The solution should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle.
102	The solution Should automatically create Service models to describe how IT infrastructure supports business services.
103	Maintain vendor details when the incidents requires vendor involvement for the closure
104	The solution should Provide a Service catalogue so as to establish a framework for Service definitions based on IT and business alignment.
105	The solution Should Provide Service blueprints to describe functional and deployment models for the Service definitions.
Integration	

106	The proposed network management system shall integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk.
107	The proposed network management system shall attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it shall be automatically created prior to submitting the ticket. NMS console shall show associated helpdesk ticket number for the alarms that generated those tickets.
108	SLA's violation on monitored end user response time shall open a helpdesk incident.
109	Proposed Application Performance Solution shall integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console.
110	The proposed Fault Management Solution shall support integration with proposed help desk or trouble ticketing system such that integration shall Associates alarms with Service Desk tickets in the following ways: - Manually creates tickets when requested by Fault Management GUI operators - Automatically creates tickets based on alarm type - Maintains the consistency of the information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets. - Helpdesk ticket number created for associated alarm shall be visible inside Network Operation Console.
111	The proposed NMS shall provide unified workflow between the fault and performance management systems including bi-directional and context sensitive navigation, such as:- Navigate from the Topology View to At-a-Glance or Trend Reports for any asset- Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports- Proposed Performance Management system shall feed in discovery from Devices already discovered in Network Management Module without starting discovery process again all together in Performance Management Engine.

Gas Level Monitoring

Sensor Range:

- NO2: 0.005 to 2 ppm
- SO2: 0.005 to 2 ppm
- CO2 : 0 to 5% (5000 ppm)
- CO : 0 to 40 ppm
- O3: 0.005 to 2 PPM
- PM 2.5: 0 to 1000 micro gms / cu.m
- PM 10: 0 to 1000 micro gms / cu.m
- Temperature: -50°C ~ 100°C
- Humidity Sensor: 0-100%
- Connectivity: USB / Ethernet connectively to graphical display
- 4G and Bluetooth communication module to achieve wireless control
- Automatic grasping the site location information, real-time update drawing monitoring network

Environmental Monitor

Measuring Parameters: wind speed, wind direction, Temp, RH, Rain & Solar Radiation

- Wind Speed Sensor
 - Range: 0 ~ 45 m/s Resolution: 0.1 m/s
 - Accuracy: $\pm (0.3 \pm 0.03 \text{ V})$
- Wind Direction Sensor
 - Range: 0-360°
 - Resolution: 1°
 - Accuracy: $\pm 3^\circ$
- Air Temperature Sensor

- Range: 0 °C ~ 70 °C
- Resolution: 0.1 °C
- Accuracy: ± 0.5 °C
- Air Humidity Sensor
 - Range: 0 ~ 100%
 - RH: 0.1%
 - Accuracy: ± 5 %
- Rain Sensor
 - Range: 0 ~ 4 mm/min
 - Accuracy: ± 4 %
- Total Radiation Sensor
 - Range: 0 ~ 2000 W/m²
 - Accuracy: ± 5 %

Multiservice Kiosk

Sr. No.	Technical Specification
1	Touchscreen Monitor: 17" – inch LCD Monitor with minimum 1280X1024 resolution. Dot pitch to be constant (0.3mm) across the panel size.
2	Keyboard: Virtual only with big buttons
3	Printer: Receipt/acknowledgement printer.
4	Scanner: Barcode scan, QR code scan, Fingerprint scan, etc.
5	Card Reader: Debit, Credit, Smart Card reader
6	Microphone: To listen to Voice instructions / Digital speech/records.
7	Disaster/safety devices: Fire, rain, dust proof devices etc. safety devices to be loaded/mounted on kiosk
8	Inbuilt UPS
9	Kiosk Body / Physical structure / panel to be advised by MSI for better kiosk physical structure as per requirements.

Box Camera (Surveillance):

Sr. No.	Specs Category	Detailed Specifications
1	Sensor	CMOS sensor with size of 1/2.8" inches or higher with progressive scan
2	Pixels	1920X1080 pixels or higher
3	Video compression	H.265, H.264 and MJPEG simultaneously
4	Frame rate	25fps-30fps
5	S/N ratio	Min.52 db
6	WDR & BLC	Off/Low/Mid/High
7	Illumination	Color:0.3 lux & B/W:0.05lux
8	Iris	DC-Iris or better
9	External IR Illuminator	External IR illuminator with visibility should be atleast 50Mtr. Illumination (color & b/w) should be sufficient to capture objects/faces at night time when there is not sufficient illumination at site.
10	Shutter speed	Vary between range of given range as follows: 1/25 to 1/66500
11	Image Improvement Functionalities	Backlight compensation, Exposure Control, WDR, White Balance, Noise Reduction, AGC, Sharpness, Brightness, Contrast, image overlay & Saturation
12	Bandwidth Control	Constant Bit Rate Mode & Variable Bit Rate Mode
13	Highest Image Resolution & FPS	1920x1080 with minimum image interval as 25FPS
14	Day/Night Functionality	Auto switch the images in to Color & Monochrome
15	Video Compression	H.264 Baseline and Main Profile & Motion JPEG video compression

Sr. No.	Specs Category	Detailed Specifications
16	Edge Recording	Edge recording and support memory card slot for on board recording during non-availability of network connectivity with minimum 64GB of memory card has to be provided.
17	Power	Through 12VDC/24VAC/POE (IEEE 802.3af/802.3at)
18	Network Connector	Should be minimum 10/100 Base-T, (Should be POE) Ethernet RJ45
19	Alarm Input & Output	1x alarm input and 1x alarm output for triggering external devices through input or output
20	Onvif Conformance	Profile S, G
21	Operational Temperature	0 °C to 55 °C
22	Networking Protocols	IPv4/v6, HTTP, HTTPSb, SSL/TLSb, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SNMPv1/v2c/v3, DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP/Protocol should meet all functional requirement of project
23	Multicast Streaming	Should have support for multicast streaming
24	Vandal Resistant Rating	IK10 or better
25	Ingress Rating	Minimum ingress rating of IP66/NEMA 4x for outdoor installation
26	Dual Streaming	Should support dual streaming
27	Firmware Upgrade	Remotely through any method like web based/software based/FTP based
28	SD Card Slot	At least one SD card slot
29	Certifications/ Standards	EN, UL & BIS
30	OEM	OEM of Camera should be in the business of supply of Cameras in India for the last 5 years or more. OEM should be a full member of ONVIF on the date of bid submission.

PTZ Camera (Surveillance):

Sr. No.	Specs Category	Detailed Specifications
1	Sensor	CMOS sensor with size of 1/2.8" inches or higher with progressive scan
2	Pixels	Total number of effective pixels should be 2.0 MP or higher
3	Signaling Standards	NTSC or PAL signaling Standards
4	S/N ratio	55 db
5	Focal Length	5.2mm - 104mm or 6mm – 180 mm
6	Illumination	Color: 0.2 lux, B/W 0.02 lux
7	Pan/Tilt Rotation	Capability to have endless 360° Pan & 180° tilt rotation
8	FOV	Horizontal FOV: 59.5° to 2.1° , & Vertical FOV: 39.0° to 1.2°
9	Shutter speed	1/25 sec to 1/10000 sec
10	Image Improvement Functionalities	Backlight compensation, Exposure Control, WDR, White Balance, Noise Reduction, AGC, Sharpness, Brightness, Contrast, image overlay, e-flip & Saturation
11	Optical Zoom	30x Optical Zoom or higher
12	Highest Image Resolution & FPS	1920x1080 or better with minimum image interval as 25FPS
13	Day/Night Functionality	Auto switch the images in to Color & Monochrome images in Day/Night
14	Video Compression	H.264, MJPEG (dual)
15	Edge Recording	Edge recording and support memory card slot for on board recording during non-availability of network connectivity
16	Power ON	Through 24VAC/12VDC or (IEEE 802.3af/802.3at)/POE
17	Network Connector	Should be minimum 10/100 Base-T, (Should be POE) Ethernet RJ45
18	Alarm Input & Output	1x alarm input and 1x alarm output for triggering external devices through input or output
19	ONVIF Conformance	Profile S, G
20	Operational Temperature	0 °C to 55 °C
21	Networking Protocols	IPv4/v6, HTTP, HTTPSb, SSL/TLSb, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SNMPv1/v2c/v3, DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP/Protocol should meet all functional requirement of project

Sr. No.	Specs Category	Detailed Specifications
22	Multicast Streaming	Support to multicast streaming
23	Vandal Resistant Rating	IK10 or better
24	Ingress Rating	IP66/NEMA4x for outdoor installation
25	Dual Streaming	Support to dual streaming
26	Firmware Upgrade	Remotely through any method like web based/software based/FTP based
27	Weight	Should not exceed 4.3kg (9lb 8oz)
28	SD Card Slot	At least one SD card slot
29	Certifications/ Standards	UL & BIS
30	OEM	OEM of Camera should be in the business of supply of Cameras in India for the last 5 years or more. OEM should be a full member of ONVIF on the date of bid submission.

