Request for Proposal
for
Selection of Agency for Operation & Maintenance of Gujarat State Date Center (GSDC) on behalf of Department of Science & Technology, Govt. of Gujarat

Volume-II
(Scope of Work and SLAs)

Gujarat Informatics Ltd
Block No. 2, 2nd Floor,
C & D Wing, Karmayogi Bhavan
Sector - 10 A, Gandhinagar – 382010 Gujarat.
www:gil.gujarat.gov.in

Abbreviations

1. **GoG**: Government of Gujarat
2. **DST**: Department of Science & Technology
3. DIT: Directorate of ICT & e-Governance
4. **GIL**: Gujarat Informatics Limited
5. **GSWAN**: Gujarat State Wide Area Network
6. **GSDC:** Gujarat State Data Centre
7. **GSCAN:** Gujarat Sachivalaya Campus Area Network
8. **OEM:** Original Equipment Manufacturer
9. **O&M:** Operations & Maintenance
10. **EMS:** Enterprise Management Suite
11. **NMS:** Network Monitoring System
12. **EMD:** Earnest Money Deposit
13. **PBG:** Performance Bank Guarantee
14. **SLA:** Service Level Agreement
15. **FAT:** Final Acceptance Test
16. **TPA:** Third Party Agency
17. **SoW:** Scope of Work
18. **IPS:** Intrusion Prevention System
19. **IMS:** Integrated Infrastructure Management System
20. **CCTV:** Closed Circuit Tele Vision
21. **MP:** Monthly Payment
22. **TENDERER:** GIL/ DIT /Government of Gujarat

Section I: Introduction

1.1. Gujarat State Data Centre (GSDC)

Government of Gujarat has set up Gujarat State Data Center (GSDC) in Gandhinagar, the State capital. GSDC includes 2600 sq.ft of server & storage area, 600 sq.ft of connectivity zone and 1300 sq.ft of control room & utility area. GSDC has been connected to all the Government offices through GSWAN infrastructure and is operationalized since 2008.

GSDC is a central repository for storing & hosting all digital data, applications and services of Government of Gujarat. GSDC provides a shared platform of Compute, Storage, Network & Security, Infrastructure component. Also providing the Cloud Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), e-mail services to Govt. of Gujarat employee, Remote management and service integration with other core infrastructure like GSWAN, GFGNL etc. The existing GSDC having is 100+ Racks and GoG has planned the new State Data Center of approximately 300 racks, which is under process.

1.1.1. GSDC Overview:

2600 Sq. ft	• Co-location/hosting of approx. 440+ Servers from various State Government Departments • Hosting of approx. 720+ Government websites and Applications • Storage capacity of approx. 3 PB+ to store State Government and Citizen's critical information/data • SAN , Backup solution, Proxy • Two sets of UPSs of 240 KVA capacity each to provide battery backup
Connectivity Zone (Network Room): 600 Sq. ft	• Firewall • Intrusion Prevention System (IPS) • Web Application Firewall (WAF) • DMZ (Demilitarized zones) • Server Load Balancer (SLB) • Routers and Layer 2/3 switches for network
Control Room and Utility Area: 1300 Sq. ft	• UPSs and Battery banks • Panel Switches • Precision Air conditioners (PAC) • FM 200 Gas cylinders to protect against fire situation • Building Management System • 24 x 7 x 365 CCTV/Surveillance monitoring system • Water Leakage Detection System • Rodent repellent system

	• Access Control System
Network Operation Center (NOC) Area: 2500 Sq. ft	• 24x7 Monitoring and Management facility for GSDC • Operations and Management Team seating arrangement for approx. • 50+ personnel
Expansion Area : 1400 Sq.ft	• 21 Rack capacity , currently 16 Racks have been installed for Cloud infra, GFGNL-DWDM, infra, NAS, eNagar and IFP projects • Separate Non-IT infra like Access Control, CCTV, WLD, Rodent repellent system Fire suppression, Fire Alarm, Electrical system, PAC and UPS of 2 x 200KVA with battery backup.

Section II: Scope of Work

Gujarat State Data Centre (GSDC) acts as a critical mediator and convergence point between open unsecured public domain and sensitive government environment. The GSDC has been equipped to host / co-locate systems such as Web Servers, Application Servers, Database Servers, SAN, and NAS etc. GSDC is a central repository for storing and hosting all digital data, applications and services of Government of Gujarat. GSDC provides a shared platform of Compute, Storage, Network, Security and Infrastructure components. GSDC also provides the Cloud Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), e-mail services to Govt. of Gujarat employee, Remote management and service integration with other core infrastructure like GSWAN, GFGNL etc. Also, during the last decade, dependency on GSDC services and its availability has become highly critical due to deployment of various government intranet applications as well as citizen centric applications. It is envisaged that selected agency shall not merely focus on carrying out O&M of GSDC to achieve the uptime as per SLA but also to progressively improve the satisfaction of its users by achieving utmost ease-of-use and better availability of GSDC services for all Government departments. Agency is expected to improve the processes as well as close co-ordination with all stakeholders like government user departments, application developers, connectivity service providers, various other implementing agencies, DST, GIL and other government offices, power utility agencies, Road and Buildings dept. offices, etc. for seamless availability of GSDC services to Government users. Selected agency is expected to arrange monthly meetings such as war room discussions with all important stakeholders for improving the close coordination and issues resolution thereby improving efficiency and efficacy of the overall GSDC services being delivered. With an objective to improve user satisfaction and reduce number of complaints / call, various measures are introduced in this RFP like Incentives for improvisation of services as well as skills upgradation and training of deployed manpower.

The scope of work under this RFP is Operations, Management & Maintenance Component: O&M of IT and Non-IT Infrastructure under GSDC.

2.1. Key actions points for GSDC O & M

2.2.1 The Successful bidder shall be responsible for the overall management of the IT and Non-IT Infrastructure and enabling infrastructure maintenance services / facility management services at GSDC for ensuring adherence of SLAs. Bidder shall implement new NMS/EMS tool at the State Data Centre that monitors / manages the entire enterprise wide application, infrastructure and network related components. Bidder shall provide the Operations and Maintenance Services for a period of 5 years following the award of the contract/as per terms & condition defined in this RFP. The bidder shall be responsible for following:

a) For better availability, preventive maintenance activity is required to be carried out at least once in a Month for all IT and Non-IT infrastructure which includes, but not limited to configuration backup and software up gradation/updation, dust cleaning, cable tagging etc.

b) Successful Bidder is required to submit preventive maintenance schedule of all equipment to DST. After performing preventive maintenance activities, bidder is required to submit the report of the same. All such activities should be done preferably in non-working hours.

c) As part of the Operations and Maintenance services, the bidder shall provide support for

the software, hardware, and other infrastructure provided/covered as part of this RFP. Bidder shall also provide 5 years comprehensive AMC. The bidder shall also provide services comprising of but not limiting to the following:

(i) Operations and maintenance services for existing and new IT and Non- IT Infrastructure supplied or commissioned by the bidder (if any as a part of O&M solution) at the GSDC for five years during the contract period.
(ii) Other IT infrastructure related support services for five years from signing of the contract/as per terms & condition defined in this RFP.
(iii) The services shall be rendered onsite from the designated premises. To provide the support at the locations where the infrastructure will be rolled out, bidder is expected to provide experienced and skilled personnel at each location.
(iv) Bidder is responsible to provide all required Hardware/software like Desktop/laptop, Hardware tools, OS, other software etc. to his resources (which are deployed under this project) to perform all the duties/works as a part of the deliverables under this RFP.

d) Warranty Support: As part of the O&M solution, if bidder has upgraded/replaced the equipment /devices/solutions at /GSDC, Bidder is responsible to supply, install & commissioning of the said new equipment including 05 years warranty services from FAT/acceptance of the equipment/solution. The bidder shall provide following Warranty services for all new equipments:
(i) Bidder shall provide a comprehensive warranty and on-site free service warranty for 5 years from the date of FAT for all equipments.
(ii) Bidder shall obtain the 5 year product warranty and 5 year remotely free service warranty from OEM on all licensed software and onsite for computer hardware, peripherals, networking equipment and other equipment for providing warranty support.
(iii) Bidder shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. Bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
(iv) Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
(v) Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period bidder shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.
(vi) Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the bidder at no cost. For any delay in making available the replacement and repaired equipments for

inspection, delivery of equipments or for commissioning of the systems or for acceptance tests / checks on per site basis, TENDERER reserves the right to charge a penalty.

(vii) During the warranty period bidder shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidders notice.

(viii) The bidder shall as far as possible repair/ replace the equipment at site.

(ix) In case any hard disk drive of any server, SAN, or client machine is replaced during warranty / AMC the unserviceable HDD will be property of TENDERER and will not be returned to bidder.

(x) Warranty should not become void, if TENDERER buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty will not apply to such supplemental hardware items installed.

(xi) The bidder shall carry out Preventive Maintenance (PM) at GSDC, including cleaning of interior and exterior, of all hardware and, if any, and should maintain proper records for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.

(xii) Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

(xiii) Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

(xiv) Bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

(xv) Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

(xvi) Bidder shall develop and maintain an inventory database to include the registered hardware warranties.

e) Bidder shall also be responsible for the comprehensive AMC of existing IT & non-IT Infrastructure (AS-IS condition). Details of the existing hardware which are required to be covered under CAMC by the selected bidder through this RFP are attached as Annexure A to H, GSDC Annexures for AMC. Currently some of the hardware is under AMC cover, however bidder will be required to provide CAMC post expiry of existing AMC cover.

f) For any IT & non-IT devices which are currently out of support or their CAMC had already been expired, Bidder is required to take all such IT & Non IT devices (AS-IS condition) into their CAMC support for entire contract period without any extra cost to GoG. Bidder, at his discretion, may replace or upgrade such devices with equivalent/better capabilities, in case of any challenges to get CAMC support.

Note:

1. **For network and security devices (Annexure-B),** the bidder, at his discretion, can take **back-to-back** CAMC of network and security components or refresh with equal or higher capabilities.

2. **For non-IT, servers, storage, and backup mentioned in this RFP** (Annexure A, D, D1 ,E,& E1) bidder can do **back-to-back OEM agreement through authorized Distributor or partner for AMC/Warranty** and shall provide a copy of the service level agreement signed with respective OEMs.

3. **The bidder, at his discretion, may upgrade/replace /refresh IT components (Annexure A & B)** with equal or higher capabilities. Bidder should take prior approval of the GSDC before the replacement. In such cases successful bidder has to perform end to end migration , implementation activity within downtime given by Tenderer. Delay in such implementation , migration will attract the penalty.

4. Successful bidder, in case of refreshed components, needs to maintain existing hardware/ software /solution as per SLA in this RFP, until successful FAT of refresh/replacement of existing component

g) There are various spare equipment/devices available with GoG as listed in various Annexures attached in this RFP. Bidder is responsible to install, commissioning the said spare Equipment/devices in line with requirement of GoG at selected location in the state without any extra cost to GoG. This also includes all other costs like but not limited to, Transportation, labour charges if any, lodging charges for technical team/resources etc.

h) There are various equipment /devices which are not in use. The list of such devices/equipment will be shared with successful bidder. Bidder is required to coordinate with DST/other appointed agency by DST for necessary disposal of said equipment/device in line with instruction received from DST/GoG.

i) During the contract period, TENDERER may discontinue the O&M and CAMC services for any equipment/device based on their usability for the Project. For such cases, the 1% of the total cost (Without Tax) of such equipment/device will be deducted from applicable yearly O&M Amount. For CAMC, quoted price by bidder will be deducted from applicable yearly CAMC amount ,based on submitted physical price breakup at GIL office. This will be applicable from the next month after the notice issued by DST/GoG for such discontinuation of the any equipment/service. .

j) "At SDC and 33 DC locations, Biometric Access control system (including all accessories like biometric Finger scan card reader, Controller, Smart card reader, Access control software, Smart cards etc.) have been installed for Access Control Management. Please refer attached Annexures-G (Biometric Access Control System) for more details. Bidder is required to provide O&M support and CAMC support (end to end support) for the said Access Control Systems & its all accessories including, but not limited to, maintenance of Access cards, issuance of new card (compatible with existing system) if any required during contract period etc. If required, Bidder may change/replace partial (component)/ whole Biometric Access Control system with equivalent/better specification with the prior approval of GSDC , in case of Bidder face any compatibility issue or EoS/EoL issue during the contract period without any extra cost to GoG."

k) End-to-End administration, management of all components at GSDC & DR.

