NOTICE INVITING e-TENDER

Online Tender documents are invited for "Revamping & Physical Expansion of West Bengal State Data Center". Reputed System Integrators having sufficient experience and credentials for successful completion of **"Similar Nature"** of work in a Government Department/PSU/Autonomous Body or any reputed organization. Bidder must have adequate Service Engineer for providing on-site warranty service within the stipulated time.

1.	Tender No. & Date	WTL/PAR/SDC/17-18/030 Dated 27.11.2017
2.	Tender Version No.	1.0
3.	Brief description of material	Revamping & Physical Expansion of West Bengal State Data Center
4.	Tender Fee	Rs. 10,000.00 (Rupees Ten thousand only)
5.	Earnest Money Deposit	Rs. 1,20,00,000.00 (Rupees One Crore twenty lakhs only) in the form of Demand Draft from any Scheduled bank in favour of Webel Technology Limited payable at Kolkata
6.	Date of Downloading/Sale of Tender document	27.11.2017
7.	Pre-Bid Meeting date & time	04.12.2017 at 11.30Hrs • Only two persons for each intending bidder's organization, who will submit the Tender Fee, will be allowed to attend the Pre Bid Meeting. • The person should have proper authorization in respective company Letter Head. • Only queries as per format (Section - O) reaching WTL by 01.12.2017 at 16.00 hrs will be taken for decision. • Queries will be entertained for those bidders who will submit the Tender Fee. • Queries will be sent to Mr. Sunit Bhattacharya (sunit.bhattacharya@webel-india.com / sunit.bhattacharya@wtl.gov.in) copy to Manager (Purchase) (wtlpurchase@gmail.com/arunava.saha@wtl.co.in) and Mr. Birojit Paul (birojit.paul@webel-india.com/birojit.paul@wtl.gov.in)
8.	Bid Submission Start date & time	12.12.2017 at 14.00 Hrs
9.	Last date & time of EMD & Tender Fee submission	20.12.2017 at 14.00 Hrs
10.	Last date & time of Bid Submission	18.12.2017 at 15.00 Hrs
11.	Date & time of Technical Bid Opening	20.12.2017 at 15.00 Hrs
12.	Venue of Pre-Bid Meeting & submission of EMD & Tender Application Fee	WEBEL TECHNOLOGY LIMITED (A Government. of West Bengal Undertaking) Plot - 5, Block – BP, Sector – V, Salt Lake City, Kolkata – 700091.
13.	Contact person	Mr. Sunit Bhattacharya (sunit.bhattacharya@webel-india.com/sunit.bhattacharya@wtl.gov.in)/ Mr. Birojit Paul (birojit.paul@webel-india.com / birojit.paul@wtl.gov.in)

1. Intending bidder may download the tender documents from the website **https://wbtenders.gov.in** directly with the help of Digital Signature Certificate. Necessary cost of tender documents (tender application fee) may be remitted through Demand Draft issued from any Scheduled Bank in favour of "Webel Technology Limited", payable at Kolkata and also to be documented through e-filling. Cost of Earnest Money Deposit (EMD) may be remitted through Demand Draft issued from any Scheduled Bank in favour of "Webel Technology Limited", payable at Kolkata and also to be documented through e-filling. The original Demand Draft against tender fees & Earnest Money Deposit (EMD) should be submitted physically to the Manager (Purchase)/Manager (Finance), Webel Technology Limited, Plot – 5, Block – BP, Sector-V, Salt Lake City, Kolkata-700 091 under sealed cover on or before 14:00 Hrs of 20.12.2017.

2. Both Techno Commercial Bid and Financial Bidare to be submitted concurrently duly digitally signed in the website **https://wbtenders.gov.in**

3. Tender documents may be downloaded from website and submission of Techno Commercial Bid and Financial Bid will be done as per Time Schedule stated in Section – D of this Tender Document.

4. The Financial Bid of the prospective Bidder will be considered only if the Techno Commercial Bid of the bidder is found qualified by the Tender Committee. The decision of the 'Tender Committee' will be final and absolute in this respect. The list of Qualified Bidders will be displayed in the website.