2 Screen – Operator Client Workstations for Command Control Centre:

Sr. No.	Features	Detailed Specifications
1	Processor	2 x Latest Intel Xeon 3 Ghz or higher
2	Chipset	Intel Chipset
3	RAM	Min 16 GB or higher expandable upto 32GB
4	Hard Disk	1 TB SATA 7200 RPM SSD Option for future expansion of additional Hard drives.
5	Optical Drive	9.5mm Slim DVD Writer
6	Graphics Card	4GB Graphics card
7	Monitor	Minimum 23 and higher Inch touch screen LED monitor, Resolution 1920*1080
8	Slots	Min 3 x PCIe All PCIe slots should be open-ended.
9	Ports	6nos or higher USB (mini 2, USB3.0), 1xHDMI/1VGA Port, 1 Audio Line-In, 1 Audio Line-Out
10	Keyboard and Mouse	Minimum 104 keys USB Keyboard and USB Optical Scroll mouse
11	Audio	High Definition Integrated Audio with Internal speaker.
12	Power Supply	Should be supplied with required power supply as per the actual site requirements
13	Operating System	Pre loaded Windows 10 Professional with recovery disc for Workstations.
14	Certification	RoHS, ENERGY STAR/BEE certified at the time of bidding.

Video Wall Display/Screen:

Sr. No.	Parameter	Detailed Specifications
1	Configuration	Seamless Videowall of DLP Cubes. Each cube size to be 70" (Inches diagonally) or more with complete configuration of 4x2 and 6x3 configuration. All cubes have to be of the exactly same size, configuration and model wise mandatorily. The wall to be installed in curved fashion with all required support system like Controller / stand for DLP Cubes / Interfaces / Connecting cables. Videowall Solution should be from Single OEM
2	Operation	24 X 7: The Video Walls & IP Controllers and all support systems should be capable of working in 24 x 7 mode without any deterioration in the

Sr. No.	Parameter	Detailed Specifications
		performance
3	Chip Type	1-chip Digital Micro Mirror Device
4	Resolution	1920 x 1200 native (WUXGA Display)
5	Light Source Type	LED light source with separate LED array for each color (RGB)
6	Brightness ANSI	Minimum 700 Lumens
7	Brightness Uniformity	≥ 90 %
8	Dynamic Contrast	1200000:1 or more
9	Redundant Dual Power Supply	Cube should be equipped with a built in dual redundant power supply
10	Hot Swappable Power Supply	The inbuilt power supply should be hot swappable
11	Control	IP based control to be provided
12	Remote	IR remote control should also be provided for quick access
13	Screen to Screen Gap	≤ 0.3 mm
14	Screen Support	Screen should have an anti-reflective glass backing to prevent bulging
15	Cooling Inside Cube	By Means of a heat pipe. No liquid cooling.
16	Cube Depth	< 800 mm
17	Maintenance Access	Rear
18	Inputs in the Cube	DVI-2, HDMI-1, HDBaseT-1, Display port-1
19	Output in Cube	DVI – 1
20	Cube control & Monitoring	Videowall should have cube control & monitoring system which can provide videowall status including source, light source, temperature, fan & power information. The system should be based on web-browser architecture. Should be able to provide an error message in three sections: a) Problem area b) Error Module Location c) Error Module Image
21	OEM	The proposed OEM make/model of display cube should have been successfully running for at least 1 year in at least 1 Smart City project in India
22	Certifications	CE, FCC, UL, BIS, IEC-60529 certified

Video Wall Controller:

Sr. No.	Parameter	Detailed Specifications
1	Display controller	Controllers to control Video Walls in a matrix of one 4x2 and one 6x3 with required number of outputs, 12 Universal inputs & DUAL LAN INPUTS along with necessary software.
2	Processor	Single Quad Core Intel® Xeon/i7 64-bit 2.0 GHz CPU or better
3	RAM	16 Gb
4	HDD	Min 500GB Hard disk Capacity should be upgradable
5	RAID	RAID 0 configured with usable space of 500 GB in each controller
6	Networking	Dual-port Gigabit Ethernet Controller inbuilt Support for Add on Network adapters Support for Optical Fiber interface Adapters
7	Accessories	DVD-R,DVD+RW,, Keyboard, mouse
8	OS	Supports 64-bit Operating Systems Windows
9	Power Supply	(1 + 1) Redundant AC-DC high-efficiency power supply w/ PFC AC Voltage 100 - 240V, 50-60Hz

Sr. No.	Parameter	Detailed Specifications
10	Chassis	19" industrial Rack mount movable Front Panel should have lockable Door to Protect Drives
11	System Reliability	Operating Temperature range : 10° to 35°C (50° to 95°F) Non-operating Temperature range : -40° to 70°C (-40° to 158°F) Operating Relative Humidity range: 8% to 90% (non-condensing) Humidity: 10 – 90% non-condensing Non-operating Relative Humidity: 5 to 95% (non-condensing)
12	Wall configuration	DVI-D Outputs as per video wall matrix with 4 spare outputs
13	Resolution	1920x1200 per output minimum (WUXGA)
14	Universal Inputs	8 Universal Inputs for each video wall (Should be able to accept at least 4 kinds of signals i.e. DVI/RGB/Component Video) along with USB 3.0
15	Redundancy Support	System Should have the redundancy support for Controller HDD, power supply & LAN (Gigabit ethernet RJ-45 connection)
16	Connectivity	Connectivity between the controller & Videowall should be on Optical Fiber cables only.
17	Video Wall, Controller, Cube & wall management	Video Wall, Controller, Cube & Wall management software should be from same OEM with at least 1 such installation (of proposed make/model) in India running for at least 1 year in any city/location/project, for ensuring smooth operations and seamless integration and feature enablement and enhancement . All licenses of the software supplied with Controller and Video Wall should be with perpetual license and cost of the same should be included in the quoted cost.
18	Controller configuration	Two controllers should be provided which can act as backup to each other i.e. a single controller should be able to drive all the cubes of both the video walls.
19	Video Wall stand	Video Wall should be mounted on stand with minimum height of 750 mm (two and half feet) with flexibility of 50 mm height

Video Wall Management Software

Sr. No.	Parameter	Detailed Specifications
1	Client & Server based Architecture	Should supports Multi client/Console control the Wall layouts
2	Scaling and display	Software enable user to display, multiple sources up to any size and anywhere on the display wall.
3	Controls	Software should support to control the Brightness, Contrast, Saturation, Hue, filtering, Crop and Rotate function as per user requirement
4	RS232, TCP/IP	RS232 & TCP/IP support should be available for other interfaces
5	Remote Control	Wall can be control from Remote PC through LAN
6	Auto Source Detection	Software should support for auto source detection
7	Layout Management	Should support for Video, RGB, DVI, ,Internet Explorer, Desktop Application and Remote Desktop Monitoring Layouts
8	Scenarios	Software should able to Save and Load desktop layouts from Local or remote machines
9	Layout Scheduler	All the Layouts can be scheduled as per user convenience Software should support auto launch of Layouts according to specified time event by user
10	Launch Application	Software should able to Support

Sr. No.	Parameter	Detailed Specifications
11	Integration with 3 rd party devices	System should offer interface to enable control from 3rd party devices like smart touch multifunctional keyboard at operator for optimized user interface and quick view of Video wall on operator keyboard/ Touch panel.
12	Live Preview	Software should able to provide live preview of Videowall in the Operator Smart touch keyboard
13	Work space allocation	Software should able to provide live preview of Videowall in the Operator Smart touch keyboard System should provide functionality to the administrator to define and allocate work space for a particular operator or a group of operators when working on a Video wall.
14	User friendly	Software should be user friendly
15	Interface	LAN
16	Scaling and display	Display of multiple sources up to any size, everywhere on the wall
17	Console View	Software enable user to select following view
		Primary Display
		Secondary Display
		Full Desktop
		Selected region
		Selected application
18	KVM Support	Keyboard, Mouse Control
		Enable/Disable Keyboards and Mouse Controls
19	Multi View	Supports multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop simultaneously
20	Short cut Keys	Should support short cut keys
21	Control operator workstations	Software/web/server based should able to Support
22	Multiple concurrent client users	Software/web/server based should able to Support