2.2. Network operations, Services and maintenance

2.3.1 The services as per the scope of the contract shall include maintaining the network equipment; ensuring running of the services (Data, Voice, and Video) with availability in line with the SLA and Round-the-clock Network monitoring. This shall include:

(a) Equipment Configuration Management
(b) Upgrading IOS/Firmware
(c) Maintaining access control list
(d) Regular review of Network
(e) Regular reports as required by DST
(f) Regular backup of NMS server
(g) Monitor GSDC Network
(h) Regular reports as required by DST &
(i) Auto backup configuration of Router and Switches
(j) Regular SLA Violation reports for Network vendors
(k) Upgrading Patches on all equipment's including NMS-Servers, network & Security Devices and hardening of network & security devices.
(l) The Successful bidder is required to maintain uptime of the network at GSDC to meet the SLA .In case the network uptime is not maintained due to non-availability of link/Bandwidth by Service provider, bidder is required to produce documentary proof (Service Desk Complaints/Incidents or Vendor assigned Tickets) in terms of certificate of downtime of network link/b/w from the service providers. In case bidder fails to provide such documentary proof the same shall be treated as non- performance of SLA and would be liable for penalty.
(m) The Successful bidder shall keep the details of all the Assets and document any changes in the assets including up-gradation and/or replacement of assets. **The asset inventory for the entire network architecture shall always be up to date and shall be submitted to DST on monthly basis.**
(n) Bidder is required to keep requisite spares to ensure adherence of SLAs and continuity of O&M operations
(o) Successful bidder will have to do operational liasoning with stake holders (link providers, state government, local bodies, third party agencies / consultants appointed/identified by GoG) to keep the GSDC up & running.
(p) The Successful bidder has to submit availability & all SLA reports on monthly basis.
(q) **Comprehensive Annual Maintenance Contract of out of warranty network equipment at GSDC:** As mentioned at point 2.2.1. (f), Successful bidder shall enter into comprehensive AMC contract for out of warranty equipment/ hardware at GSDC. List of existing devices, for which currently AMC is either not available or will expire during the Contract period of this bid, is placed at as GSDC Annexures for CAMC, bidder will have to provide AMC for these items till the end of this contract.

TENDERER may direct bidder to provide the CAMC of any existing or new devices including all components, accessories etc. (not covered in this RFP) at rate of 7% per year of the device purchased cost (Without Tax).

(r) In case TENDERER decides to migrate the network to IPv6, the successful bidder shall prepare the migration plan and execute the same within 6 months. Failing to the same will attract the penalty of Rs. 1000 per week.

(s) Bidder has to provide UPS & Battery Health, impedance Reports in every month after completing proactive maintenance every month. Bidder will have to replace batteries at the start of **1st and 4th year of the contract period during 1st and 13th quarter.**

2.4 EMS/NMS for SLA and Performance Reporting

2.4.1 The Successful bidder shall operate and maintain an Enterprise Management Suite (EMS)/Network Management System (NMS) and SLA and Performance Monitoring System for GSWAN backbone at Network Operation Centre (NOC) and GSDC components centrally at SC. Currently, GSWAN is monitored through CA-NMS tool and GSDC is monitored through CA-NMS. The device count for GSWAN is 22000 & for GSDC device count is 5000. The successful bidder is required to maintain & manage the existing tools and to provide comprehensive support till the migration & Go-Live of on new solution. Bidder to replace this tool with appropriate equivalent to higher capabilities NMS/EMS tool with necessary hardware, software and licenses on taking over the O&M Operations. During the contract period, bidder has to provide additional licenses & required hardware and software without any cost at time of addition of new node if required. If any of the functionality/requirement listed below are not supported by existing/ proposed tool, bidder has to provide/fulfil the functionality by customizing the solution it self. The EMS/NMS tool should provide Supervision and Call Centre support for GSWAN and GSDC. The selected bidder shall be responsible to install & provide support for EMS / NMS. The EMS/ NMS tool for GSWAN will be used by GSWAN O&M operator, and for GSDC components the tool has to be managed and monitored by the bidder selected under this bid. The selected bidder shall provide a separate instance for GSWAN. The EMS/NMS tool should be managed by the Successful Bidder for the complete contract period and shall be used for regular monitoring of the network and GSDC. Successful bidder shall configure/ provision the systems to be used by GoG for audits and also help in monitoring the service level parameters on an ongoing basis as defined in Service level agreements. The TENDERER or its designated agency shall have access to all generated reports for service levels audits and monitoring. Successful bidder shall deploy adequate access policy and security policy on the systems in consultation with TENDERER for ensuring authenticity and integrity of the reports. The system shall essentially have 3 components, Network and Data Centre Management component, Helpdesk & SLA Management component. The TENDERER or its designated agency should be able to view the SLA Management component. The Successful bidder shall be responsible for creating network monitoring environment through the following:

a. The EMS/NMS system shall be configured to automatically discover all

manageable elements of the GSWAN and GSDC.

b. All network components shall be configured to alert the centralized EMS/NMS server in case of any events, so as to reflect real status of all network components and links across GSWAN and GSDC.

c. The NMS should also poll all network devices and other IT and Non-IT components in GSWAN & GSDC at regular intervals in order to determine their status and working.

2.4.2 The functional requirements of the EMS/NMS system are as follows:

a) **Alarm Correlation & Root Cause Analysis Capabilities**

(i) Solution should provide alarm correlation and facilitate reduction of total number of alarms displayed by means of intelligent alarm correlation, suppression and root cause analysis techniques built in to the system. The system must ensure reduction in MTTR by means of advanced event correlation, filtering and root cause analysis.

(ii) It should have capability to perform cross domain correlation with alarm correlation from Network Monitoring tool, Systems monitoring tool and other domain monitoring tools.

(iii) Alarm Filtering should allow flexible filtering rules for NOC staff to filter the alarms by category, severity, elements, duration, by user, by views, by geography or by department.

(iv) Ability to apply severity to alarms according to predefined rules.

(v) It should be possible to add description to the alarms.

(vi) The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.

(vii) The system should be able to clearly identify configuration changes as root cause of network problems

(viii) Alarms should be mapped to the live topology views and real time updates to topology based on alarm occurrences.

(ix) Historical Reporting of alarms must be possible and system should be able to store large volumes of alarm data for historical reporting purpose

(x) It should be possible to convert Critical Alarms into Incidents for auto ticket generation into proposed Helpdesk tool.

(xi) Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.

(xii) Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.

(xiii) Consolidated network view embedded with digital maps

(xiv) The selected O&M agency shall develop and provide a mobile application for

incident management, alerts, and notifications for GSWAN & GSDC. The app should be able to generate alerts / notifications in case of occurrence any network downtime related incidents. The application shall be hosted at Gujarat State Data Centre. The app shall provide role based access to the engineers at state level, district level & taluka level as well as to GIL/DST authorities, as required. The selected O&M agency shall be responsible to maintain & manage the app hosted at GSDC.

b) Network Fault and Performance Management

(i) The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.

(ii) The Network Management function should have a graphical topological display of all discovered network devices in real time.

(iii) The proposed Network Fault Management solution must also provide network asset inventory reports

(iv) It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across GSDC/GSWAN and any further Network connectivity's planned in future by simple addition of required licenses without any change in topology.

(v) The proposed Network Fault Management solution must support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery. It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms.

(vi) The discovery must also support device redundancy discovery in case of virtual IP addresses using vendor specific protocols such as VRRP and HSRP.

(vii) The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices. When a report is run the administrator must have an option of specifying the number of consecutive days the port must be "unused" in order for it to be considered "available".

(viii) The proposed solution must provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed management system must also intelligently determine which ports are operationally dormant. This will help in analyzing capacity needs of the Network ports and better network capacity planning across the GSWAN network.

(ix) It should support integrated Fault, Performance, and Configuration Management features from a single solution.

(x) It should show live interface connections between discovered network devices and must be able to do mapping of LAN and WAN connectivity with

granular visibility up to individual port levels

(xi) It should proactively analyze problems to improve network performance.

(xii) The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display.

(xiii) The Network Management function should poll or collect and analyze the large volumes of fault and performance data. Once collected, it should automatically store data gathered in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and performance analysis.

(xiv) The Network Management function should have a feature of discriminated polling of devices.

(xv) The Network Management function should be able to monitor device performance in near real time

(xvi) It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.

(xvii) Solution should have a provision for suppression of maintenance alarms during the maintenance period.

(xviii) The proposed performance management system shall provide network, server and database performance information, alarms and also reporting interface(s) for components. The current performance state of the entire network & system infrastructure shall be visible in a console.

(xix) The proposed solution must scale to large networks while supporting a single web interface for access to reports. The system must support multiple locations and a distributed deployment for collection and monitoring. Primary instrumentation should exist at the Central Site.

(xx) The Proposed solution must support out of the box trend reports on group of metrics or group of devices in a single report. This will help understand the performance of multiple devices against a KPI (Key Performance Indicator)

(xxi) The proposed solution must support out of the box capacity planning reports that assist in the analysis of capacity needs based on projected load.

c) Network Performance Reporting

(i) Solution should be able to collect Key performance measurements and statistics (CPU, Memory, availability, reachability, package loss, latency etc.) from all network domains and store it. This data is to be used for evaluation of performance of the end-to-end network infrastructure/ services.

(ii) Solution should have functionality for KPI calculation on the raw metrics

collected.

(iii) Solution should be able to do Trend analysis from the performance data.

(iv) Should be able to generate web-based reports both near real time and historical data for the network.

(v) It should be possible to view live report.

(vi) Solution should support historical storage of aggregated data for one year and data backup.

(vii) Proposed solution should be able to also provide a threshold and profile capability on the KPIs monitored on the network in order to understand the impact of failures and degradations which eventually results in downtime/network unavailability.

(viii) The system shall be able to support separate warning and violation threshold levels, so that in the event of gradual service quality deterioration, warnings shall be generated before critical level thresholds are breached.

(ix) Out of the box fault and performance reports

(x) Customizable Reporting should be possible .

(xi) It should support automatic base lining on historical data, and thresholds that can be adjusted as required, based on data collected.

(xii) It should have a secured interface with role based access and privileges.

(xiii) Availability of drill-down reports.

(xiv) Solution should offer off-the-shelf Reports for KPIs such as Availability, Uptime, and Resource Utilization.

(xv) Solution should have the capability to export the reports results in standard file formats like CSV, pdf etc.

(xvi) Should be able to present the reports through web and also generate “pdf” / CSV / reports of the same.

(xvii) Solution should have capability of exporting report in open interface formats for business intelligence tools, excel, etc.

(xviii) Solution should support capability to periodically generate (scheduled reports) and distribute statistics reports to the designated team members at customer side.

(xix) Solution should provide options to perform progressive trend analysis with multiple fixed time windows like 1 day, 1 week, 2 weeks, 1 month, 6 months etc.

(xx) Solution should allow configuring threshold crossing alerts on KPIs. It shall be possible to define threshold profile(s) for raw counters or KPIs/KQIs and generate alarms or threshold crossing alerts which would be

forwarded to the Fault Management system or Event Correlation Engine.

(xxi) Solution should support retrieval of historical performance data collected at any monitored point and archived on the server. The solution should allow aggregation of historical data.

(xxii) Solution should facilitate reports summarized by time – Hour, Day, Week, Month, Quarter, Year and by Property- service, location, department etc.

(xxiii) Should able to generate reports on predefined / customized hours.

(xxiv) Highly Flexible Group based Reporting: It shall be possible to use a KPI at different network element levels (individual Network Device, Interface, Group of Network Devices, Links, etc.) and time dimensions.

(xxv) Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.

(xxvi) It should be able to generate SLA Reports on Availability & Performance.

(xxvii) Should create historical performance and trend analysis for capacity planning.

(xxviii) Should have capability to exclude the planned-downtimes or downtime outside SLA.

d) Centralized ITIL Aligned IT Service Desk:

(i) The existing Service Desk is one of the most essential components of Network Operations Center. It is the central mechanism for NOC staff to track and respond to requests and problems logged by end users and also work upon other NOC functions such as Change Management, Knowledge Management, Release Management, etc. Thus, it is expected that the proposed Service Desk is well aligned to maximum number of ITIL processes such as:

a. Incident Management
b. Request Fulfillment
c. Problem Management
d. Change Management
e. Release & Deployment Management
f. Knowledge Management
g. Service Asset & Configuration Management
h. Service Catalog Management
i. Service Level Management
j. Service Portfolio Management
k. Availability Management
l. Capacity Management
m. Event Management
n. IT Service Continuity Management

(ii) **General Requirements of Service Desk**

a. Should able to support and handle large volume of incidents
b. Should able to support and handle large volume of service requests
c. Should able to support and handle large volume of changes
d. Native integration of processes i.e. Incident Management with Change Management and vice-versa
e. Native integration of processes with Knowledge base i.e. automatically creation of knowledge base post closure of tickets
f. The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge management, Asset Management and CMDB
g. Able to create and modify forms as per GoG/DST requirement
h. Able to define different SLAs for different services / domains , vendors
i. Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units
j. Able to define different workflows for different processes
k. Able to send automatic escalation mails as defined in workflow
l. Should be able to integrate CMDB from different federated data sources and build a single CMDB
m. Should provide email based interactions allowing ticket creation, update and approval of request.
n. Should able to integrate with Active Directory and populate user information automatically
o. The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.
p. The system should have graphical interface to define, visualize and update ITIL processes

(iii) **Service Catalogue Functionality**

a. Should support single service catalogue for end users to submit and track service request, spanning ALL IT services
b. Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT services
c. Various types of Customer profiles should be supported such as, for ex: Profile-1: CMO, Profile-2: IAS Cadre, Profile-3: Grade 2 Officers and so on.
d. Integrates with any underlying service management including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment

e. Should have catalogues that cover standard and non-standard IT services
f. Users should be able to request for services on behalf of other employees and the system should track the request as if the request has been initiated by the user requesting for the service.