Table of Contents

CONTENTS OF THE TENDER DOCUMENT

The Tender document comprises of the following:

SECTION – A

SCOPE OF WORK

Job title: "Revamping & Physical Expansion of West Bengal State Data Center"

1. Executive Summary:

1.1. Project Background:

West Bengal State Data Center was established in 2010 by Government of West Bengal for on-premise hosting and managing e-Governance Applications of the State Government under National e-Governance Plan (NeGP) of the Government of India.

The existing Data Center of 3500 Sq ft was built seven years back to facilitate Central Government's NeGP initiatives by on-premise hosting of Government. Applications at State Data Center (SDC). Several Applications have already been hosted at SDC , 26 nos under a Cloud and another 18 numbers Collocated. Separate remote Data Recovery services have been provisioned at National Data Center, Shastri Park, New Delhi through storage based replication of data with a provision of future Disaster Recovery (DR)-Compute for Applications hosted with SDC-cloud only and Host-based DR full Services for the Collocated Applications at the NDC-end.

West Bengal State Data Center (WBSDC) has been developed by the State of West Bengal, which is envisioned as the 'Shared, reliable and secure infrastructure services center for hosting and managing the e-Governance Applications of State and its constituent departments' and the same has been developed as a part of Mission Mode Project under National e-Governance Plan (NeGP) and to ensure adherence to common principles and policies towards realization of the vision.

Department of Information Technology and Electronics, Government of West Bengal (DIT&E, GoWB) was the key and core stakeholder of implementation of various Mission Mode Projects under NeGP and West Bengal Electronics Industry Development. Corporation. Ltd (WEBEL) has been identified as the State Implementing Agency (SIA) towards the support of such implementation. A Composite Team has been formed with the officers from WEBEL and National Informatics Center (NIC) for shouldering the responsibility of techno-administrative support of overall SDC operations, management and hosting various departmental applications at SDC.

Now, Webel Technology Limited, earlier a subsidiary of West Bengal Electronics Industry Development Corporation Limited will execute the work related to e- Governance activities as Nodal Agency, as per decision of the State Government through the change of rules of Business. Webel Technology Limited has now become separate entity under the administrative control of Department of Personnel and Administrative Reforms and E-Governance, Government of West Bengal. Accordingly WB State Data Centeractivities are now to be taken care of by Department of Personnel and Administrative Reforms and e- Governance, Government of West Bengal with Webel Technology Limited as the Nodal Agency. Webel Technology Limited is authorized as both State Nodal

Agency (SNA) and State Implementing Agency (SIA) for all e- Governance related activities in place of M/S West Bengal Electronics Industry Development Corporation Limited.

State Data Center would provide much functionality and some of the key functionalities are Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration. Setting up of State Data Center was one of the key Initiatives under NeGP Scheme. DeitY proposed to set up State Data Center for the States to host services, applications and infrastructure and to provide efficient electronic delivery of G2G, G2B and G2C services.

Since the State Data Center has already completed 6 ½ years of operation, most of the compute is utilized and would require upgradation. The technology used in the current Data Center is 7 years old and would require refresh to keep up to date for security reasons and as per industry standards.

Currently almost all items of the existing SDC has gone obsolete and was declared out of support by the respective Original Equipment Manufacturers (OEM) and the devices are in very critical condition. In view of the above immediate replacement of the obsolete items is extremely important for smooth operation of WBSDC , part of which have been taken care in the DPR. The Data Center is currently facing a huge demand from the State User departments for hosting their applications.
In view of the above, it was decided to comprehensively develop an all new Data center in the 2nd Floor of Moni Bhandar Building, Webel Bhavan, Salt Lake, Kolkata. The area of the proposed data center is 5000 Sq.Ft. approximately and it will have an integration with the existing Data Center.