Indoor LED display for Public

Sr. No.	Parameter	Detailed Specifications
1	Screen Size	Minimum 3000mm x 1700mm or higher
2	Pixel Pitch	1.58 mm Indoor or better. (Lower Pixel Pitch is considered better)
3	LED Configuration	RGB 3 in 1 SMD
4	Pixel Density	398892 pixel / Sq. Mtr
5	Horizontal Viewing Angle	160 Degree
6	Vertical viewing	160 degree
7	Refresh Rate	>3000Hz
8	Operating Temp Range	-10 to 40 Degrees
9	Calibrated Brightness	800 cd/m2
10	Contrast Ratio	3000:1
11	Grey Scale	15-Bit
12	Colors	35 Trillion
13	Dimming Capability	0 – 255 Level
14	Power Input	100 ~ 240 VAC ,
15	Relative Operating Humidity	10% - 90% RH
16	Max Power Consumption	190 W/M2
17	Total Weight per cabinet	Below 8.5 Kgs (Without Mounting Frame)
18	IP Protection	IP40 Front / IP20 Rear
19	Lifetime	50,000 hrs.

Sr. No.	Parameter	Detailed Specifications
20	Service access	Front or Rear
21	International Certifications	UL, CB, CE, FCC, CCC
22	Mandatory Indian Certification	BIS
LED Display Controller		
1	VIDEO SIGNAL INPUT	1 x DVI
2		Resolution: 1920x1200, 2048x1152, 2560x960, & other user defined resolution (under 2.3 million pixels)
3	SIGNAL OUTPUT	RJ45/Fiber-Optic
4	Maximum Load Capacity/Frame Rate	2.3 Million pixels/30-60Hz
5	Maximum Width Output	2048 pixels
6	Maximum Height Output	1200 pixels
7	Input Voltage (AC)	AC 100 – 240V @ 50/60Hz
8	Operating Voltage	4.7 – 6.V
9	Operating Current	0.45 – 0.7A
10	Operating Temperature	-20 – 75 deg C
11	Operating Humidity	0% - 95%
LED Video Processor		
1	Signal Input	3 x Composite 1 x S-Video 1 x YPbPr 2 x VGA (RGBHV) 1 x HDMI (1.3a with HDCP) 1 x DVI (HDMI) 1 x Optional Module (SDI/ HD-SDI/ 3G-SDI or VGA/ DVI/ HDMI) 1 x VGA(RGBHV) 2 x DVI
2	Output Resolution Support	1024 x 768@60Hz / 75Hz 1280 x 1024@60Hz / 75Hz 1600 x 1200@60Hz 1920 x 1080@50Hz / 60Hz 1366 x 768@60Hz 1440 x 900@60Hz 2048 x 1152@60Hz 2304 x 1152@60Hz 2560 x 816@60Hz
3	Switching Features	Seamless Switching, Fade-in / Fade-out switching & Blend switching in random input signals. 4 custom PIP / POP display modes, which can be switched by pressing one button AIAO(Any In Any Out) function allows to display any captured picture in specific area on the screen Other Features
4	Other Features	HD Text, Flash, Graphics & Logo Overlay Picture Freeze function 2304 x 1152 or 2560 x 816 output for single machine. Multi-machine in parallel, multi-unit installed in parallel drive indefinite LED lattice Easy setup and adjustment through knob and keys on the panel. Full design RS232 command for operating and sting 2 LED Transmission Cards Built-in ability (sending cards are optional) 24 / 7 Application
5	Operating Temperature	0 deg - 40 deg
6	Relative Humidity	15% to 85%
7	Power	100-240VAC 35W 50 / 60Hz
Power Distributor		
1	Cabinet size	605MM*525MM *300MM (WXHXD)

Sr. No.	Parameter	Detailed Specifications
2	Cabinet Material	SGLCC/ GI-120 GSM, T=1.2mm
3	Cabinet Finish	RAL 7035 (Grey)
4	Cabinet Mounting	Wall Mount/Pole Mount
5	Ingress Protection	IP-54
6	AC input	220 V – 240 V
7	AC out put	6 x 220V
8	AC Power Max	25KW
9	AC power Max Each output	5 KW
10	Surge protection	Class C
LED Control Software		
1	Supports Relevant LED Controllers	
2	Support Multiple LED walls	
3	REAL/Virtual Mode to support larger resolutions	
4	User Friendly wall configuration	
5	Complex wall configuration	
6	Output resolution Configuration	
7	Redundant Port Configuration	
8	Manual Brightness, Gamma and Color temperature adjustment	
9	Automatic Brightness adjustment schedule based	
10	Automatic Brightness adjustment ambient light based	
11	Power Control	
12	Automatic and Timer based Power ON/OFF	
13	Power Control for Third party equipment's	
14	Display Control Kill, Lock and Run. Run with Inbuilt Color patterns	
15	Health Parameters Monitoring of Display	

Camera Type 3 - Dome Camera (Command Center):

Sr. No.	Specs Category	Detailed Specifications
1	Sensor	CMOS sensor with size of 1/3" inches or higher with progressive scan
2	Pixels	Total number of effective pixels should be 2MP or higher
3	Signaling Standards	Should be capable to support NTSC and PAL signaling Standards
4	Lens	Varifocal lens with focal length 3mm-12mm
5	Remote/ Auto Focus & Zoom	Allow automatic/motorized focus and zoom remotely
6	Illumination	Illumination capability for Color: 0.5 lux, B/W: 0.05lux or better
7	Lens Type	Auto-Iris or better
8	FOV	FOV between given ranges for horizontal FOV: 36° to 82° , & Vertical FOV:22° to 55°
9	Image Improvement Functionalities	Backlight compensation, Exposure Control, WDR, White Balance, Noise Reduction, AGC, Sharpness, Brightness, Contrast, image overlay & Saturation
10	Highest Image Resolution & FPS	As minimum to 1280x960 with minimum image interval as 30FPS
11	Day/Night Functionality	Capability to auto switch the images in to Color & Monochrome images in Day/Night
12	Video Compression	Capable of H.265, H.264 file & Motion JPEG video compression
13	Edge Recording	Capable of providing edge recording and support memory card slot (Can support up to 64GB or better support) for on board recording during non-availability of network connectivity
14	Audio	Two way audio with multiple transmission modes like Simplex/Duplex (In Built Microphone is preferable)

Sr. No.	Specs Category	Detailed Specifications
15	Audio Compression	G.711/G.726/AAC
16	Power ON	Through 12VDC/24VAC/POE (IEEE 802.3af/802.3at)/POE+
17	Network Connector	Should be minimum 10/100 Base-T, (Should be POE)Ethernet RJ45 or better
18	Audio Connector	3.5mm jack for audio input and output minimum one-one each
19	Alarm Input & Output	1x alarm input and 1x alarm output for triggering external devices through input or output
20	Onvif Conformance	Profile S, G
21	Operational Temperature	0 °C to 50 °C
22	Networking Protocols	IPv4/v6, HTTP, HTTPSb, SSL/TLSb, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, , SNMPv1/v2c/v3, DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP/Protocol should meet all functional requirement
23	Multicast Streaming	Should support to Multicast Streaming
24	Vandal Resistant Rating	IK10 or better
25	Dual Streaming	Support to at least dual streaming support with different combinations of resolutions and fps
26	Firmware Upgrade	Remotely through any method like web based/software based/FTP based
27	SD Card Slot	At least One Slot
28	Certifications/ Standards	EN, UL & BIS
29	OEM	OEM of Camera should be in the business of supply of Cameras in India for the last 5 years or more. OEM should be a full member of ONVIF on the date of bid submission.