(iv) **Service / Help Desk (Incident and Problem Management)**

a. Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT services that shall span across multiple domains like GSWAN, GSDC etc.
b. Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
c. The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations
d. It 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
e. It should have the ability to search multiple built-in knowledge bases like the incident, problem, and known-error database simultaneously without requiring the agent to search each knowledge base individually.
f. It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
g. Should support full text search capabilities
h. Should centralize all known error and problem workarounds into a single, searchable knowledge base
i. The incident Management solution should be completely integrated to the CMDB to ensure that CIs can be associated with the ticket to provide better visibility
j. The incident management solution should have the ability to initiate the change request on a button click
k. The solution should have the ability to associate an incident with an existing change request, a problem or known error for tracking purposes
l. It should allow the CI to be associated with tickets.

(v) **Change & Release Management**

a. The solution should be able to track a request for change through the different stages of lifecycle of a change request
b. The tool should facilitate the identification of the change type and associated workflow For example: standard, normal, and emergency
c. The tool should facilitate the differentiation of normal Changes For example: Category - Minor or Small, Category - Significant or Medium,

Category – Major or Large

d. The tool should facilitate the ability to create simple to complex request workflows through sequential and parallel tasking
e. The tool should notify all the users about the scheduled changes/outage and sent a reminder to responsible contacts for implementation of change.
f. Change management should have fields to record impact analysis and, back-out plans, within the change record
g. The tool should facilitate of post implementation reviews for implemented changes after defined time interval
h. The application should have the ability to assign change advisory board (CAB) responsibilities to change management roles
i. The tool should facilitate ability of authorized roles to reject changes For example, status of reject, ability to record reason for rejects notification
j. The change approval engine should be configurable such that approvals can happen if either one of the individuals approves a change, or a majority approve the change, or certain people in the committee approve the change etc. It should also incorporate multi-staged approvals like MD-GIL, JS-IT, Sec-IT etc.
k. Change management should be capable of integrating with CMDB to facilitate access to CI attributes and relationships to enable change assessment and authorization
l. Solution should provide a consolidated view of the tasks that the release management team must perform to drive the completion of the change requests and activities required to close the release.
m. Solution should provide Change and Release Calendar views for the current schedule of releases, change requests, and business events for any potential conflicts.
n. The solution should have the ability to prompt change planners with suitable time slots for conducting a change depending upon the changes that have been scheduled/in progress, risk associated with it and the priority of the change.
o. The solution should have the ability to identifying and flagging changes that are being done by various team to prevent change collisions.

(vi) **Knowledge Management**

a. The tool should have the knowledge management OOB - knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions.
b. The tool should allow the creation of different access levels (i.e. Read only, write, create, delete) to knowledge management system
c. The tool should allow creation and enforced use of data input rules for creating knowledge records For example: mandatory fields for content

and information; QA and change approval to move from draft to production

d. The tool should allow for the entry of free-form text, images, attachments, etc.
e. The tool should automate the population of knowledge records with author and owner data, creation date, as well as any other attributes required by organization
f. The tool should facilitate the identification of redundant or duplicate information, whether in single record or multiple records
g. The tool should allow automating notification to interested parties on submission new knowledge/solutions applicable to them
h. The tool should have a powerful search engine to sort, retrieve and search using advanced search options, search content in multiple format, and also search within knowledge records
i. The tool should allow displaying FAQs and highlight the newly added knowledge content
j. The module should allow integration with all other modules of service management to enable knowledge records to be quickly created from records with associated links.
k. The solution should have the ability to prompt users with interactive set of questions and answers that will eventually guide the users to the relevant solution.
l. The module will facilitate opening of a problem record directly from a menu for pro-active tracking of problem activity as well as from an incident record for reactive tracking of problem activity.

(vii) **Configuration Management database (CMDB)**

a. 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
b. Reconciliation of data should be possible with multiple data providers based on common attributes and ability to define precedence rules on attributes
c. 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
d. The proposed helpdesk solution must allow the IT team to see the CI relationships in pictorial format, with a specified number of relationships on single window.
e. The CMDB should have built-in drift management capabilities to capture and report on infrastructure drift based on infrastructure attributes like RAM, memory, etc.
f. Should provide Attribute-level normalization and reconciliation to leverage existing data from external sources and realize the goal of having one

dependable source of configuration data.

(viii) **Service level Management**

a. Solution should support comprehensive SLA management platform
b. Manage service levels for delivery and support of business services
c. Must allow creating and applying various operational level parameters to Incidents, Requests, Changes, and Release management modules.
d. Real-time visualization of service level targets, penalties.
e. The module should link available support hours to service levels when calculating deadlines as well as suspend SLA calculation for certain criteria – ex. 'pending information from customer'
f. The SLM module should integrate with incident and problem management to automate escalation, and notification activities based on response and resolution targets
g. It should also integrate with change management to provide access to service level agreement details, implementation windows, change blackout periods, and availability requirements
h. The application should have a predefined/customizable field to indicate & track the progress/status of the lifecycle of ticket(s). It should contain predefined status codes and allow defining new status codes
i. The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure For example: IDs of individuals or groups opening, updating & closing records; dates / times of status & activities updates, etc.

(ix) **Dashboard Reporting**

a. The Solution should provide a centralized Dashboard that picks up relevant business metrics from the service management solution giving at-a-glance visibility to key operational initiatives.
b. GoG/DST assigned staff members should be able to graphically view the health of their business services and its related ticket KPI's pertaining to different categories and departments configured in Service management tool.
c. These dashboards need to be dynamic that allows user to drag and drop these metrics and create custom dashboards without any coding.
d. The Dashboards should support rich formatting capabilities to represent the data in different chart formats.

e) **Business Services Dashboard**

(i) Proposed Business Services Dashboard should provide flexible, role-based dashboards (for IT executives and service owners of GoG/DST) and operational consoles (for operations managers in NOC and technical staff) for a common understanding of service status, risks and quality problems.

(ii) The proposed Business Services Dashboard Solution must enable intelligent service modeling by importing IT components (like network

devices, server resources, applications, transactions etc.) from the management tools that directly manage infrastructure and applications:

(iii) The Service Dashboard should display business service status in real-time.

(iv) It should be possible to determine impact of network faults and performance degradation on customer services. .

(v) Solution should perform cross domain correlation between network alarms and degraded performance data received from multiple domains.

(vi) Solution should show the real time status of real time status of service problems for all the underline impacted services.

(vii) The Business Process Views should have capability to provide business oriented views of the IT infrastructure management.

f) **Service Level Management**

Service Level Management will be one of the crucial functions of Network Operations Center. SI's must propose a full fledge Service Level Management System that helps define, document, monitor, measure, report, and review the level of IT Services.

(i) SI's must propose a full-fledged Service Level Management Solution that allows for tracking of various service level performances of IT Infrastructure and vendor performance.

(ii) The product should be able to measure, collect, and import performance and SLA data from a wide range of sources, including performance Management modules

(iii) The SLM System should help to compute the automated weighted average score of the SLA metrics and arrive at the monthly/quarterly/half-yearly/yearly service penalties as per the contract/SLA with different agencies

(iv) The solution should support SLA violations alerts during the tracking period.

(v) The solution should support the creation of different contracts which are currently underpinning with vendors.

(vi) The solution should support managing and maintaining a full history of an SLA.

(vii) Solution should support SLA violations in context of effective "impact" .

(viii) The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators measured across infrastructure and vendors

(ix) The solution must have a unified repository to capture and manage all service level templates.

(x) The solution must provide detailed control/methodology of the metrics that are being collected

(xi) The solution must contain out-of-the-box content for best practices frameworks such as ITIL.

~~(xii)~~ The solution must support the concept of service templates, Service templates grouping and metric groupings.

(xiii) The solution must allow for grouping and composition of Services

(xiv) The solution must have a pre-configured catalog of reusable Service Level Calculations and Aggregation methods.

(xv) The solution provide document repository capabilities for supplemental documents associated with SLAs, SLA Management & Reporting process

(xvi) The solution must support management of service level agreement in a central repository.

(xvii) Creating of new service level agreements must be easy to be used by business and non-technical users.

(xviii) The creation of SLA must be done via a Wizard driven interface

(xix) The solution must allow for customization of the service level agreement.

(xx) The solution must have the ability to define and calculate key performance indicators (KPIs) from an End to End Business Service delivery perspective.

(xxi) The solution must support dependencies between business and technical metrics.

(xxii) The solution must support dependencies between supplier's contracts and internal or external contracts.

(xxiii) The solution must support weighting of Service Level Indicators

(xxiv) The solution must have the ability to manage multiple SLAs for the same contract party

(xxv) Manage scheduled and un-scheduled maintenance windows

(xxvi) The solution must support SLA approval/validation workflow

(xxvii) The solution support role base access to service level agreements

(xxviii) Links to external or internal sources can be created from within service level agreements.

(xxix) Integration of SLA Creation & Reporting/Monitoring modules

(xxx) The solution must support aggregation and correlation of performance data relatively to contractual agreements.

(xxxi) The solution should be an integrated with Business dashboard

(xxxii) View of Contract Parties & current SLA delivery levels

(xxxiii) View of Services & current SLA performance

(xxxiv) The solution must support standard and user configurable aggregation

(xxxv) The solution supports SLA Alerts escalation and approval process.

(xxxvi) The solution must make it possible to find the underlying events that cause the service level contract to fail.

~~(xxxvii)~~ The solution must provide annotation capabilities that must appear in reports generated against the service level.

(xxxviii) Timing for collection of data is configurable.

(xxxix) Ability to define Adapters to data source in a visual manner without coding.

(xl) Design, customize, & Generate reports easily & based on User Roles

(xli) The system must include the ability to generate customer SLA document from SLA information entered in the solution

(xlii) The solution must allow for reporting across customers, Type of Customer, Business unit, Service, Product any configured area of measurement.

(xliii) Reports should be created in a friendly manner using visual tools and wizards without any code or database query configuration.

(xliv) Report module and SLA Management module must be integrated to provide ease-of reports configuration and execution.

(xlv) The solution must support data integrity in reports correlation and present the end users indication regarding reports which includes data manipulations, corrections and exceptions,

(xlvi) The solution must allow the distribution of reports to appropriate roles/ people, through Web-based interface/ Web Portal, or via email.

(xlvii) The solution must support single sign-on as well as integrate LDAP for user login and authentication.

g) **IT Asset Management**

SI must propose an IT Asset Inventory Management Solution that shall enable centralized and automated management of IT assets governed from Central Site.

(i) Solution must be able to discovery IT Assets for Inventory Management Purposes

(ii) The discovered IT Assets must be maintained in a single IT Asset Repository database for better and single pane of glass visibility for all IT Assets

(iii) The discovery should have feature of scheduling the discovery at specific periods

(iv) The discovery solution or IT Asset Management solution should also support IT Asset inventory import from other data sources such as excel inventory, monitoring tools like Network Monitoring tool for a holistic IT Asset Inventory collection.

(v) IT Asset Management solution must be able to integrate with proposed monitoring solutions to perform auto discover into Asset Management database.

(vi) Solution must be able to track Warranty / AMC of all IT Assets

h) **Network Configuration Automation**

(i) The Network Monitoring Solution must also have Configuration Automation feature for the monitored compatible devices.

(ii) The system should be able to clearly identify configuration changes as

root cause of network problems.

(iii) The system should support secure device configuration capture and upload and thereby detect inconsistent "running" and "startup" configurations and alert the administrators.

(iv) The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements:

a) Capture running configuration
b) Capture startup configuration
c) Upload configuration
d) Write startup configuration
e) Upload firmware

(v) The proposed fault management solution must able to perform "load & merge" configuration changes to multiple network devices

(vi) The proposed fault management solution must able to perform real-time or scheduled capture of device configurations

(vii) The proposed fault management solution must able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.

2.4.3 Successful bidder shall provide the following:

(a) NMS reports including Bandwidth utilization report & Link up-time report & network equipment health check report on a monthly, daily basis.
(b) Change management carried out by Helpdesk operation.
(c) Network Device Performance Report for SC-DC-TC and other priority offices, Weekly Monthly.
(d) Change management report – Monthly
(e) New Location Connectivity –Weekly, Monthly
(f) Asset Report Location wise – Monthly
(g) Help Desk Report – Daily, Weekly , Monthly
(h) NetQOS Report about utilization of Network protocol and GOG applications.
(i) Vendor SLA Violation Report – Weekly , Monthly
(j) Audit Report – Monthly
(k) Network Utilization Report – Monthly
(l) Network performance after Integration (with other network) Reports – every 6 months.
(m) VC & other Web Event completion report –Monthly
(n) Preventive Maintenance Report - Quarterly

2.4.4 Successful bidder shall have to consult TENDERER for finalizing the report formats and frequency formulating a Communication Plan prior to the start of services. Successful bidder shall also enable the GoG designated Officer to be able to view any

(up-to-date/ historical) reports related to GSWAN and GSDC at any point of time via a Web-based interface to the NMS.

2.4.5 Bidder should also provide on-line Dashboard where, DST can get summary view of GSWAN and GSDC Connectivity and Health Status.