1.2. Key highlights of the Proposed Data Center: -

- The proposed Data Center area is approximately 5000 sq. ft. (2nd floor) & as well as utilization of expansion area in the 1st floor of 1100 Sq.ft for setting up LT panel/DG sync Panel/UPS/Battery backup (redundancy in LT panel).
- Total Racks provisioned in the Data Center is 76 Racks in Phase 01, Phase 02 & Phase 03 out of which 42 will be utilized in phase 01 & Phase 02 as per current Plan. The rest has been provisioned for future expansion.
- Provisioning of Electric feed (Grid Power) from different sub-stations is preferred subject to availability to connect Grid Power to separate LT panel.
- Redundant new LT panel at the SDC end has been provisioned in the DPR which will be utilized as the main LT panel for the current scenario instead of existing LT panel/DG sync Panel. Currently existing LT panel/DG sync Panel has gone obsolete and was declared out of support by the respective Original Equipment Manufacturers (OEM) and the devices are in very critical condition. In view of the above immediate replacement of the obsolete items are utmost necessities for smooth operation of WBSDC.
- All Non-IT and IT equipment will be installed to operate in N+1 mode to maintain redundancy
- Cold Aisle containment will be used for better power efficiency.
- Precision AC will be used for server farm area and cooling for auxiliary areas will be maintained by using comfort ACs.
- DDoS, Next Generation Firewall with IPS, WAF and End-Point-Protection etc. are used to protect the network and data from any vulnerabilities and threats.
- An implementation vendor for design, supply, installation and commissioning of Data Center as per specified requirements would be selected through open tendering process. It is estimated that it will require approximately 25 weeks to complete the Data Center implementation and migration followed by 5 years of operations and maintenance support for the Data Center.

1.3. Scope of Work

1.3.1. Business Case

Build the 2nd Floor of the existing building comprising of 5000 Sq.ft and 1100 Sq.ft in the 1st Floor of the existing building. The space will be utilized for expansion of the West Bengal State Data Center.

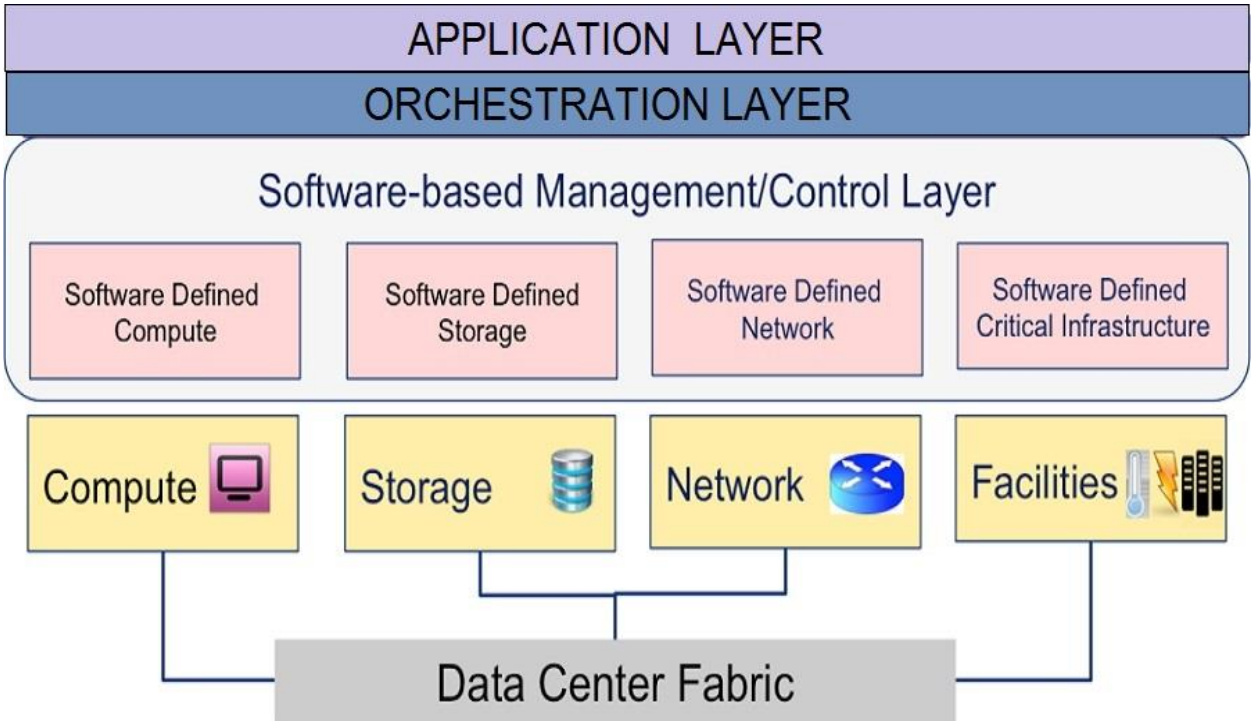
1.3.2. Goal

Create a hosting space to meet the demand of the user departments for hosting their applications in the State Data Center. Also to create a highly secure flexible, automated , managed cloud service environment deploying the latest industry computing infrastructure for keeping the user department applications secure , highly scalable and available.