IP Phones (with display) :

- Minimum 3.5" screen 4 Line phone
- High-fidelity Audio
- IEEE Integrated Switches
- Low Power PoE Class 1
- Backlit Graphical Displays
- Electronic Hook-switch
- Enterprise-grade Security
- IPv6 support
- SIP
- AES/SRTP Encryption

IP phones (without display):

- Minimum 3.25 x 1.25 inch , 396 x 162 pixels
- High-fidelity Audio
- IEEE Integrated Switches
- Low Power PoE Class 3
- SIP
- Support for 2 wired extension microphones
- AES/SRTP Encryption

Multifunctional Keyboard with touchscreen panel screen:

Sr. No.	Parameter	Detailed Specifications
1	Interface Type	The multifunctional keyboard with an integrated touch LCD screen provides virtually unlimited functionality and an intuitive user interface
2	Main Function	With just a single multifunctional keyboard and mouse, it is possible to access multiple workstations, other sources and/or large screens, all without loss of performance.
3	Display Unit	Integrated, touch-sensitive 10.1" LCD
4	Resolution	1280 x 800 pixels at 60 Hz
5	Color depth	24 bit (RGB888) or better
6	Contrast ratio	500:01:00
7	Brightness:	320 cd/m2
8	Visible angle	170°(Horizontal & vertical)
Keyboard Switches		
9	Type	Industrial Grade
10	Contacts	High-quality alloy for rugged operation
11	Action	Pressure point click
12	Pressure force	50 ± 20 cN
13	Life time	minimum 20 million actuations
14	Speakers	2 x 8 watt RMS at 8 Ω
15	Network connections	1 x RJ45 1000 BASE-T Ethernet with PoE+.
16	Audio	2 x 3.5" jack line stereo 48 KHz 16 bit and microphone stereo
17	USB	3 x USB-A (2 x USB for keyboard / mouse; 1x transparent USB 2.0 full speed 16 end points)
18	USB (service port):	1 x USB (2.0 full-speed) type mini-B 5–pole or equivalent
19	Standards & protocols	IEEE 802.3ab: 1000 BASE-T, Gigabit Ethernet
20	Ethernet protocol	IPv6/IPv4 (fixed addressing), dedicated connection or via Ethernet Switch / IP router, ARP, ICMP-Echo (ping), IGMPv3 report (multicast)
21	Motion sensors	Two units(Left & Right)
22	Dual AC Power	100 - 240 V AC, 1.5 A
23	Supply (in Watts)	Typical: 8.5 watt IEEE 802.3 at (PoE +) in case of Power Supply over Ethernet
24	MTBF	50,000 hours or more
25	Operating Condition	Operating temperature: 10 - 40 °C Storage temperature: 0 - 60 °C Installation location: Interior Relative humidity: 45 - 85 %, non-condensing
26	Smart Connector for Keyboard	The keyboard connector card shall be primarily used with the multifunctional keyboard to operate directly-connected local computers at Operator Desks & give access to Video wall as on when required
27	Connectivity	The keyboard connector card shall be equipped with an integrated 2-port Gigabit Ethernet switch and can be connected with the IP-based keyboard, mouse, video signal, USB, audio-matrix solution and the multifunctional keyboard via Ethernet.
28	Signal /communication	The keyboard connector card can send and receive data (USB, audio, and serial) from two computers via Gigabit Ethernet to and from the multifunctional keyboard.
29	Capacity	Up to 8 keyboard connector cards can be connected via Ethernet with the multifunctional keyboard (or 16, if only keyboard/mouse channel 1 and audio channel 1 is used).

Variable Message Sign boards:

Sr. No.	Parameters	Minimum Specification
1	Display Size (W x H)	Minimum 25Ft X 9 Ft
2	Pixel Pitch	10 mm or lower
3	LED Configuration	RGB 3 (1R/1G/1B)
4	LED Type	DIP/SMD
5	Pixel Density	Minimum 10,000 pixels per sqm or higher
6	Half Gain Horizontal / Vertical Viewing Angle	H 140 deg / V 45 deg or better
7	Refresh Rate	<=1920 Hz or better
8	Temp Range	0 to +50 Degrees C or better
9	Gray Scale Processing	12 Bit or better
10	Brightness (Calibrated)	5000 cd/m² or better (Ensure excellent Image quality).
11	Maximum Power Consumption	850 w/sq. m or lower
12	Dimming Capability	256 levels
13	Power Input	100 ~ 240 VAC
14	Individual Tile/Cabinet Dimensions	As per OEM
15	Contrast Ratio and MTBF	1500:1 or better; MTBF>=10000hrs
16	Access For Maintenance	Rear
17	IP Level	Front IP65 / Rear IP54
18	Quality/Health & Safety/Environmental Certifications of OEM/OEM subsidiary in India (Copy to be submitted along with the bid	Quality Management System 9001:2015 ,
		Occupation health & Safety Management System - OHSAS 18001:2007,
		Environmental Management System 14001: 2015
Rack Frame Power Distribution Unit		
1	Front Door	2 Hinges with Rack & Aircon bolted
2	Wall Mount Clamp	Welded on Rack frame rear side
3	19" pillar front & 19" pillar rear	Bolted on rack side wall
4	Locking Arrangement	To be provided with a locking system
5	Limit Switch	The rack door to be provided with a limit switch

6	Earth	Earth studs should be provided in the rack for earth purposes
7	Cable points	Cable entry and exit points should be provided in the rack
8	Mounting	Should be possible to mount the rack either on a pole or on a wall with options of different mounting types
9	Rack Internal size	19" rack
10	Material	GI 120 gsm thickness 1.5 mm
11	IP rating	IP54
12	AC input	~100-240V
13	AC Power Load Min.	510KW
14	AC power Load Min. Each output	3KW
15	Surge protection	Class C
16	Over temperature protection	Selectable from 30 deg to 60 deg C
17	Remote Control	Power Distribution Unit can be controlled from remote location over IP
LED Controller (Same Make as LED screen)		
1	Control Port	RS232
2	Signal Input	DVI with resolution capability of 1920 x 1200 or better
3	Signal Output	RJ45
4	Minimum Load Capacity	2 Million Pixels
5	Input Voltage	100~240 VAC
6	Operating Temperature	5~40 Deg C
Mechanical Structure For Mounting Of LED screen		
1	Mounting Structure	LED screen should be mounted on unipole/bipole or other structure as per the site requirement. Structure should be earthed properly and provided with lightning arrestor as well.
2	Material	Should be made from mild steel and painted black along with anti-rust coating.
Communication Interface		
1	Ethernet Interface	
a	Number of Ports	One 8 pin RJ45
b	Speed	10/100 Mbps, auto MDI/MDIX
2	Serial Interface	
a	Number of Ports	One
b	Serial Standards	RS-232
3	Serial Communication Parameters	
a	Parity	Even, Odd, Space, Mark

b	Flow Control	RTS/CTS and DTR/DSR (RS-232 only), XON/XOFF
c	Baudrate	100 bps to 250kbps
4	Serial Signals	
a	RS-232	TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND
5	Software	
a	Network Protocols	Should Support ICMP, IPv4, TCP, UDP, DHCP, BOOTP, Telnet, DNS, SNMP V1, ARP, HTTP, SMTP
b	Configuration Options	Web Console, Serial Console, Telnet Console, Windows Utility
6	Physical Characteristics	
a	Housing	Metal
b	Weight	350 g or less
c	Dimensions	With ears minimum: 75 x 80 x 20 mm
7	Environmental	
a	Operating Temperature	0 to 55°C
b	Ambient Relative Humidity	5 to 95% (non-condensing)
8	Power Requirements	
a	Input Voltage	12 to 48 VDC
b	Input Current	128.7 mA @ 12 VDC
9	Certifications	
a	Safety	UL 60950-1
b	EMC	EN 55022/24
Outdoor Cabinet Air Conditioner		
1	Power Supply	230VAC ±15% 50Hz/60Hz
2	Working Temperature Range	0 to + 55 deg C
3	Max Noise Level	60dB(A)
4	IP Grade	IP55
5	Weight	< 16 Kg
6	Refrigerant	R134a for harsh conditions
7	Dimensions	Minimum 500 x 300 x 160 mm (Hx WxD)
8	CE & ROHS Compliant	Yes
9	Surface treatment	Outdoor type powder coating
10	Cooling Capacity	500W@L35/L35
11	Power Consumption	210W@L35/L35
12	Power Supply	230±15% AV 50/60 Hz
13	Internal Airflow	120 m³/h