2.4.6 Successful bidder would generate and provide Reports as stated below periodically. Bidder shall also be under obligation to provide any other reports as asked by DST, GoG or its representatives.

2.4.7 General Reporting Features:

(a) Shall be able to present the reports through web, and also generate "PDF" version reports of the same.

(b) Should provide user flexibility to create customized reports according to the user privilege level.

(c) Should provide information regarding capacity utilization and error statistics for physical and logical WAN links

(d) Should create reports on trend analysis and capacity planning from historical data and also by considering Mean Time Between Failure (MTBF) of equipment.

(e) Should be capable to send the reports through e-mail to predefined user at pre-defined interval.

(f) Should have capability to exclude the planned downtimes from SLA.

(g) Should be able to generate web based reports both in near real time and historical data for supported devices.

2.4.8 Availability Reports

(a) Overall Network Availability and Uptime Report on Daily, Weekly, Monthly, Yearly basis through GUI.

(b) Uptime & Availability Report for Vendor/Service provider; MPLS network, Leased Lines, LAN, Server on Daily, Weekly, Monthly, Yearly basis.

(c) Uptime & Availability Report on Network Devices: Router, Switch, Security Appliance on Daily, Weekly, Monthly, Yearly basis.

(d) Uptime & Availability Report of UPS at State, District & Taluka level on Daily, Weekly, Monthly, Yearly basis.

(e) Mean Time To Acknowledge (MTTA) and Mean Time To Repair (MTTR) Reports.

2.4.9 Performance Reports

(a) Overall Network Device Performance (Router, Switch, Security Appliance) – CPU and Memory Utilized at State, District & Taluka level.

(b) Every Link Input/Output Utilization (percentage, bps, kbps, mbps, octets/sec) on Leased Line, Wireless, Trunks between Switches, Link errors (Leased Lines, ISDN, Trunks, etc).

(c) Should be able to indicate the Network Latency, Flapping Links, Changed Link Metrics, Prefix List and New Prefixes on each leased links at State, District & Taluka level.

(d) Trend report based on Historical Information.

2.4.10 SLA Based Report:

(a) Should be able to do computation of SLA for entire GSDC and GSWAN network and Individual links

(b) Should be able to generate automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports

(c) Should be able to present "At-a-Glance" report comprising critical SLA parameters

(d) Should provide component level report.

2.4.11 Inventory Status Report:

(a) Equipment Inventory report –device name, device part number & serial number, device model number deployed at SC, DC & TC level.

(b) Change Management report - change audit reports, changes by user and change detail reports provide immediate visibility into whether or not the defined CCM process is working and being followed.

2.4.12 Event & Fault Management Report

(a) Should provide details about the number of complaints received due to failure of network devices and Voice devices.

(b) Should provide the exact time and date when the complaints was resolved on daily, monthly and yearly basis. This should include the time taken to resolve the complaint and the reason due to which fault had occurred.

2.5 Quality of Service (QoS)

2.5.1 Successful bidder shall configure quality of service (QoS) parameters on network switching and routing devices for end-to-end QoS for voice, video and other critical traffic over the network. Successful bidder shall configure network management policies for managing all the network and security devices using network management systems. Bidder will also be responsible for generating NETQOS reports from NMS tool and adhering to such policies that are issued from time to time by GoG.

2.6 Helpdesk / Contact Centre

2.6.1 For servicing the GSDC users, currently following Helpdesk/Contact centre has been installed at Gandhinagar for providing Helpdesk services to GSWAN and GSDC users.

(Contact centre solution: Cisco BE7H-M4-K9 with all required Hardware, Software, cables, tools, accessories etc. for contract centre solution)

The Helpdesk would be operated by a Third Party vendor appointed by TENDERER. The Bidder is required to provide following support under Helpdesk service.

- The Helpdesk should allow GSDC users to log queries / complaints on a centralized phone number, which should be resolved as per the Service Level requirements.
- The helpdesk queries / complaints related to connectivity, security, configuration or any other issues which relate to the usage of GSDC should be handled by the Helpdesk. Daily report of calls logged and resolved should be generated and submitted to GoG.
- GoG has implemented the Helpdesk Centre from NOC. Bidder is responsible to maintain the required hardware, Helpdesk Software and licenses to setup this Helpdesk during entire contract period.

- The Helpdesk software should be able to take care of classification, automatic escalation, management, status tracking and reporting of incidents as expected by the service level requirements.
- Status tracking should be available to GSDC users through the centralized Help Desk number as well as online through software. Helpdesk software should also give a report on status of calls and violation of SLAs during disposal of such calls. Bidder shall be responsible to provide training to the Call Centre Agents to use the Helpdesk Software. Bidder shall deploy one resource to coordinate with the Helpdesk team to assign priorities to tickets generated.
- Bidder is required to provide additional UMI for chat boat facility on Whatsapp (on registered mobile) as well as on GSWAN web page, FAQ and Navigation to register complaints in Helpdesk tool with possible answers for the same. It is required to be prepared in consulting with TENDERER. To implement this chat boat facility required compute power and storage can be used of GSDC. To implement this solution in premises of SDC, if any additional Operating System (OS), Data Base (DB) is required, bidder has to account the same in future on its own .

2.6.2 Problem Resolution and Sign-Off

GSDC users would report any network related problem through online Helpdesk interface or by calling the Centralized Helpdesk number. The severity of the call will be automatically decided according to the Helpdesk Severity Matrix detailed in the SLA section. The Bidder will keep track of Helpdesk performance. This online report would contain:

(a) Trouble Ticket Number as generated in the Online System
(b) Time at which the problem was logged
(c) Problem Description
(d) Customer Details – Contact and Location
(e) Helpdesk Engineer
(f) Problem Resolution Time
(g) Cause of problem

2.9 Operations & Maintenance of Gujarat State Data Centre (GSDC)

2.9.1 The scope of work to be undertaken by the bidder for Operations, Management and Comprehensive Annual Maintenance Contract (CAMC) of the IT & Non-IT Infrastructure for the Gujarat State Data Centre (GSDC) is mentioned below.

(a) The selected bidder shall be responsible for O&M and CAMC of all IT and Non-IT Infrastructure installed in GSDC. The list of equipment, period to be covered under O&M and CAMC is placed as GSDC Annexures for O&M and CAMC
(b) The selected bidder shall ensure an uptime of 99.741% on monthly basis for both IT and Non-IT Infrastructure components.
(c) Bidder must produce Standard Operating Procedures (SOPs), processes, Technical design/architecture, layouts/templates and must be well documented for operating each IT and Non-IT Infrastructure components and should be kept updated with most recent changes.

(d) The scope of work during the operations phase should cover but not limited to following areas:

(i) System, Servers, Storage, Database, Security & Network - Administration, Configuration, Hardening, Maintenance and Operations Management
(ii) Backup and Restore Services
(iii) Preventive and Corrective Maintenance
(iv) Asset Management Services
(v) Vendor Management Services
(vi) Email/Messaging Services
(vii) GoG on premise private cloud services
(viii) MIS Reports (monthly, quarterly or as and when asked by DST)
(ix) Implementation and Compliance of ISO Standards (existing 27001:2013 and 20000:2018). Bidder shall ensure the ISO Certification is kept current and updated during the Contract period without additional cost
(x) Application and Website Hosting Management
(xi) Patch Release Update management
(xii) Software (Operating System, Anti-Virus, Enterprise Management Suite, Spam & URL filter etc.) - Administration, Configuration, Hardening, Maintenance and Operations Management
(xiii) Non-IT Infrastructure Management and Maintenance shall include equipment/components but not limited to Transformers, Circuit Breaker, DG Set, Electrical/Mechanical components, UPSs, battery banks, electrical cables, industrial sockets, Fire and Safety system, water leakage detection system, Building Management System (BMS), Surveillance systems (CCTV), Access control, Public Address System, Pest and rodent repellent system, Civil Infrastructure, Racks, Power Distribution Unit (PDUs), Precision Air Conditioners (PAC), False Ceiling , Data Centre Floor and NOC Area etc. The detailed list of Non-IT Infrastructure Items is placed at GSDC Annexures for Non IT/ CAMC
(xiv) GSDC covers approx. 4500 Sq. of area (Server, Network and Utility area), 1400 Sq ft. of expansion area and 2500 Sq. ft. of NOC-Office area, the responsibility of the selected bidder for O&M purposes.

2.9.2 The scope of work is not only limited to currently deployed IT and Non-IT Infrastructure components at Gujarat State Data Centre but also includes O&M for any additional equipment/devices/hardware/software that is supposed to be deployed at SDC during the contract period of 5 years.

2.9.3 Agency will be responsible for O&M for any additional equipment/devices/hardware/ software procured by DST, 1% of the cost exclusive of applicable taxes for each additional equipment/devices/hardware/ software component, per annum would be applicable for additional payment as part of O&M and SLA of 99.741% uptime and other applicable SLAs if any as defined by TENDERER will be enforced on additional equipment /devices /hardware /software.

2.9.4 Agency will be responsible for CAMC for any additional equipment /devices/

hardware/software procured by DST, 7% of the cost exclusive of applicable taxes for each additional equipment/ devices/ hardware /software component, per annum would be applicable for additional payment as part of CAMC and SLA of 99.741% uptime and other applicable SLAs if any as defined by TENDERER will be enforced on additional equipment /devices /hardware /software.

2.9.5 Bidder has to maintain, manage and provide end to end support for the current and future in-house developed application(s) at GSDC in line with DST requirement. Currently GSDC has developed ADVAIT portal which having multiple application/OSS tools like GSDC Dashboard, GSDC-VC (Jitsi), GSDC-Drive (SFTP server), GSDC-Git (Gitea server), GSDC-LMS (Moodle), GSDC-API-Gateway (WSo2), GSDC-ClouchDB (No-SQL), GSDC-ELK (presentation tool).

2.9.6 Currently GSDC has provided few co-location service to dept./agency like GUVNL, IFMS, GFGNL, eGujCop, CTD, CoT, CTP etc. Bidder has to co-ordinate with respective dept./agencies for the infrastructure support.

2.9.7 Following services shall be provided by the O&M agency under the basic infrastructure services, but not limited to the following:

(a) Ensure availability (99.741%) of the SDC IT & Non-IT infrastructure

(b) Facilitate hosting of departmental application, websites and infrastructure at the SDC.

(c) Ensure proactive maintenance of IT and Non-IT Infrastructure components and repair or replacement of defective IT Infrastructure components deployed at the SDC which is under valid AMC contract.

(d) TENDERER may procure necessary software licenses as required from time to time and the same shall be implemented, customized and managed by the O&M agency.

(e) Any IT and non-IT component (for the devices whose AMC is included) that is reported to be faulty / non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in the Service Level Agreement (SLA). The selected bidder shall ensure that the uptime commitment as per SLA is met.

2.10 Operations & Maintenance of GoG on premise Private Cloud Enabled IT Infrastructure

2.10.1 The Successful bidder (O&M operator) would be responsible for end-to-end operation and Maintenance of the Entire Cloud Enabled Infrastructure, provisioning, OS installation, application hosting and support, DB support and any other technical support related to application / website hosting etc.

2.10.2 The successful bidder would be responsible to ensure that any Vulnerability or security advisory, as notify by CERT-IN, NCIIPC, NIC-CERT, OEM and any other agency should be fixed/complied as per the SLA. The successful bidder (O&M operator) would keep track of such notification and intimate concern authority at GSDC and TENDERER immediately.

2.10.3 The Successful bidder (O&M operator) would be responsible of hosting of various departmental application on Cloud/server infrastructure as per the direction of TENDERER.

2.10.4 The Successful bidder (O&M operator) would be responsible to prepare checklist which is to be used or filled by the various line departments/ board/ corporation for services that would be hosted or migrated in GSDC cloud infrastructure.

2.10.5 The Successful bidder (O&M operator) would be responsible to ensure that the application to be deployed does not disrupt the GSDC operations and affect other GSDC infrastructure in terms of performance and security.

2.10.6 The Successful bidder (O&M operator) would be responsible for configuration of server parameter, Operating systems administration and tuning.

2.10.7 The Successful bidder (O&M operator) would be responsible for operating system administrating, including but not limited to management of users, processes, resource contention, preventive maintenance of updates & patches to ensure that the system is up to date.

2.10.8 The Successful bidder (O&M operator) would be responsible for Re-installation in the event of system crash/failure.

2.10.9 The Successful bidder (O&M operator) would be responsible for maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, network utilization, cluster parameters etc.

2.10.10 The Successful bidder (O&M operator) would be responsible for event log analysis generated in all the sub systems including but not limited to cloud tools, servers, operating systems, applications etc.

2.10.11 The Successful bidder (O&M operator) would be responsible for ensuring that the logs are backed up and truncated at regular intervals.

2.10.12 The Successful bidder (O&M operator) would be responsible for periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

2.10.13 The Successful bidder (O&M operator) would be responsible to ensure the upkeep of existing systems that would be reused and incorporate necessary changes for new applications if any during the tenure of the contract.

2.10.14 The Successful bidder (O&M operator) would be responsible for identification, diagnosis and resolution of problem areas to the Cloud infrastructure and application, database and maintenance of assured SLA levels.

2.10.15 The Successful bidder (O&M operator) would be responsible for preparing, implementation and maintenance of standard operating procedures for maintenance of the infrastructure based on the state's policies.