1.3.3. Desirable capabilities of Software Defined Cloud Enabled Data-center –

i. Unified life cycle management for the overall cloud solution with enterprise class support.
ii. Future proof to adopt technology changes and innovation.
iii. Open Standards and Open Source based private cloud landscape.
iv. Should have a capability to manage cross platform virtualization with cloud management platform.
v. OpenStack/Open Source based framework for the complete cloud deployment.
vi. Complete agent-less automation with life cycle management.
vii. Single and Unified run-time environment.
viii. The solution should able to scale to PaaS and SaaS if desired.
ix. It should have capability to manage hybrid cloud environment.
x. It should support generic x86 environment and leading hardware OEM'
xi. Data Driven & Ready for the unpredictable
xii. Ready for DevOps & Application Lifecycle Management

Broad Architecture of Cloud Enabled Data Center:



1.3.4. Brief Scope of Work:

i. Build the entire 5000 Sq.ft area in the 2nd Floor of the existing building comprising Civil, Electrical & Flooring works

ii. Build the 1100 Sq.ft in the 1st Floor of the existing building which will be utilized for the expansion of Electrical & UPS Room

iii. Replacement of all the obsolete and End-of-Life (EOL)/End-of-Support (EOS) IT equipment, Non-IT Infrastructure.

iv. Establish a highly scalable , secure, managed and outsourced Cloud infrastructure with stringent SLAs for near 100% availability and excellent quality of services

v. Fully Orchestrated, Cloud enabledThreat Protected, Security Compliant and automated data center with possible inclusion of Hyper converged System.

vi. Managed Virtualized Storage with dynamic thin provisioning.

vii. Monitored, Multi SLA Managed with integrated dashboard for entire IT and non-IT systems as best as suitable.

viii. The expansion of IT equipment's will be done based on demand from the State department users

ix. Deploy a SDN/NFV ready environment for connectivity of computing, security and service delivery equipment.

x. As per the Proposed Architecture, there is capacity space for 76 Racks in the expansion area in the 2nd Floor of the existing building, but currently 42 Racks will be deployed to cater the current demand.

Currently 28 racks will be procured and the rest 14 will get moved from the current DC with the migration of applications. The rest will be procured based on requirement.

xi. The Infrastructure in the 1st Floor will be migrated to the 2nd Floor

xii. The space in the 1st Floor will be utilised for general purpose

xiii. The expansion in the 2nd floor will consist of advanced security features like Firewall with IPS, Web access firewall, URL filter & Server security Solution to mitigate all the possible threats to the applications & Infrastructure of the State Data Center

xiv. All applications to be hosted in the State Data Center will undergo VA/PT testing before being deployed in the State Data Center

xv. The entire Data Center will be designed, built and will be operated by the Data Center Operator with Facility Management Services for period of 5 years.

xvi. Application Support, management ,enhancement , cloud enablement will be the responsibility of the Application owners (User Department)

xvii. Complete Implementation of the following systems:

- CCTV Surveillance
- Access control system
- BMS Controller
- VESDA System
- Water leak detection system
- Fire Suppression System
- Fire Detection system
- Rodent Repellent System
- Public Address System
- Fire Proof Enclosure for Media Storage
- Common Alarm System

1.3.5. Revamping Strategy and Roadmap

The 2nd Floor of the State Data Center building is currently having vacant space of approximately 5000 Sq. ft. The design approach incorporates the current space requirements and also keeps provision for accommodating additional racks space to cater to future possible expansion. The 2nd Floor of Moni Bhandar is proposed for expansion of the State Data Center and in phases . Computing equipment procurement will be phased out as per future demand and requirements of the User Departments . However the Civil and Electrical system works will be carried for the entire 2nd Floor in the building.

Since the expansion will take place in the 2nd Floor of the Data Center building, there will be a network connection from 1st floor of the building to the second Floor of the building. When the advanced infrastructure in the 2nd floor is ready , equipment with their corresponding applications will be migrated from the existing 1st floor Data Center to the new floor. Till the entire migration process is complete there has to be network connectivity between the two floors. Subsequently, the space in the 1st Floor will be used for two sets of power systems (UPS , Battery, LT Panel etc) and the rest of the space released for other general purposes.