14	Display Panel	Should be provided with a display panel to show parameters like cabinet temperature, indications for - cooling, running of external fans, flashing on alarm
15	Anti-theft design	The mounting of the AC should have an anti-theft design
16	Communication from AC	AC should be able to send diagnostic communication to remote location over IP
Network Switch		
1	Switching Capacity	1 Gbps
2	No. of ports	5
3	Power Supply	DC 5 V / 0.55 A
4	Maximum Packet Forwarding Rate	148.8 kpps
5	802.3x flow control	yes
6	Auto MDI/MDIX	yes
Router		
1	Parameter	
a	Uplink	1*LTE module (dual SIM), 1*RJ45 FE (configurable)
b	LAN-RJ45	3(4)*RJ45 FE
c	LAN-Wi-Fi	11n 2T2R
d	Mgmt. Port	1*RJ12 RS232 (Console)
e	Log Storage	1*USB 2.0
f	Cellular Band2	LTE: 800/900/1800/2100/2300/2600 MHz,UMTS: 850/900/1900/2100 MHz, GPRS/EDGE: 850/900/1800/1900 MHz
g	Antenna	2*5dBi detachable ant.(WiFi), 2*3dBi detachable ant. (3G/4G)
h	Power Source	Dual DC 9V ~ 48V
2	WAN Functions	
a	WAN	Multiple WANs, Failover / Load Balance,
		Configurable Ethernet/4G
b	Cellular	2G/3G/LTE,
c	Ethernet	Dynamic IP, Static IP, PPPoE, PPTP, L2TP
d	IPv6	Dual Stack, 6-in-4, 6-to-4
3	Basic Functions	
a	Ethernet	LAN IP, Subnet Mask
b	WiFi System	802.11n 2T2R MIMO 300Mbps (2.4GHz)
c	WiFi Operation	AP Router, WDS, WDS Hybrid Modes
d	WiFi Security	WEP, WPA,WPA2, WPA-PSK, WPA2-PSK, 802.1x
e	VLAN	Port-based, Tag-based

f	NAT	Virtual Server/Computer, DMZ Host, PPTP/L2TP
g	Routing	Static, Dynamic: RIP1/RIP2, OSPF, BGP
h	QoS	Policy-based Bandwidth Control and Packet Flow Prioritization
i	Redundancy	VRRP or equivalent
4	Object Definition	
a	Scheduling	Time Schedule List
b	Grouping	Host Grouping List
c	External Server	Email, Syslog, RADIUS, SCEP, FTP
d	Certificate	My Certificate, Trusted Certificate, Issue Certificate
e	Security	
f	VPN Tunneling	IPSec, OpenVPN, PPTP, L2TP, GRE; Tunneling with Full Tunnel, Tunnel Failover
g	VPN Scenario	Site to Site, Site to Host, Host to Site, Host to Host, Hub and Spoke, Dynamic VPN
h	VPN Capability	IPSec: up to 16 tunnels
i	Firewall	SPI Firewall with Stealth Mode, IPS
j	Access Control	Packet Filter, URL Blocking, MAC Filter
k	Authentication	Captive Portal
5	Service	
a	Cellular Toolkit	SMS, Data Usage, SIM PIN, USSD, Network Scan
b	Event Handling	Managing / Notifying Events: SMS, Syslog, SNMP Trap, Email Alert, Reboot
6	Administration	
a	Configure & Management	Web, Telnet CLI, Command Script, TR-069, SNMPv3 standard & AMIT MIB
b	System Operation	MMI, System Information, System Time, System Log, Backup & Restore, Reboot & Reset
c	Diagnostic	Packet Analyzer, Diagnostic Tools
7	Environment	
a	Operation Temp.	0°C ~ 60 °C
c	Humidity	10% ~ 95% (non-condensing)
Auto Brightness Sensor		
1	Rated voltage	5V
2	Operating temperature	-30°C~70°C
3	Operating humidity	0~99%
4	Brightness range	0~65535 lux
5	Cable	5m

6	Features	Monitor the ambient brightness to achieve automatic brightness adjustment of LED display
		Asynchronous
		Outdoor use proofing
		No external power supply required

4. OPERATION & MAINTENANCE PHASE

4.1. SCOPE OF WORK, DELIVERABLES & TIMELINES

The selected MSI shall operate and maintain the ICT Infrastructure including but not limited to Server room, Active, Passive, Applications, hardware and software etc. for the period of 5 years from the date of Go-live and completion of implementation. The minimum specified work to be undertaken by the selected MSI for providing IT FMS services has been categorized as under:

- i. IT FMS Services for equipment's/items and related services for the equipment's installed or to be installed at DSIR during the contract period
- ii. Co-location support to user departments/agencies for the equipment's installed in DSIR wherever FMS services are not applicable.

Facility Management Services for equipment's/items:

Following are the major activities to be carried out by the MSI during Operate and maintenance period;

4.1.1. Asset Management Services

- a. Tendering authority will provide the current list of assets to the selected MSI. The MSI shall be required to create and maintain database of all the assets procured/installed at DSIR as per following details:
 - i. The database should have information like make, model, configuration details, serial numbers, licensing agreements, warranty and AMC details, place/location of installation etc.
 - ii. The MSI shall be required to create and maintain Software inventory with information such as Licenses, Version Numbers and Registration Details along with their configuration details and history.
- b. The MSI shall be required to record installation and removal of any equipment and inform tendering authority even if it is temporary.
- c. The MSI shall be required to perform software license/patch management and notify tendering authority on licensing contract renewal before 3 months of expiry.
 - d. The MSI shall be required to register all software (in case not registered) with respective OEMs however renewal cost for the licenses shall be taken care by MSI
- e. The MSI shall use existing software for Asset Management Services with integration of DCIM tool, if possible.

4.1.2. Preventive Maintenance Services

MSI in co-ordination with equipment service provider shall provide preventive maintenance services for all the equipment's for which maintenance services are to be provided by MSI at least once in every quarter. The preventive maintenance shall include

- a. Cleaning and removal of dust and dirt of the equipment with appropriate precautions.
- b. Conduct inspection (check for loose contacts in the cable and connections etc.), health checking of all components of the equipment's, testing, satisfactory execution of diagnostics and necessary repairing of equipment.

- c. MSI shall intimate and take due approval from purchaser before carrying out preventive maintenance activity.

4.1.3. Corrective Maintenance Services

The details of the work to be undertaken by MSI are as follows:

- a. Troubleshooting of problems related to the equipment's/network/services and rectification of the same.
- b. MSI shall co-ordinate with respective OEM for supplied items/maintenance service agency for repairing/ replacement of defective parts/components.
- c. Get Replaced parts/components beyond repair with parts/components of same or better specifications ensuring compatibility.
- d. Get arranged suitable standby for parts/components with same or better specifications till the time the original part/component is repaired or replaced so that daily business is not affected.
- e. The Maintenance support for equipment's shall include all passive components like screws, clamp, fasteners, ties anchors, supports, ground strips, wires, fiber connecting kits, gears, spares, power-cables, lightening, Network cables etc.
- f. Maintenance support services pertaining to Cabling and OFC shall include:
 - i. Splicing, repairing & testing of OFC.
 - ii. Re-fixing/shifting of cables/OFC whenever switches and racks are shifted or otherwise.
 - iii. Removing and laying of UTP cable and I/Os with casing, etc. in case renovation activity is undertaken in any of the data centers/server room covered under the project.
 - iv. Replacement/repair of OFC/UTP/Power cables & connectors/ ports/ equipment on entire laying route within the data center/server room
 - v. Maintenance of cables and conduits of equipment
 - vi. Documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems.

4.1.4. Configuration and reconfiguration/rollback of equipment's/network/services

- a. The MSI shall be responsible for configuration/re-configuration/rollback of all the equipment's /Software /services as and when required.
- b. The MSI shall maintain a record of hardware and software configurations of all equipment's including the details of different policies implemented on the devices such as VLAN configurations, access control lists, routing filters, clustering details etc. MSI shall keep regular backups of the configurations of each of the devices.
- c. MSI shall adhere to the change management procedures already defined to ensure that no unwarranted changes are carried out on the devices. All the changes must be formally approved by the MSI designated team leaders and recorded. The Purchaser /designated agency shall communicate such change management procedures and their amendments made time to time.
- d. MSI shall do proper version management of all the configurations.

- e. MSI shall ensure that these configurations are not accessible in general and must be kept confidential with the Purchaser and project manager as per security policy of Data center.
- f. MSI shall have the capabilities to configure or reconfigure hardware/software installed in data centers during the contract period.

4.1.5. Vendor Management Services

MSI shall coordinate with external vendors for upkeep of equipment's/software/services to meet the SLA and shall liaison with respective vendors/OEMS for repairs/replacement of items and/or update/upgrade/troubleshoot the software/services. To perform this activity, the MSI shall

- a. Maintain equipment/software/service wise database of the various vendors and service providers with details like contact person, telephone numbers, escalation matrix, response time and resolution time commitments, expiry date of Maintenance Services/Warranty/Software Assurance/Support etc.
- b. Log and escalate the calls with respective vendors/OEM/service providers within 1 hour from occurrence of incident/ problem, repetitive pursuance and coordinate with them to get the equipment repaired/problems resolved.