2.10.16 The Successful bidder (O&M operator) would be responsible to take backup of operating system, Virtual Machines and application as per stipulated policies of GSDC.

2.10.17 The Successful bidder (O&M operator) would be responsible for monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.

2.10.18 The Successful bidder (O&M operator) would be responsible for Real time monitoring, log maintenance and reporting of backup status on regular basis.

2.10.19 The Successful bidder (O&M operator) would be responsible for prompt problem

resolution in case of failures in the backup processes.

2.10.20 The Successful bidder (O&M operator) would be responsible for preparing various MIS reports on Daily/Weekly/Monthly/Quarterly basis. These MIS reports would be contained (but not limited to) Log of backup and restoration, Summary of systems rebooted, summary of issues/complaints logged with the OEMSs. Summary of changes undertaken in the Cloud infrastructure major changes like configuration changes, patch updates, etc. and minor changes like log truncation, volume expansion, user creation, user passwords reset, etc. Virtualization layer patch update status of all servers including the Virtual Machine running on it. Component wise server as well as Virtual Machines availability and resources Utilization. Summary of any revamped hosting on the Cloud Infrastructure. Consolidated SLA/ (Non)-conformance report. Summary of component wise uptime. Log of preventive/ Scheduled maintenance undertaken. Details of Patch, updates, Vulnerability fixes released and implementation status of same. Details of break-fix maintenance undertaken. Consolidated component wise availability and resource utilization. Reports as directed by the State for SLA calculation. Further, any other reports as directed by TENDERER/GSDC composite team.

2.10.21 The Successful bidder (O&M operator) would be responsible for knowledge transfer, Operating manuals and SOP's included (but not limited to) Various checklists prepared for cloud enablement of application, details of services that are already hosted on the Cloud infrastructure. Installation and configuration details of hardware and software deployed. Contract details of OEM and representative for onsite warranty and back-to-back OEM support. Any other details that may be required by TENDERER/GSDC.

2.10.22 The details of cloud infrastructure, tools and licenses installed are listed in relevant annexures.

2.11 IT Infrastructure Security Administration

2.11.1 The activities to be carried out under security administration shall include, but not limited to the following:

(a) Addressing the ongoing needs of Security Management including, Monitoring and Management of various devices / tools such as Firewall, SIEM Tool, Intrusion Prevention System, Content Filtering and URL Blocking, Virus Protection, Load Balancer, W A F , DMZs, VLANs, Proxy and vulnerability protection through implementation of proper patches and rules as per best practices.

(b) Carrying out periodic Vulnerability Analysis and Penetration Testing (VAPT) to ensure that SDC systems and network are safe and secure. This activity has to be performed atleast once in month and on need basis as per GOG instructions.

(c) Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.

(d) Ensuring that patches/workarounds for identified vulnerabilities are patched/ blocked immediately.

(e) Respond to security breaches or other security incidents and ensure that workaround / patches are made available for the same.

(f) Provide a well-designed access management system, security of physical and digital IT assets, data and network security, backup and recovery etc.

(g) Maintenance and management of IT security devices, including, but not limited for 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.

(h) Ensuring that the IT security policy is maintained and updates to the same are made regularly as per ISO 27001:2013, ISO 20000:2018 guidelines.

(i) Access Control Management
    (i) Audit Trail and Log Analysis
    (ii) Establishing and monitoring access control

(j) Firewall policy management which will include the Configuration & Patch Management Intrusion Detection System Management: This arrangement shall include Incident Handling and recovery. The Incident Handling Procedure (IHP) has to be followed as per the guidelines drawn by the DST, GoG. This would also include virus and spam control, policy configuration & management. The audit logs shall be maintained by the Bidder for review. The bidder would also establish counter measures that are needed for the perceived risks. The bidder shall establish the counter measures to mitigate the risk.

(k) The successful bidder would be responsible to ensure that any Vulnerability or security advisory, as notify by CERT-IN, NCIIPC, NIC-CERT, OEM and any other agency should be fixed/complied as per the SLA. The successful bidder (O&M operator) would keep track of such notification and intimate concern authority at GSDC and TENDERER immediately.

2.12 Vendor Management Services

2.12.1 The activities shall include, but not limited to the following:

(a) O&M agency shall coordinate and follow-up with all the relevant vendors of the State User Department to ensure that the user problems and issues are resolved in accordance with the SLAs agreed upon with them by updating the GIL / DST, GOG as and when deviation in the SLA is reported.

(b) O&M agency shall also ensure that unresolved issues are escalated to respective user departments / GIL / DST, GOG in accordance with the escalation matrix.

(c) O&M agency shall also coordinate with Chief Information Officers (CIOs) / Officers designated by the User Departments who would host their IT infrastructure at the SDC and ensure that the issues are resolved in accordance with the SLA signed between the User Departments and their vendors/ Application Developers. O&M agency shall maintain a track of SLA performance for such vendors.

(d) O&M agency shall maintain database of the CIOs / designated officers and various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.

(e) O&M agency shall draw a consolidated monthly SLA performance report as defined by the GIL / DST, GOG / Departments across vendors for consideration of the user departments. (Monthly & Quarterly - for GSDC)

2.13 License Management

2.13.1 The activities shall include, but not limited to the following:

(a) All the software licenses should be in the name of Government of Gujarat.

(b) O&M agency shall keep the record of all the software licenses and track software usage throughout the IT setup so as to effectively manage the risk of effective usage of software installed at the SDC.

(c) The O&M agency shall avoid the unauthorized usage of Licensed Software. In the event of any claim asserted by Third Party of Infringement of Copyright, Patent or Trademark arising from the use of IT components or software, the O&M agency shall be entirely responsible to extinguish such a claim. If the O&M agency fails to comply and the DST, GOG is required to pay the compensation to the Third Party resulting from such infringement, the O&M agency shall be responsible for the compensation including all expenses, court costs and lawyer fees.

(d) Bidder is responsible for overall license management.

2.14 Email/Messaging Services:

2.14.1 Currently MS Exchange 2016 is being used for an e-mail service. The activities shall include, but not limited to the following:

(a) End-to-end management of messaging systems

(b) Administration of mail servers

(c) Monitoring performance and management of user accounts, mail boxes, mail protocols and address book.

(d) Backup and archival management.

(e) Transactional log management.

(f) Implementation of mail policies as defined by the State and in accordance with the prevailing Cyber laws , including, user security, access control, encryption, mail box sizes, mail sizes, spam, content filtering, etc.

(g) Management and monitoring mail queues, mail routing of incoming and outgoing Internet mail.

(h) The O&M agency shall be responsible for

(i) Maintaining the messaging application and individual mailboxes,

(ii) Adding / removing Mail IDs with permission from DST.

(iii) Troubleshooting any problems in the messaging system and messaging client.

(iv) Monitoring the mailbox usage.

(v) Ensuring timely delivery of mails.

(vi) Keeping a track on the mails getting dropped and taking backups of the mailboxes at regular intervals.

(vii) Purging and compaction of mail boxes at regular intervals for optimum utilization of resources as per the policies.

(viii) Monitoring the performance statistics including mail server utilization statistics, memory management, CPU utilization and disk space utilization according to the Service level agreement.

(ix) Deployment of SPAM filter and monitoring mechanism.

(x) Maintaining and troubleshooting spam/content filter applications

(xi) Regular updation of Blacklist / whitelist and manual spam filter rules.

(xii) Operate and Manage Gateway Level content filtering/mining mechanism.

(xiii) Prepare log report from messaging system including Anti-Spam and Content Filtering for reporting the incidents of SPAM mails, Virus Mails and Accessing the restricted sites/contents. The report to be submitted to TENDERER on periodic basis for review and taking corrective actions.

(xiv) Manage gateway level SMTP antivirus and Anti-spam solution.

(xv) Security and Maintaining Confidentiality, Integrity and Availability of the E-Mail Data and Services.

(xvi) All incoming and outgoing mail traffic shall be routed through gateway anti-virus and checked/ verified to be malicious content free.

(xvii) In house OTP based password change solution has been implemented by existing DCO. Bidder is responsible for overall end2end support for existing OTP solution or bidder may provide equivalent or better OTP solution.

2.15 Server Administration and Management Services (all servers including Cloud infra)

2.15.1 The activities shall include, but not limited to the following:

(a) Installation and Configuration of server, Hardware & OS parameters, operating systems administration and tuning.

(b) Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of upgrades including migration to higher versions and patches to ensure that the system is properly updated.

(c) Installation/Re-installation of the Operating System for newly procured hardware/software licenses or in the event of system crash/failures.

(d) Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, network utilization (server network card bandwidth utilization) etc.

(e) Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc. Ensuring that the logs are backed up and truncated at regular intervals.

(f) Periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

(g) Ensuring the upkeep of existing systems that would be reused and also incorporate necessary changes for new applications if any during the tenure of the contract.

(h) Troubleshooting issues in the infrastructure, network and applications to determine the areas where fixes are required and ensure resolution of the same.

(i) Identification, diagnosis and resolution of problem areas pertaining to the SDC's IT Infrastructure and application and maintenance of assured SLA levels.

(j) Implementation and maintenance of standard operating procedures for maintenance of the IT infrastructure based on the State's policies.

(k) Management of the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc.

(l) System administration activities shall include tasks including but not limited to setting up the servers, executing hardware upgrades, hardening and software

updates when necessary.

(m) Recommend required preventive maintenance plan to the GIL / DST, GOG and should prepare schedule accordingly.

(n) Necessary information as and when requested by the GIL / DST, GOG.

(o) Coordination with the GIL / DST, GOG for smooth functioning of the services.

2.16 Storage Administration and Management Services

2.16.1 The activities shall include, but not limited to the following:

(a) Configuration of the storage system at SDC.

(b) Management of storage environment to maintain performance at desired optimum levels.

(c) Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, VTL etc.

(d) Configuration of SAN whenever a new application is hosted on the SDC. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.

(e) Provide reports on storage performance, growth, trend analysis and other reports as and when asked by GSDC/TERNDERER

2.17 Backup and Restore Services

2.17.1 The activities shall include, but not limited to the following:

(a) Backup of database and application as per stipulated policies at the SDC.

(b) The backup of necessary data/information will be carried out by the O&M agency in consultation with TENDERER. The backup schedule like daily, weekly, monthly should be designed and implemented by the Bidder. Bidder will have to submit these backup reports periodically to the TENDERER.

(c) Ensuring prompt execution of on-demand backups/restoration of volumes, files and database applications whenever required by User Departments or in case of upgrades and configuration changes to the system.

(d) Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.

(e) Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets.

(f) Physical security of the media stored in fire resistant cabinets

(g) Drill activity for the backup and restore to be done by the O&M agency. The application vendor will provide the assistance to the O&M agency as and when required regarding the drill activity and the O&M agency would be responsible to take the back up in concurrence with the application vendor and GIL / GoG in accordance with the defined back up policy.

(h) Off-Site backup of the database and the applications as per stipulated policies shall be carried out by the O&M agency for SDC.

(i) O&M agency should be responsible for successful DC-DR replication.

2.18 Installation and Configuration of Application Infrastructure

2.18.1 O&M agency shall provide installation and configuration support for the application

infrastructure to be hosted by User Departments. The activities shall include, but not limited to the following:

(a) O&M agency shall undertake pre-installation planning at the State Data Centre.

(b) O&M agency shall be responsible for co-ordination during the commissioning of the storage, network & security components and related basic infrastructure at the SDC.

(c) O&M agency shall carry out the planning and layout design for the placement of equipment in the SDC in consultation with the existing Implementation Partner. The plan and layout design should be developed in a manner so as to optimally and efficiently use the resources and facilities being provisioned at SDC.

(d) The plan and design documents for the departmental application servers, thus developed shall be submitted to the user departments for approval and the acceptance would be obtained prior to commencement of installation.

(e) The O&M Agency shall carry out Server, OS, Application, Database & Services Hardening as per Best Practices and GSDC Guidelines. The O&M Agency shall also check & verify that the Application Infrastructure (both Hardware and Software) is in compliance with GSDC's policy, process & procedures/Guidelines.

2.19 Integration Testing

2.19.1 This shall be a black-box testing role primarily to ensure that the application to be deployed does not disrupt the SDC operations and affect other infrastructure in terms of performance and security. The technical tasks (Functional, performance, security and Load testing) to be carried out shall include, but not limited to the following:

(a) Functional Testing: Ensuring that the application functionality as described by the department works adequately on the SDC environment.

(b) Performance Testing: Ensuring that the application meets expressed performance requirements on the SDC servers by using performance test tools and performance monitoring tools

(c) Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

2.20 MIS Reports (For GSDC)

2.20.1 O&M agency shall submit the reports on a regular basis in a mutually decided format. The following is only an indicative list of MIS reports that may be submitted to the TENDERER:

(a) Daily reports

(i) Summary of issues / complaints logged at the Help Desk

(ii) Summary of resolved, unresolved and escalated issues / complaints

(iii) Summary of resolved, unresolved and escalated issues / complaints to vendors.

(iv) Log of backup and restoration undertaken.

(v) Security Incidents

(vi) Component wise Report (Server, Network, Security devices, SAN/NAS, Backup, Website Updation, etc.)