4.1.6. Network Management Services

The scope of work under network management services would include –

- a. To ensure continues operation and upkeep of the LAN Infrastructure at the DSIR including all active and passive components so that the network is available 24 x7 as per the prescribed SLA.
- b. Configuration/Reconfiguration/deployment and Management of various policies like Security policies, Access policy, IP Policy, routing policy, firewall policies etc. as per ISO requirements for providing accessibility between external links and their infrastructure hosted at the Data Center/server room in co-ordination with respective vendors including but not limited to opening/closing of specific ports on network devices.
- c. Configuration, management and maintenance of Network Management Software deployed at the Data Center/server room.
- d. Performance tuning to ensure resilient performance, reliability and high availability of the network services. A performance matrix has to be provided by vendor to the Tendering Authority on monthly basis and as and when required.
- e. Coordination with DRDC.
- f. The MSI shall also be responsible for integration, management, maintenance configuration/reconfiguration of any additional Internet Bandwidth/networks which needs to be integrated with DSIR network during entire contract period.
- g. The MSI shall be responsible to monitor the availability of various links and their packet drop, latency and utilization at the Data Center/server room network .The MSI shall also maintain logs on the basis of time, interface, IP address, application wise etc. for traffic analysis for the requisite period defined in respective policies.

4.1.7. Server Management Services

MSI has to provide these services for existing servers and servers to be procured in future.

- a. MSI shall manage the servers on end-to-end basis including server administration, performance tuning, hardware and software support and upkeep of the server. The MSI

shall also undertake installation/re-installation of all the servers in terms of operating system, databases, clusters, virtualization, Application Server software, latest Software updates/upgrades, patches etc.

- b. MSI shall provide device/peripherals management, user management, file system management, files management services for the servers.
- c. MSI shall implement operating system security/hardening and application server software level security for the servers.
- d. MSI shall deploy and upload/configure/host and manage web sites, application software and databases on the servers as per requirement and policies. The MSI shall also coordinate and provide all assistance/services to the purchaser and the users of respective websites/applications for smooth operations and resolution of day-to-day problems.
- e. MSI shall assign rights on servers to different user's w.r.t. FTP, Remote Access etc. as per defined policies.
- f. MSI shall also maintain and manage Domain Name Server (DNS).
- g. MSI shall be responsible to maintain optimum utilization of all the equipment's w.r.t. keeping close watch on optimum performance of Hardware/OS/Network software/processes/database with detecting contention, wait state and queue of jobs on the equipment's, Network, I/O, storage/concurrent load on the devices, etc. and implementing necessary measures to rectify the issues. A performance matrix has to be provided by vendor to the Tendering Authority on monthly basis and as and when required.

4.1.8. Backup & Recovery Management Services

- a. MSI shall ensure periodic backups of all the servers OS through the backup servers installed in the Data Center/server room as per policy/ guidelines.
- b. MSI shall take backup of VM's, Server Configuration, Databases, and Storage etc.
- c. The MSI shall restore the backups as and when required with having minimum downtime.
- d. MSI shall be responsible for proper labelling and housing of the backup media for identification and retrieval.
- e. MSI shall be responsible for Backup tool and Storage Manager Installation, configuration, administration, maintenance and troubleshooting.
- f. Transfer of data from one Data Centre to another Data Centers/ DR Sites.

4.1.9. Help Desk Support

- a. The MSI shall provide 24 x 7 help desk support from ABCD building
- b. The MSI shall maintain ITIL Compliant helpdesk tool including configuration/reconfiguration/ upgrade/update.
- c. MSI shall log all calls received through any medium viz. telephone/email/in writing/in person, shall generate a ticket mentioning type of problem, Severity level etc. using helpdesk tool and forward the same to concerned FMS team/person, Project OIC(s) and user.
- d. The MSI shall provide various services to different users on demand basis as and when required as mentioned in RFP. The request would be made on help desk by the user by dedicated help line number/Specific email account and MSI shall get approval from the officer in charge of the Data Center/Server Room as designated by the purchaser. The

resolution time for such services would be as per SLA. However, the purchaser/authorized entity may scale up the severity level depending upon the requirements.

- e. The indicative lists of such services but not limited to as under -
 - i. Change Request for opening/closing of a Port on device
 - ii. Request for FTP rights
 - iii. Request for Internet Access as per policy
 - iv. Request for DNS Entry
 - v. Request for uploading of Web Site/Applications/Databases on Web/Application/database servers in non-virtualized, virtualized, cloud environment in the Data Center/server room as per the requirement.
 - vi. Change request for Routing Policies
 - vii. Change Request for Firewall Policy
 - viii. Request for Installation/Re-Installation of Server, OS, etc.
 - ix. Request for Installation/Re-Installation of Databases
 - x. Request for assigning rights on devices/servers/database/network

4.1.10. Database management services

- a. MSI shall undertake tasks of managing changes to database schema, creation/alteration of Database, disk space, storage, user roles, parallel distribution of data on storage to balance the I/O load.
- b. MSI shall periodically perform configuration checks and fine tune the databases with respect to performance and proactive identification of potential problems
- c. MSI shall provide performance monitoring, Maintenance and tuning of the databases on a regular basis as well as proactive health check-ups.
- d. MSI shall manage database upgrade, patch upgrade, patches, and updates as and when required with planned minimal downtime.
- e. MSI shall provide database performance and health reports to the purchaser as per standards.
- f. MSI shall assign rights on database for different users.
- g. MSI shall upload / create/alter users and assigning privileges and Roles
- h. MSI shall create logical objects/procedures/triggers/functions/packages in the database on the request of designer/developer of the applications.
- i. MSI shall be responsible for taking database backups, restoration and recovery of Database as per the policy.
- j. The backup policy would be framed by the MSI keeping in view of severity of different databases and MTTR. The policy would be approved by DICDL and gradually be updated as per requirements.
- k. MSI shall be responsible to maintain optimum utilization of all the equipment's w.r.t. database operations and keeping close watch on optimum performance of Hardware/OS/Network software/processes/database objects with detecting contention, wait state and queue of jobs on the equipment's/memory objects/ processes/ Network/ I/O/ storage/concurrent load on the devices, etc. and implementing necessary measures

to rectify the issues. A performance matrix has to be provided by the MSI to DICDL on monthly basis and as and when required.

- l. MSI shall implement monitoring of uses of devices/objects/users as and when required.
- m. MSI shall be responsible for implementing Database Audit of devices/ objects/ transactions/ users to identify malicious/suspected activities as and when required through database tools or writing its own scripts.

4.1.11. Storage Administration and Management Services

The MSI shall be responsible for the configuration/reconfiguration and management of the storage solution and shall provide the following services:

- a. Manage key resources in the Storage solution
- b. Manage interconnects between key resources in the Storage solution
- c. Receive asynchronous notification that the configuration of the Storage solution has changed
- d. Manage the health of key resources in the Storage solution
- e. Manage the available performance of interconnects in the Storage solution
- f. Receive asynchronous notification that the performance of the Storage interconnect solution has changed
- g. Manage the zones being enforced in the Storage solution
- h. Manage the storage volumes in the Storage solution
- i. Manage the connectivity and access rights to Storage Volumes in the Storage solution
- j. To facilitate the purchaser in connecting to the Storage later and provide access rights as required.
- k. To ensure optimum uses of storage and to provide advisory.

4.1.12. Security Administration and Management Services

The objective of this service is to provide a secure environment in compliance to the ISO security policy. This service includes:

- a. Addressing the ongoing needs of security management including, but not limited to, monitoring, troubleshooting of various devices/ tools such as firewall, IPS/IDS, virus protection, and vulnerability protection through implementation of proper patches, procedures and rules.
- b. Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.
- c. Ensuring that latest patches/ workarounds for identified vulnerabilities are applied immediately. Any up-gradation of software such as antivirus signatures etc. in the Data Center/server room shall be the responsibility of the MSI during the entire period of FMS. MSI shall enforce update/upgrade management.
- d. Respond to security breaches or other security incidents by taking corrective measures, providing guidelines to users and coordinate with respective OEM in case a new threat is observed to ensure that workaround /patch is made available for the same.

- e. 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, from viruses.
- f. Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 27001, BS 7799 and BS 15000 guidelines.
- g. Compliance of security regulations defined by Government of India or any other Govt. Authorized agency such as CERT-IN etc.