(b) Weekly Reports

(i) Issues/Complaints Analysis report for virus calls, call trend, call history, etc.

(ii) Summary of systems rebooted.
(iii) Summary of issues / complaints logged with the OEMs.
(iv) Security Incidents
(v) Inventory of spare parts in the SDC.
(vi) Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

(c) Monthly reports
(i) Component wise IT infrastructure availability and resource utilization
(ii) Consolidated SLA / (non)-conformance report.
(iii) Summary of component wise Data Centre uptime.
(iv) Summary of changes in the Data Centre.
(v) Security Incidents
(vi) Log of preventive / scheduled maintenance undertaken
(vii) Log of break-fix maintenance undertaken.
(viii) Consolidated component-wise Non-IT and IT infrastructure availability and resource utilization.

(d) Half-yearly Reports
(i) Data Centre Security Audit Report
(ii) IT infrastructure Upgrade / Obsolescence Report
(iii) Risk Assessment, Risk Management and Risk treatment Report

(e) Incident Reporting
(i) Detection of security vulnerability with the available solutions/workarounds for fixing.
(ii) DoS attacks, Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.
(iii) Software license violations.

(f) MIS for reporting Attendance
(i) O&M agency has to report attendance on monthly basis.

(g) MIS reports related to Application Enhancements

(h) The O&M agency shall submit the following indicative list of deliverables for any change request, application enhancement.
(i) Impact Analysis Document
(ii) Estimation of efforts with basis of estimation and breakup of estimation
(iii) Tentative Project schedule
(iv) Code coverage results
(v) Unit Test cases & results along with Defect Statistics
(vi) System Test Plan, Cases & results (STS, STR) along with Defect Statistics
(vii) Integration Test Cases & results along with Defect Statistics.
(viii) Performance Test Report and Performance Tuning Report
(ix) User Training Manual
(x) Traceability Matrix

(xi) List of common errors and resolutions

2.21 ISO 27001 ISMS Standards for GSDC

2.21.1 O&M agency is responsible for maintaining the overall Information Security posture at GSDC. The O&M agency would be responsible for establishing, operating, monitoring, reviewing, maintaining and continuously improving the Information Security Management System (ISMS) at the GSDC. The O&M agency shall be responsible for the implementation, sustenance of ISO/IEC 27000 standard and subsequent renewals/ upgrades to ISO 27000 certification from the certification body such as STQC, BSI, DNV, BVQi, etc.

2.21.2 The regular revision/review/change of Policy, process & procedure documents as and when required is the responsibility of the O&M Agency.

2.21.3 O&M agency has to take consent of DST, GoG in case of any changes required in policy manual or documentation.

2.21.4 O&M Agency has to carry out Risk Analysis to identify and assess potential risks that could affect continuity of businesses at GSDC. O&M Agency will also be responsible to recommend and implement adequate measures such as Risk Treatment to counter/ mitigate, the risks identified.

2.21.5 O&M Agency will responsible for preparing and carry out testing and execution of Business Continuity Plan and Disaster Recovery Plan

2.21.6 O&M Agency will conduct Workshops and Training sessions for all GSDC stake holders to create awareness of ISMS implementation. GSDC stake owners will be made familiar with ISMS implementation and risk management approach selected for SDC.

2.21.7 O&M agency will be responsible to apply and maintain the latest ISO 27001 certification for the contract duration.

2.22 ISO 20000 ITIL (Information Technology Infrastructure Library) Standard for GSDC

2.22.1 ISO/IEC 20000 adoption in Gujarat SDC infrastructure helps in ascertaining that the Services delivered to the GIL / DST, GOG / User Departments by the O&M agency are:

(a) As per the agreed Service levels

(b) Professionally managed with domain expertise

(c) Project Risks are well understood and managed

2.22.2 O&M agency shall be responsible to implement ISO/IEC 20000 standard which shall promote the adoption of an integrated process approach to effectively deliver managed services to meet the SDC, GIL / DST, GOG and User Departments.

2.22.3 **Methodologies for ITSM/ITIL standard:** applicable methodology shall be adopted to implement ISO 20000 standard to establish the objectives and processes necessary to deliver results in accordance with GIL / DST, GOG requirements as well as the SDC policies and to implement the processes accordingly. O&M agency shall monitor and measure processes and services against policies objectives and requirements and report the results and take actions on the differences and continually improve process performance.

2.22.4 Alignment of information technology services and strategy.

2.22.5 To create a formal framework for current service improvement projects.

2.22.6 To improve relationship between different departments via better definitions & more

clarity in terms of responsibility and goals.

2.22.7 To create stable framework for both resource training and service management automation.

2.22.8 O&M Agency will conduct Workshops and Training sessions for all GSDC stake holders to create awareness of ISMS implementation. GSDC stake owners will be made familiar with ISMS implementation and risk management approach selected for SDC.

2.22.9 O&M agency will be responsible to apply and maintain the latest ISO 20000 certification for the contract duration

2.23 Database Administration & Management Services

2.23.1 The activities shall include, but not limited to the following:

(a) End-to-end management of database on an ongoing basis to ensure smooth functioning of the same.

(b) Management of changes to database schema, disk space, storage, user roles.

(c) Conduct code and configuration reviews to provide tuning inputs to the State / User Department in order to improve the application & DB performance or resolve bottlenecks if any.

(d) Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.

(e) Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions.

(f) Continuous monitoring and periodic review of Database Logs, to identify performance bottlenecks, suspicious activities, signs of compromise, etc.

(g) Use of DBA tools related to performing database creation, maintenance, and database monitoring tasks.

2.24 Change Management

2.24.1 The activities shall include the following, but not limited to the following:

(a) Tracking the changes in hard / soft configurations, changes to applications, changes to policies, applying of upgrades / updates / patches, etc.

(b) Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.

(c) Any changes (as and when required) at the architecture or configuration level for GSDC related components is part of the O&M activity and it should be carried out by the O&M Agency.

2.25 Application Related Services

2.25.1 The Information in this clause shall govern the methodology by which Application Related Services shall be provided to the State Data Centre at Gandhinagar.

2.25.2 Application related services shall complete the entire spectrum of services to be provided by the O&M agency. The objective of application related services is to facilitate the user departments by providing them with “One Stop Shop” for their requirements. As a part of these services, the O&M agency shall provide support for bug fixes, installation of OS & required softwares, enhancements, operational support,

and assistance to the User Department. These services have been classified under the following four categories depending upon the extent of application support that may be required by the User Departments:

(a) Application Monitoring and troubleshooting
(b) Website and Application hosting and management
(c) Application Enhancement
(d) Application Migration

2.25.3 The application hosted at the SDC will require management in the functionalities which includes, but not limited to the following:

(a) Monitor the departmental applications on a day-to-day basis to ensure that the application functions reliably.
(b) Monitor application to ensure that the application does not suspend, hang etc.
(c) Monitor components, including but not limited to, Application servers, Database Servers, Web Servers, Middleware and other application servers on an ongoing basis to ensure smooth functioning of the applications.
(d) Ability to troubleshoot problems, monitor erratic behavior through the application logs. Further, the O&M agency shall co-ordinate with application vendor for resolution of application related issues.

2.25.4 Coordinate with the application vendor / user department to manage and install patch upgrade as and when required with minimal downtime. Ensure configuration management and backups of patch to rollback in case of problems.

2.26 O&M of Physical Infrastructure

2.26.1 All the devices installed as part of the physical infrastructure should be monitored and managed on a 24x7x365 basis. The physical infrastructure management and maintenance services shall include, but not limited to the following:

(a) Operation and management of Building Management System. Proactive monitoring of the entire Physical infrastructure installed at through Building Management Software. Current BMS tool may be upgraded/replaced.
(b) Management of Physical Access to the premises as per the policies set by the Department of Science and Technology.
(c) Monitoring, recording and reporting usual and unusual movements in and around the premises.
(d) Material inward/ outward control as per policies set by the Department of Science and Technology.
(e) All human movement should be monitored.
(f) Monitoring and managing safety and surveillance equipment like CCTV, Access Control, Fire detection and Suppression etc.
(g) Issuing access control as per approval from the Department of Science and Technology.
(h) Reporting incidents to the Department of Science and Technology.
(i) Co-ordinate with respective trusted personnel and communicate with authorized maintenance personnel for various utilities at the Data Centre as required.
(j) Manage and monitor Diesel level/ requirements at its full capacity of the DG Set.

Prevent the contamination of diesel by diesel bug or any other microorganisms. Diesel is consumable item, which will be charged on actual basis.

(k) Vendor Co-ordination for various physical Infrastructure components

(l) The bidder shall install a mechanism which will generate logs for diesel consumed through the use of tamper proof automatic measurement.

(m) Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent or higher configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.

(n) The selected bidder shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by TENDERER or authorized authority.

(o) CCTV footage is to be kept to meet legal, regulatory, ISO Policies compliance requirements and would be stored in GSDC SAN/NAS during the contract period. The record retention period shall be as per policies of TENDERER.

(p) The bidder should ensure high availability for power on 24x7x365 basis and should maintain all the systems/subsystems for power availability.

(q) Ensure availability of the physical Infrastructure including Power, include of DG, UPS, Cooling, CCTV, Access Control, Intelligent Racks, Fire detection and suppression systems, Rodent Repellent systems, Water leak Detection Systems and other components included as part of physical Infrastructure related services.

(r) O&M AGENCY will have to submit monthly/quarterly MIS reports of each components as per the SLA

(s) O&M AGENCY should log SR/Incidents calls in service desk related to each component.

(t) Proactive and reactive maintenance, repair or replacement of defective components (IT and Non-IT/ Hardware and Software) related to Physical Infrastructure systems and sub-systems. The cost of repair and replacement shall be borne by the selected bidder. IT and Non-IT hardware here refers to systems such as IT and non-IT hardware and software being used for maintaining and monitoring Physical Infrastructure e.g., BMS, Access control, etc.

(u) For network and security devices **(Annexure-B),** the bidder, at his discretion, can take back-to-back CAMC of network and security components or refresh with equal or higher capabilities.

(v) For non-IT, servers, storage, and backup mentioned in this RFP bidder can do back-to-back OEM (**Annexure A, D/D1 and E/E1)** agreement through authorized Distributor or partner for AMC/Warranty and shall provide a copy of the service level agreement signed with respective OEMs.

(w) The bidder, at his discretion, may upgrade/replace /refresh IT components (Annexure A & B) with equal or higher capabilities. Bidder should take prior approval of the GSDC before the replacement. In such cases successful bidder has to perform all migration activity within downtime given by Tenderer. Delay in such

implementation/migration will attract the penalty.

(x) Successful bidder, in case of refreshed components, needs to maintain existing hardware/ software /solution as per SLA in this RFP, until successful FAT of refresh/replacement of existing component.

(y) The Bidder shall maintain documentation for installation, testing, commissioning of any system/sub-systems that is installed or upgraded.

(z) Acceptance test shall be carried out for any system that is installed and/or upgraded.

(aa) The bidder shall carry out comprehensive fire drills as per Policy/Guidelines specified by DST and submit drill reports to TENDERER on regular intervals.

(bb) Bidder shall record all the incidents/issues related to physical infrastructure services, security, systems and Sub-systems in the Helpdesk.

(cc) The bidder shall carry out periodic Risk assessment of the Physical Infrastructure as per Policy/Guidelines specified by DST and provide a Risk Assessment report including recommendations. Assessments/Policies/Guidelines defined are based on ISO 27001 and ISO 20000 Standards.

(dd) The bidder shall provide training to resources deployed at periodically.

(ee) The bidder shall carry out current state assessment on an annual basis to determine the state of all the components installed and maintained, on completion the bidder shall submit a recommendation/up gradation report.

(ff) Full compliance to all the policies, procedures, processes, guidelines, Government-Acts, Rules & Regulations, etc. The bidder shall provide full compliance/adherence of all activities performed by them, to the aforementioned statutes, without any additional cost to TENDERER.

(gg) Maintenance and monitoring of Current CCTV System with IP base Cameras with high resolution and night vision cameras. The O&M Agency is responsible for the integration of the Cameras with the NVR/DVR/SAN Storage and ensure that at least 30 days 720p HD CCTV Footage is stored on the NVR and backup of CCTV footage beyond 30 days should be taken existing SAN/Tape Library, of GSDC. The bidder should ensure that the CCTV system is compatible with SAN/NAS/Tape Library of GSDC.

2.26.2 Transformer, Circuit Breaker, Electricity and DG Set Maintenance & Management:

i. The O&M agency shall be responsible for Operations, Management and Comprehensive Annual Maintenance of Transformer, Circuit Breaker, HT/LT Power Cables, Electricity and Diesel Management for the entire project period. The O&M agency shall ensure that diesel shall be there in the DG sets at its full capacity in case of power failure. O&M agency has to maintain register for monitoring and reimbursing the diesel consumption for the DG set. The DG set will be procured by Tenderer along with its maintenance support & the selected O&M agency will be responsible for its Operation & maintenance only.

ii. Tenderer has procured New DG set (Supernova 1010 KVA) with 1-year warranty support, post that bidder need to consider CAMC from expiry date and O&M from contract start date.