4.1.13. ISO 27001 and ISO 20000 certification and sustenance for 5 Years

- a. It is the responsibility of MSI to get a fresh ISO certificates for DC/server room, and sustenance of the same till the Project End Date at his own cost.
- b. For the maintenance of these certifications, the MSI is required to adhere to all the policies and ensure documentation and maintenance of reports as required for maintaining the certification.
- c. MSI would be responsible for operating, monitoring, reviewing, maintaining and improving the Information Security Management System and Facility Management Services at the Data Center/server room till project end date.
- d. MSI must coordinate with authorized certifying agencies for maintaining the continuity of the certifications and receive the continuity certificates from authorized certifying agencies till the end of the project period. The MSI will correspond with and provide all relevant information to the certifying agencies for the purpose. All the cost towards maintenance and for new/continuity/extension of the certificates will be borne by the MSI for the entire project period. Fees and other expenses payable to the certification agency shall be borne by the MSI.
- e. Activities to be performed for ISO certification
 - i. Current state assessment of ISO 20000/27001 processes, technologies, skills and operations
 - ii. Gap analysis and recommendations for improvement based on ISO 20000/27001 requirements
 - iii. Design and development of new/modified policies/ processes
 - iv. Recommendations on updating of new/modified ITSM/ISMS as and when required
 - v. Deployment of new/changed processes
 - vi. Training of operating personnel on processes
 - vii. Handholding the operating personnel for audit readiness
 - viii. Certification
 - ix. Support for 5 years
- f. Min. MSI Resources on site for implementing/achieving ISO 27001 and ISO 20000 Certification is as follows:
 - i. Process/tools consultant ISO 27001: 1No.
 - ii. Process/tools consultant ISO 20000: 1No.

4.2. Table for O&M (Operation and Maintenance) Reports

Sr. No.	Scope of Work	Activity	Deliverable	Timeline
1	Facility Management Services and Colocation Support	Asset Management Services	List of Hardware/Software with all details as mentioned in Scope of Work under Asset Management Services clause.	Within 15 days from the end of respective quarter
		Preventive Maintenance Report	Equipment wise and date wise detailed reports of preventive maintenance services provided during the quarter along with copy of call report. Assessment report of performance and future requirement with respect to the equipment's covered under preventive maintenance.	
2		Corrective Maintenance Reports	Equipment wise and date wise detailed and MIS reports of corrective maintenance services got provided during the quarter	
3		Configuration and reconfiguration/ rollback of equipment's / network / services	Configuration document (latest) for selected equipment's/ software, as may be finalized by tendering authority as per approved format.	
4		Vendor Management Report	Date wise details of calls logged with external vendor and their resolution time to monitor compliance with the SLA signed with the respective vendor, if any.	
5		Network Management Report	Network up time report of all network devices and network connectivity links/ leased lines Performance Matrix report monthly/quarterly	
6		Server Management Report	a. updates/upgrades, patches history report b. Server up time report along with logs	
7		Backup and recovery services	Exception report along with related logs	
8		Help Desk Support	Detailed SLA compliance report and logs	

9		Database Management Report	Performance, Growth and Patching reports as per the scope	
10		Storage Management Report	Utilization and capacity reports as per the scope	
11		Security Administration	Exception report as per the scope	
12		Service Levels	Service Level Reports	

Note: MSI has to provide all the reports and deliverables mentioned above and provide any additional reports as required by DICDL as and when required.

4.3. Manpower Resource Table at DSIR

Sr. No.	Role	1 st Year	2 nd Year	3 rd Year	4 th Year	5 th Year
1	Project Manager	1	1	1	1	1
2	Application/Database Expert	1	1	1	1	1
3	Network Specialist	1	1	1	1	1
4	Data Center/Server Room Specialist	1	1	1	1	1
5	EMS/NMS Support Engineer	1	1	1	1	1
6	IBMS/Surveillance Specialist	1	1	1	1	1
7	Helpdesk Support	5	5	5	5	5

4.4. Minimum Qualification, Relevant Experience & Certifications

Sr. No.	Role	Min. Qualification, Relevant Experience & Certifications	Penalty on Non availability of each resource per day
1.	Project Manager	B.E./B. Tech/MCA + MBA/PGDBM/PGDM + 10 Years relevant experience in IT/ITeS + PMP/ PRINCE2 Certified	5000
2.	Application/Database Expert	B.E./B. Tech/MCA + 8 Years relevant experience + OEM certified L3 engineer	3000
3.	Network Specialist	B.E./B. Tech/MCA + 7 Years relevant experience in OFC implementation	2000

4.	Data Center Specialist	B.E./B. Tech/MCA + 7 Years relevant experience in Network Management + CCNA/CCNP or equivalent	2000
5.	EMS/NMS Support Engineer	B.E./B. Tech/MCA + 8 Years relevant experience + OEM certified engineer	3000
6.	IBMS/Surveillance Specialist	B.E./B. Tech + 8 years of experience in relevant domain (Surveillance/ & IBMS)	3000
7.	Helpdesk Support	Graduate diploma / Diploma in Computer Science with 2 years of relevant experience	500

5. IMPLEMENTATION SCHEDULE (ACTIVITIES, MILESTONES AND DELIVERABLES)

The MSI is to produce a detailed implementation schedule based on the key milestone activities and timings in this section.

The calendar dates showcased in the implementation plan are indicative, actual dates may vary based on the actual date of award of contract.

Implementation Plan

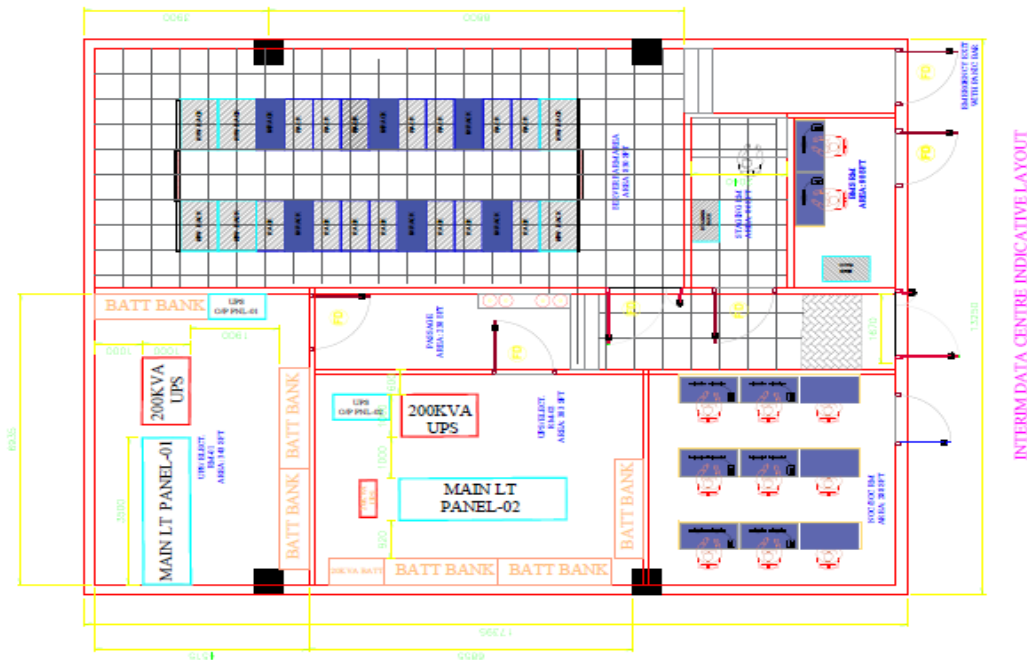
Work Package	Domain	Sub Domain	2020					2021											
			Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Basic Network Infrastructure Work package	City wide networks - Network Active/ Passive	Smart city network for all ICT enabled city provided services																	
		Switching and routing																	
		Network security																	
		Network for Buildings like ABCD Complexes																	
	City wide sensors																		
	Set up of Server Room	Server room physical infrastructure																	
		Common servers for IT considering work packages																	
		Storage and backup (including data archiving)																	
		Server room and DC Integration																	
	Enterprise and Network Management System																		
City Integrated Operations Platform																			
City Applications Work Package	ERP	ERP/ Shared services																	
		City Asset Management																	
		Scheduling for managed assets																	
	Customer Relationship Management																		
	Industry Specific Solutions for Utilities																		
	Master data governance & Data Migration																		
	City applications & Integration with existing State Government eGovernance applications	City Applications - Webportal																	
		City Applications- Single Window clearance																	
		City Applications - Multi service kiosk																	
		City Applications - Integration of existing State Government eGovernment applications																	
Mobile application platform																			
Process workflow																			
Integrated Operations Work Package	Surveillance Solution deployment																		
	CIOC – City Integrated Operations Center																		
	CIOC - Surveillance and video analytics																		
	CIOC - AV hardware & software																		
	CIOC - Helpdesk Solution, IPBX System																		
	Integrated Building Management System software (IBMS) at Service Areas																		
	Variable Message Sign Board	Variable message sign boards & City Wide Signage																	
	System integration																		
Parallel Run																			

Operate and Maintenance period

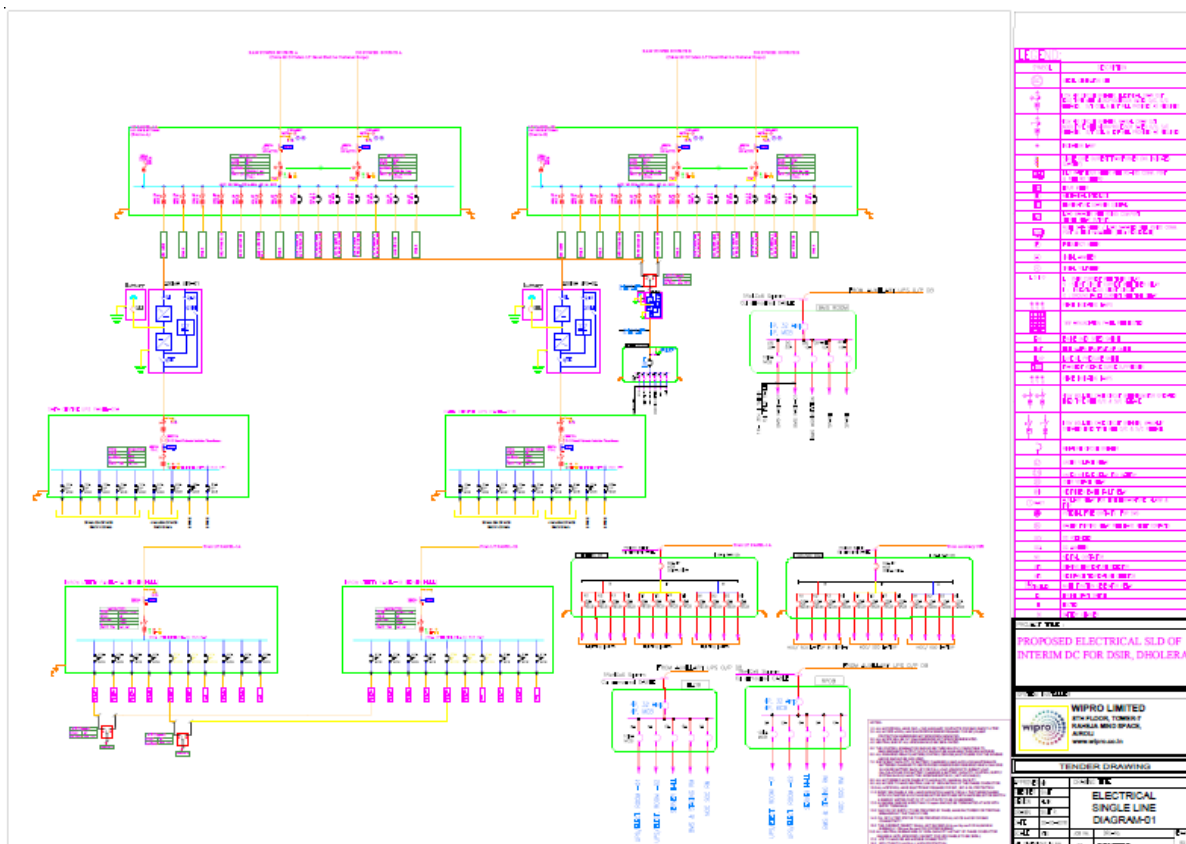
Work Package	2021				2022								2023								2024								2025								2026												
	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov
Operate and Maintain	Year 1				Year 2								Year 3								Year 4								Year 5																				

5.1. Annexures

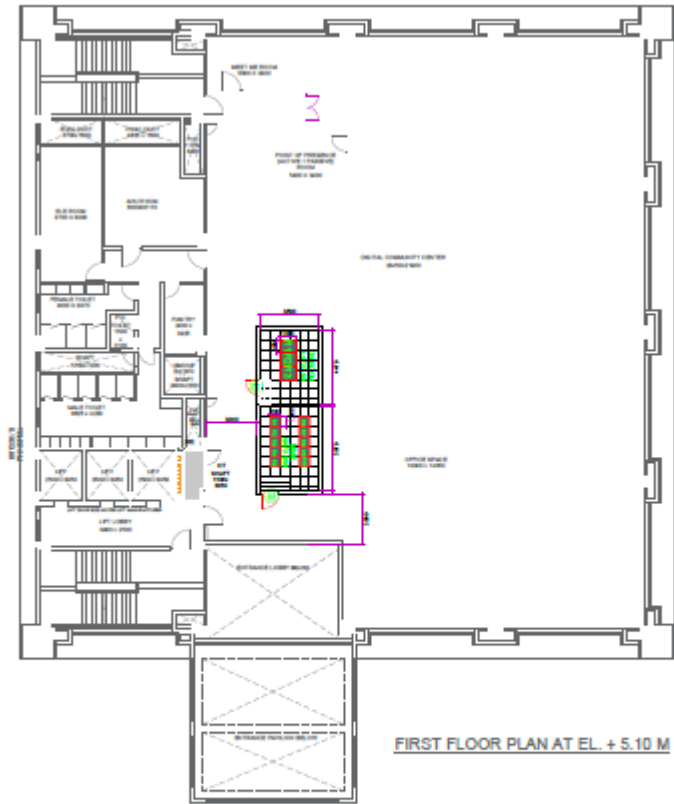
5.1.1. Server Room Layout



5.1.2. Server Room Electrical SLD Layout

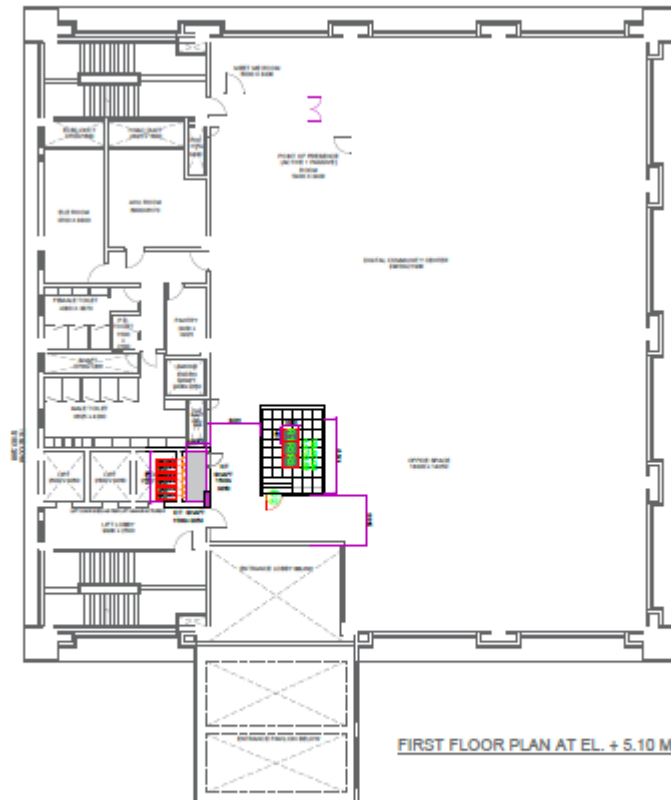


5.1.3. City DICDL Building 1st Floor ICT Rooms Layout



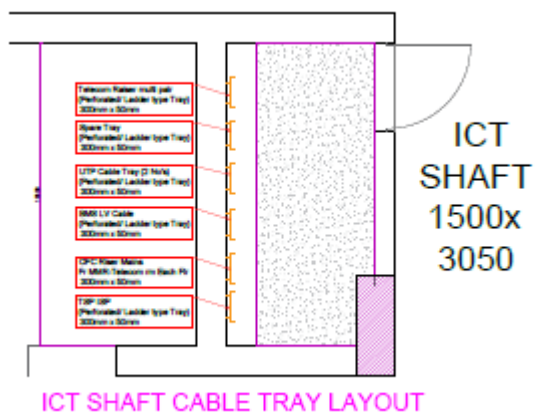
FIRST FLOOR PLAN (CITY SPV BUILDING)

5.1.4. City DICDL Building 2nd - 8th Floor ICT Rooms Layout



TYPICAL OTHER FLOORS PLAN (CITY SPV BUILDING)

5.1.5. City DICDL Building ICT Shaft Schematic:



ICT SHAFT CABLE TRAY LAYOUT