New DG set Detail is as follow;

- New DG set -Supernova 1010 KVA (Perkins engine)
- Serial- LFS3LX22B34529
- Warranty Completion Date- FAT pending.
- If DIT/GIL wish, then only consider AMC rate provided by bidder from 2nd year onwards

iii. Procedure for monitoring and reimbursing the Diesel consumption for the DG set:

(a) There will be a register maintained and kept with the O&M agency showing the following columns:

Sr. No	Date	Current Reading	Fuel Available	Date of filling	Qty. Filled	Total fuel available	Signature of DST, GoG	Signature of O&M agency
1								
2								

(b) Reimbursement of diesel cost will be done on Monthly basis along with Monthly Payment.

(c) TENDERER shall verify the diesel consumption from the log book maintained and MIS generated.

(d) The O&M agency will submit the bill (original bills of petrol/diesel pump) for every purchase along with their invoice for reimbursement.

(e) Payment will be processed by TENDERER based upon verification of bill with the register entry on Monthly basis.

2.27 Preventive Maintenance Services

2.27.1 Check, Repair/Replace any loose contacts in the cables/connectors & connections on a regular basis.

2.27.2 Conduct preventive maintenance every three months or as directed by the TENDERER (including inspection, testing, satisfactory execution of diagnostics and necessary repairing of the equipment).

2.27.3 Cleaning and removal of dust, dirt etc. from the interior and exterior of the equipment on a daily basis.

2.27.4 Preventive Maintenance Activities of components as per their manufactures' recommendation/advice.

2.27.5 The Data Centre operator will keep a web based monitoring format and schedule of preventive maintenance services and shall provide reports to the DST, GoG as and when asked.

2.27.6 The Preventive Maintenance shall be carried out in Non-Prime Hours only under prior intimation and approval from TENDERER.

2.28 Corrective Maintenance Services

2.28.1 Warranty and maintenance/troubleshooting of hardware problem of all supplied

IT & Non-IT Infrastructure including network (active/passive) equipment, Security, etc. and support infrastructure equipment UPS, AC, DG Set etc. and rectification of the same.

2.28.2 Troubleshooting of problems arising in the network and resolving the same.

2.28.3 Documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems.

2.29 Asset Management Services

2.29.1 The O&M agency shall be required to create centralized online repository of all the equipment/software, licenses procured/Installed, all contracts/WO issued by DST/GIL . The details of all assets like hardware, software, peripherals, manuals, media and other related peripherals, etc., shall be maintained by recording information like make, model, configuration details, serial numbers, licensing agreements, warranty, place of installation etc.

2.29.2 Record installation and removal of any equipment under the project and inform TENDERER even if it is temporary.

2.29.3 Create Software details with information such as Licenses, cost, Version Numbers, validity, support if any and Registration Details.

2.29.4 Perform software license management, notify TENDERER on licensing contract renewal and assist them in getting the license renewed.

2.29.5 Asset Management services of physical and IT infrastructure under the project must conform to ITIL framework.

2.30 **Configuration/Reconfiguration Management Services**

2.30.1 The successful bidder shall maintain complete configuration including reconfiguration (in & soft form in safe environment) for all equipment and handover the same to the TENDERER at the time of completion of project or as and when asked by the TENDERER.

2.30.2 The O&M agency shall define and adhere to the change management procedures and also ensure that no unauthorized changes are carried out. Any changes shall be incorporated with prior approval of the TENDERER.

2.30.3 The O&M agency shall do proper version management of these configurations as they are bound to change from time to time.

2.30.4 These configurations shall not be accessible in general and must be kept confidential.

2.31 Resource Requirement for Operation, Services and Maintenance

- The minimum requirement of manpower resources, their qualification and responsibility of each resource is given below. This is minimum indicative list of resources and based on actual requirements, the bidder may deploy any number of resources to meet the SLA. TENDERER shall not pay any cost for additional resources required to operate, maintain, monitor & manage the GSDC as per the SLA. In case support staff is not available or is on leave, the bidder is required to provide the

alternative personnel with same or higher technical capabilities of the non-available personnel. Prior intimation is required for such replacement and non-availability of the personnel. If prior intimation is not provided, penalty will be levied .

- Bidder has to provide additional onsite resources to maintain SLA and provide operational support 24x7x365.
- In case of exigency & requirement, manpower should be available onsite within 30 mins during non-working hours.

Note: Below resources are indicative. GSDC is giving 24 x7 services and has heterogeneous OS, DB, network, security etc., the Bidder should evaluate scope of work, work load, domain, subject expertise and SLA compliance and based on that depute number of resources.

Sr. No.	Designation	Gen.	Min. Qualification, Relevant Experience & Certifications
1	Technical Manager (SDC)	01	Graduate + Min. 15 Years relevant experience in IT/ITeS (minimum 6 years' experience for managing data centre) + PMP/ PRINCE2 Certified
2	Cyber Security Expert	02	Graduate + Min 10 years of Relevant experience in Network security Management + Certification: CCSE / PCNSE / CISM / CISA / CISSP/CEH
3	Network Expert	01	Graduate + Min 10 years of Relevant experience in Network Management + CCNP or equivalent
4	Cloud Specialist	02	Graduate + Min 10 Years relevant experience in IT cloud management+ OEM Certified.
5	Server Admin	01	Graduate + Min 10 years Relevant experience of different flavors of OS + OEM certified experts.
6	Database Admin (DBA - expert	01	Graduate + Min 10 years Relevant experience + OEM certified engineer
7	Storage & Backup Admin	01	Graduate + Min 10 years Relevant experience + OEM certified engineer
8	EMS/NMS Engineer	01	Graduate + Min 8 years of Relevant experience + OEM certified engineer
9	BMS Manager – L3	01	Graduate + Min 10 years or Diploma + Min 15 years of Relevant experience
10	BMS Engineer – L2	03	Graduate + Min 5 years or Diploma + min 10 years of Relevant experience
11	Electrician	01	Diploma + Min 4 years or ITI + Min 8 years of Relevant experience
	Total - GSDC	**15**	

Penalties for non-availability of aforesaid resources will be Rs 15000 per day per resource.

Roles & Responsibilities of proposed Manpower resources

S. No.	Description	Roles & Responsibilities
1	Technical Manager (SDC)	• Responsible for overall management of the Data Centre, user SLA commitments, performance, availability, response time, problem resolution. • Should be responsible for effective Resource management, System & Resource planning, based on business forecast • Overall in-charge of O&M of the IT Infrastructure and SDC. • Coordinating with third party agencies, bandwidth operators and software/equipment's vendors. • Should be the single point contact (SPOC) for managerial responsibilities and direct interface with TENDERER. • Management & compliance of ISO Policies, Process, Procedures and other applicable legislations, policies, guidelines…etc. • Carry out Documentation, technical report writing…etc. • Interface & co-ordinate with stakeholders for the Tickets raised in the Help Desk. • Should have very strong communication skills and technical writing skills. • Should possess working knowledge of ITIL, ISO 20000 & ISO 27001 • Draft BCP process for identified critical applications • Run through mock drills of approved DR and BCP periodically • Adopt and develop DR and BCP guideline and other industry best practices
2	Cyber Security Expert	• Responsible for Firewall Management, Intrusion Management, Antivirus & Patch Management, Security Management. • Responsible for Firewall Rules and Policies Management and Troubleshooting Implementing of NAT/PAT, SSH, signatures, etc. • Plan & Implement comprehensive security policies and practices for entire infrastructure. Signatures updating, blocking of unwanted traffic Antivirus updates, Patch updates, managing the network security on day to day basis. • Monitoring any flooding, DoS, Intrusion attempt in real time during the office hours • Penetration Testing, Manual Testing, Writing Custom Exploits/Scripts. • Expertise in understanding information security, incident response, intrusion detection and prevention • Expertise in Data & Traffic Analysis, Network (TCP/IP), UNIX, Windows, Linux. • Experience in using System Security/Vulnerability Scanners /Sniffers • Experience with operating SIEM tool • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning

3	Network Expert	• Responsible for network uptime, performance and other related services. • Network monitoring and proactive network uptime maintenance. • Network management (routing), Router Configuration and Troubleshooting, upgradation, Link Performance Management of L3 and L2 Switch at Data Center and GSWAN Network on day to day basis. • Support administration, Change Management, Liaison with Bandwidth Provider officials and external vendors, bandwidth and facility management • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning
4	Cloud Specialist	• Should have expert knowledge of VM allocation, patching , day to day operation, configuration and management functionality, cloud Security etc. but not limited to below points • On and above Roles of SME Server domain, he should have knowledge of MS Cloud as existing cloud is based on System center • In future cloud may change , so should have advance knowledge of Virtualization, Orchestration layer, Configuration Manager, Self Service portal, cloud tools etc. • Experienced in quality practices, techniques, and tools at all layers of the stack • Knowledge of the IaaS, PaaS, SaaS, • Installation, configuration and management knowledge of Containers and Micro services architectures • Expert understanding and experience in deployment and troubleshooting various technologies of different Cloud and Systems automation, enterprise network communications/protocols, Windows and Linux authentication and authorization, Virtualization technologies • Should have integration knowledge of Private, Public and Hybrid cloud • Serve as an integrator between business needs and technology solutions, helping to create technology solutions • Build, install, configure, analyze, tune, and troubleshoot Windows operating systems both on premise and in cloud IaaS providers • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning

5	Server Admin	• Managing server infrastructure services for GSDC's System maintenance, storage, backup etc. • Responsible for system configuration, scalability, performance, load balancing, OS administration / management, troubleshooting & Debugging and monitoring of servers. • Implement the back-up plan for storing and retrieving of data, maintain servers, machines, printers and also responsible in resolving the real time (RT) requests raised by users as per SLA. • Internet Management, E-Mail management, Service Management, End point solutions management, Systems Management, Proxy, content filtering and Internet access management for users, managing Messaging servers. • Monitoring application components, including Application servers, Web Servers, on an ongoing basis to ensure smooth functioning of the applications.
5	Server Admin	• Role involves senior level troubleshooting / Root Cause Analysis (RCA) for areas including, but not limited to: • Active Directory (AD) related issues - DNS zone issues; Sites • Client support - Provide recommendations for configuration or other improvements to the environment • Expert Knowledge of Microsoft Windows 2012 to 2022, Linux,unix OSS Administration, Install, Configuration • Expertise to fast learn and implementation of Open Source Software in DC Environment • Expertise in Container, Docker, Kubernetes , new technology • Expert knowledge on Virtualization: VMWare, Microsoft System Center / HyperV Administration, PowerShell • Should have expertise in troubleshooting, co-ordination with support of OEMs • Expert Knowledge on Microsoft & other OS troubleshooting skills and tools. Including OS Hardening and Vulnerability assessment. • Knowledge of TCP/IP, DHCP, DNS and Troubleshooting. • Knowledge on TCP/IP, DNS, DHCP, Power shell scripting • Knowledge of AD group policies. • Working knowledge of Linux systems Cloud - Azure and AWS. • Backup Technologies (Commvault,networker etc) • Should have worked on supporting an enterprise class Data Center. • Familiarity with development, tools, languages, process, methods and troubleshooting of Microsoft Azure based solutions. • ITIL Process knowledge (Problem, Incident, Change Management) • Exceptional communication skills • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning

6	Database Administrator	• Responsible for various databases like, but not limited, mysql, mssql ,postgresql, nosql administration, should be responsible for database and application change management procedure. • Responsible for management of database repository, creation, deletion, modification, backup and restore of databases and their tables. • Troubleshooting knowledge of different RDBMS like MS SQL, MySQL , PostGreSQL, Oracle and No-SQLs (MongoDB,CouchDB etc) • Microsoft (MS), MySQL, PostgreSQl Clustering troubleshooting • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning
7	Storage & Backup Admin	• Backup of operating system, database and application as per stipulated policies at the SDC. • Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies. • Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by User Departments or in case of upgrades and configuration changes to the system. • Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes. • Media management including, but not limited to, tagging, cross- referencing, storing, logging, testing, and vaulting in fire proof cabinets. • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning
8	EMS/NMS Engineer	• The resource should be able to administrate and manage the existing EMS Tools (Refer Annexure for the detailed list of tools) / the new EMS tools which are supplied as a part of this RFP. • Managing Network operations using EMS tool. • Managing Network Monitoring. • Responsible for monitoring of adherence to defined SLA by vendors by making effective utilization of deployed EMS tools in GSDC and GSWAN. • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management. • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning

9	BMS/ Facility Manager with Technical Background (24X7 Shift)	• PSO (Physical Security Officer) for operations of control room which includes CCTV, ACS, PRS, WLDS, FAS, FSS and other technical components required for smooth functioning of the Data Centre. • Good communication skills to be able to interact with vendors. • Responsible to prepared gap analysis in deployed /proposed solutions • Design and develop infrastructure blueprints for the implementation of new solutions. • Responsible for impact analysis and design modifications to existing systems to support new solutions. • Responsible for end-to-end ticket management.
10	Technical Assistant/ Electrician	• Regular maintenance and daily check-up of DG Set, Transformer and HT Circuit Breaker, Power Cables, LT switch gear check-up and meter readings, Lighting Maintenance.

Note: It is clarified that the responsibilities and numbers mentioned against the position type are only indicative, it is the responsibility of bidder to provide requisite resources of right competency and experience to completely discharge functional requirements of Operations & management, Error reporting, SLA compliance, support (installation of applications, software, networking devices, OS, Storage, Backup) and the cost of such manpower should be part of the bid being quoted by the bidder.

2.31.1 The manpower deployed by the bidder for carrying out and providing services shall necessarily be Core resources except the following:
Electrical Assistant

2.31.2 All O&M resources deployed by the bidder should be on the bidders' payroll. The complete set of manpower resources proposed by the Bidder shall be on-site manpower only and strictly dedicated for this contract. Noncompliance of such deployment would result into imposition of penalty / termination of the contract as per the terms and conditions of RFP.

2.31.3 Before deployment/replacement of any manpower, successful bidder has to submit the resume and after taking interview by the TENDERER, bidder can deploy the manpower after selection. After taking interview, if candidate found best suitable without relaxing min experience & certifications, bidder may relax above mentioned minimum education qualification for that candidate.

2.31.4 The manpower deployed by the bidder shall report to the respective nodal officers nominated by TENDERER.

2.31.5 The Bidder has to provide supporting IT and Communication Infrastructure to such manpower, during entire contract period without any extra cost to the TENDERER. Workspace shall be made available to the bidder by the concerned offices. Bidder has to ensure that the Support personnel deputed during all stages of the project shall carry an Identity Card duly authenticated by the TENDERER.

2.32 Hand-over/take-over existing Operations (Duration 2 Months)

- If, other than the existing agency is awarded the work, the selected agency will be responsible to complete the transfer of Knowledge & Handing/Taking over activity from existing agency within **two** months of issuance of LOI/WO.
- After successful completion of H/T over process, all supporting documents will be handed over to the Selected Agency.
- During this period, only O&M charges will be paid to Selected Agency on pro-rata basis. SLA or Penalty clause will not be applicable during **2 months** of Hand-over/Take-over process. Selected Agency will responsible to provide confirmation about successful Hand-over/Take over operations from existing agency at the end of **2 months** period. The selected agency shall depute the required resources as per the requirements of tender document for carrying out the operations activity.
- Successful agency is required to issue Completion certification for completion of this H/T over process. Existing Agency will provide necessary handholding and transition support to new agency.

Section III: Service Level Agreement (SLA)

3.1. Definition

SLA defines the terms of the O&M agency's responsibility in ensuring the performance of the network based on the agreed performance indicators as detailed in the agreement.

3.2. Network uptime

The table below summarizes the performance indicators for the services to be offered by the bidder. The detailed description of the performance indicators, SLA Terms and their definitions are elaborated in the following sections.

3.3. Network SLA Terms & Definitions

S. No.	SLA Terms	Description
1	Uptime	'Uptime' refers to GSDC availability i.e. "%Uptime" means ratio of 'up time' (in minutes) in a month to Total time (in minutes) in the month multiplied by 100.
2	Planned Outage	'Planned Outage' refers to unavailability of GSDC services due to infrastructure maintenance activities such as configuration changes, up gradation or changes to any supporting infrastructure. Details related to such planned outage shall be approved by the TENDERER or authorized authority and shall be notified to all the concerned stakeholder in advance (at least seven working days before). It is desirable that such outage shall be taken on Sundays or other Government holidays to the extent possible.
3	Unplanned Outage	'Unplanned Outage' refers to an instance in which no traffic can pass in or out GSDC to which users are connected

3.4. Denial of Service

3.4.1. Denial of Service (DoS) is the most common form of attack on the Network, which leads to network unavailability for the genuine network users. Successful Bidder shall respond to Denial-of-Service attacks reported by departments/ GSWAN users or GSWAN maintenance personnel within 15 minutes of intimation to the helpdesk. Denial of Service attack can be defined as sudden burst of network traffic leading to more than 90-95% utilization of the GSWAN bandwidth in any segment or complete network. In such a scenario operator shall perform an analysis of the issue, verify whether the network utilization is due to genuine user requirements or it is a denial of service attack. In case it is identified as DoS attack, operator shall identify the source of Denial of Service attack, and shall disconnect the source or network from GSWAN backbone and resolve the issue to ensure availability and performance of the backbone.

3.5. GSDC Operations Management

3.5.1. Successful bidder is required to maintain Contact Center (Helpdesk) at the State level with an appropriate Helpdesk tool. Helpdesk shall act as a SPOC (Single Point of Contact) for all the GSDC related incidents, service requests, issues reported by the government departments or any other related stakeholders of the GSDC. Each issue, incident, service request need to be recorded in the Helpdesk tool (with allocation of unique identification

number) and the response,resolution, closure timelines shall be monitored by the State or its authorized agencies.

Sr.No.	Severity	Response Time	Resolution Time
1	Level 1	15 mins	30 Mins
2	Level 2	30 mins	1 hrs
3	Level 3	60 mins	3 hrs
4	Level 4	120 mins	10 hrs

Section IV: Penalties

4.1. GSDC

Successful Bidder shall be paid Monthly Payment (MP) as per the services provided to TENDERER. The overall penalty would be calculated cumulatively & it will be generally capped at 10% of MP amount. If the cap of overall penalty is reached in two consecutive Months, the penalty cap for the third month onwards, for each Month will increase by 5% over the penalty cap for the preceding month till it reaches 25% of the MP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the TENDERER shall be within its rights to undertake termination of contract if or anytime the penalty increases by 15% of the MP. Once the penalty cap has increased beyond 10%, if the bidder through better performance delivery for any month, brings the leviable penalty below 10% then the computation of the 1st of the 2 consecutive Months as referred above will reset and will begin afresh. Availability will be calculated on a monthly basis.

4.1.1 Penalties for delay in takeover:

If successful bidder fails to complete the taking over of existing O&M of GSDC within the 90 working days from the project kick off date , a Penalty of 0.50% of Monthly Payment for each week of delay or part thereof shall be levied, until the completion of take over process and signoff from DST/GIL. If the delay continues beyond 12 weeks, DST/GIL may terminate the Agreement and forfeit the PBG.

4.1.2 Penalty for Delay in implementation of EMS/NMS and refresh/upgrade/replacement of devices/solutions:

S. No.	Activity	Timeline	Penalty
1	Delay in SITC & FAT of supplied Hardware/software	T+ 90days	0.5% of Contract value per week or part thereof for delay (Delay beyond T+90days DST/GIL may terminate the contract and/or Forfeit the PBG).

T= O & M start date

Note: The above clause for penalties due to delay in FAT shall only be applicable for the delay attributed solely to the successful bidder as per his roles and responsibilities, delay due to other reasons shall not be considered.

4.1.3 Penalty for Delay in taking Insurance:

Successful bidder will take insurance of the equipment under O&M within Six months from the date of signing of contract. Penalty of INR 1 lakh per week after six months from the kick of date shall be levied.

4.1.4 Penalty for delay in VA/PT:

The successful bidder has to conduct VA/PT as per defined interval as mentioned in this RFP. The penalty for delay in completing VA/PT attributed to Bidder will be Rs. 2000/Day.

4.1.5 Delay in ISO certification Number of days Renewal due date

For any delay in ISO Certification, the penalty for delay attributed to bidder will be Rs. 15,000 /- per day

4.2. SLAs for GSDC

Sl. No.	SLA	Target	Penalties in case of breach in SLA	Remarks
1	Uptime of all IT & Non-IT components & services under scope	99.741% (at each individual component level)	For each 0.5 slab (lower) a penalty 1.0 % on MP shall be charged for each component.	For each component 99.241-99.741 - 1.0% of MP 98.741-99.241 - 2.0% of MP and so on. If the uptime goes below 96.741, additional penalty of 1% will be charged on MP for each slab 1% downtime.
2	Closure of Audit Findings	100.00%	Rs.10,000/- per day delay for closure of each high and medium classified audit finding Rs. 2,000/- per day delay for closure of each low classified audit finding	Periodic Audits will be conducted by DST or DST Authorized personnel, the Audit Findings shall be closed by the O&M Agency within 21 working days or a s per the closure schedule defined by the Auditor. If there is any delay in closing the audit findings then penalties will be levied.

3	Incident Resolution	Priority Level 1 Incident - Within 30 mins Priority Level 2 Incident - Within 1 hr Priority Level 3 Incident - Within 3 hrs. Priority Level 4 Incident - Within 10 hrs.	Level 1 Incident 0.5% of MP for every 1 hr or part thereof delay in resolution; Level 2 Incident 0.5% of MP for every 1 Hr or part thereof delay in resolution; Level 3 Incident 0.5% of MP for every 2 hrs or part thereof delay in resolution Level 4 Incident 0.5% of MP for every 5 hrs or part thereof delay in resolution	Incidents will be logged in the Helpdesk and the O&M Agency will have to resolve the incident and provide necessary updates through the Help Desk Portal and co-ordinate with the stakeholders. Root Cause should be identified for all incidents; if root cause is not identified then additional penalties will be levied.
4	Request Resolution	Priority Level 1 Request - Within 30 mins Priority Level 2 Request - Within 1 hr Priority Level 3 Request - Within 3 hrs. Priority Level 4 Request - Within 10 hrs.	Level 1 Request 0.25% of MP for every 1 hr or part thereof delay in resolution; Level 2 Request 0.25% of MP for every 1 Hr or part thereof delay in resolution; Level 3 Request 0.25% of MP for every 2 hrs or part thereof delay in resolution Level 4 Request 0.25% of MP for every 5 hrs or part thereof delay in resolution	Requests (like e-mail password reset, firewall port opening, hardening,hosting etc.) will be logged in the Helpdesk and the O&M Agency will have to resolve the request and provide necessary updates through the Help Desk Portal and co-ordinate with the stakeholders.
5	Change Resolution	Timeline as defined in – Implementation plan and approved in Change advisory Board (CAB)	Delay of Rs. 1000 per day for closure of Change Request.	Penalty will be applicable only in case of delay attributed to the bidder.

6	Security Breach	Detection of security Breach - within 30 minutes Mitigation of Security Breach - within 1 hr from the time of Breach	3% Of MP for every 30 minutes delay in detection and additional 1% for every 1 hr delay in the mitigation of security breach	The security breach will include but not limited to successful penetration of any Virus, trojan, malwares, zero- day attacks, intrusion, Denial of Service Attacks etc., up to the server level. In case of any compromise of data due to the Security Breach then double penalty will be levied (this will not be counted within the maximum penalty cap limit).
7	Miscellaneous Penalty for Cloud	Provisioning and De-Provisioning of Virtual Machines	Within 30 Minutes	Rs. 1000 for 1st Hour Rs. 3000/Hour for delay in every subsequent Hour
8		Uptime of Virtual Machines, Cloud Management Layer, Virtualization and Cloud Solution	99.974%	For each component 99.241-99.741 - 1.0% of MP & 98.741-99.241 - 2.0% of MP and so on If the uptime goes below 96.741, additional penalty of 1% will be charged on MP for each slab 1% downtime.

4.3. Improvement Strategy & Incentives

a) The bidder is expected to put in efforts to improve the defect management processes by improving on the response as well as resolution time of the incidents like downtime of GSDC services. Also, seamless availability of GSDC services heavily depends on multiple factors like:
   - Co-ordination between resources of various agencies like power utility, bandwidth, O&M operator, application developer & GoG department / offices, etc.
   - Proactive monitoring & analysis of occurrence of incidents (security, downtime, etc.) & availability of GSDC services
   - Seamless availability of GSDC services

b) The successful bidder shall form a process improvement strategy for better availability of GSDC services. The improvement strategy shall focus on the proactive monitoring and

analysis of historical incidents & its frequency of its occurrence; standard operating process & measures for effective co-ordination between the stakeholders (within & outside GoG) & proactive measures in reducing the incidents resulting in loss of GSDC services. The bidder may deploy technological tool for defect management & its resolution tracking. Regardless of the cause/factor resulting into non-availability of GSDC services, the ultimate objective of this improvement strategy is to achieve improvement in-

- Response & resolution time for incidents
- Availability of GSDC services by reducing incidents resulting into non-availability of GSDC services
- Satisfaction of users of services of GSDC

c) With a goal to achieve zero defect resulting into the better availability of GSDC services, the tenderer shall incentivize the appointed O&M agency on following Parameters:

Sr. No.	Deliverable	Targets	Incentive Amount / %
2	Technology innovations / new initiatives for performance improvement like (any of the following): • Find out the vulnerabilities which can be convent into security breach (like ZERO day) in existing system • Performing Ethical hacking for GSDC and give constructive contribution in improving the security of GSDC • Implementation of Open Source Software (OSS) which will improve the functionality, operation of GSDC. IP will remain with DST/GSDC. • Reward against reduction of complain by implementing free third party tool (which is not in DCO's	Per Instance	Appreciation letter will be given by GSDC/DST.

	O&M and AMC)		
3	Best employee award to encourage employee	Quarterly (Best Feedbacks / Comments received from top officials)	Top Performer award to the employee in the form of appreciation letter will be given by GSDC/DST.
4	Reward to employee against the new invention, Paper Submission in International General. However, IP will remain with DST/GSDC.	-	Appreciation letter will be given by GSDC/DST.