- Phase 01: 28 racks will be deployed in Phase 1 in the 2nd floor. However the complete Civil and electrical works has to be carried out in entire 2nd floor. The compute and other equipment will be unpacked and cleaned up in the staging area and then brought in the DC Phase 01 core space.
- Phase 02: In Phase 02, 14 Racks will be shifted from the existing DC to the 2nd floor .The rest of the racks will be procured based on demand requirement from the State User Department.
- Phase 03: This phase can accommodate and additional 20 racks . This is kept vacant for future expansion requirements . Currently this space will be used as a Conference room.

Precision AC , UPS , Network equipment , Compute infrastructure for Phase 03 would be purchased only when the demand from User Departments exceeds that provided in Phase01 and 02 .With this approach, the CAPEX will come down and items will be procured based on the demand and requirements.

As per the understanding and detail analysis, proposal for future services in the Data Center will be as follows-

The major offerings to the various Government Departments would be in the form of a Private Government cloud running one or multiple of the established Hypervisors. Virtual machine licenses will be given to user departments who would be ready to bear the additional cost.

Some large customers , who would demand a large Computing environment and would have large user base with a lot of I/O and networking requirements will be provided Virtualized Machine(s) or Physical Machines on Convergent or Hyper Convergent platforms. This infrastructure cost has to be borne by the user departments themselves.

The existing discrete Server and storage infrastructure today will be gradually moved into Cloud as and when the same becomes End-of-Life and End -of Support.

The network would gradually move to Software defined Networking with Leaf and Spine architecture which would give better utilization of the switching fabric. The network aggregation layers will have having 40 Gb bandwidth, and the rest will be on a 10 Gb backbone.

Security appliances should be deployed to provide Advanced Persistent Threat, Defense in depth, Malware and Hack Prevention.

2. Detailed Scope of Work

The overall responsibilityof the successful bidder shall be to/for

- Expansion of the West Bengal State Data Center in the 2nd Floor of the existing building.
- Design, Procure, Install, integrate and Commission the proposed expansion of the Non IT and IT Infrastructure for the West Bengal State Data Center.
- Assist and conduct the Final Acceptance test as planned jointly with the PMU and Composite Team. The FAT will be conducted for the items to be supplied, installed, configured and commissioned by the bidder.
- Migration of Servers and other necessary items based on business requirement with minimal downtime as possible.
- Facilitate the migration of Applications with necessary infrastructure to be hosted as responsibility of migration of application will be with user department. The migration from 1st Floor to the 2nd Floor is to be included in the entire scope of work. No separate cost will be part of the financial bid .
- Take the necessary transition/handover from the existing DCO under the guidance of the competent authority prior to 3 months to the expiry of the contract in May 2018**
- Take over the Operations and maintenance from the existing DCO for the 1st Floor. The transition from existing DCO can be carried out in parallel run for a period not less than 3 months .On successful FAT, or on 17th May 2018 , whichever is earlier Operations and maintenance will start for the selected bidder under this new contract

**Note: The Current Data Center Operator is responsible for Operation and maintenance of the existing Data Center in the 1st Floor of the Mani Bhandar building. The contract for Operation and maintenance of the existing DCO expires on 16thMay 2018

Details of transition and knowledge transfer :

Starting 3 months prior to the expiry of the contract, the selected bidder will take necessary knowledge transfer from the existing DCO and will provide operation and maintenance support until the entire infrastructure of the 1st Floor is shifted to the 2nd Floor of the existing building. The cost incurred in the Transition period will be inclusive of the Data Center Implementation cost. The selected bidder should plan for the migration period with minimum downtime. The bidder shall add additional components as would be necessarily required to meet the requirement given in the SLA. The service provider has to provide the complete solution to the Government and fill all the gaps of the existing system and which are not covered in this RFP. Bidders are requested to read through carefully the entire tender document prior to responding to the tender.

The bidder should upgrade the Operating system and other software licenses which are already under support till May 2017 to their latest versions at or before the migration of the systems.

Government of West Bengal proposes to select a Systems Integrator (SI), who will build the proposed expansion area and thereafter take over for operation & maintenance/ FMS support for a period of 5 years, extendable to another 2 years with 10% cost escalation per year after 5 years. However, WTL will have their own discretion for

handover of the expansion area of the State data center to existing DCO and in such case, the 5 years O&M/ FMS period will not be entrusted to the selected SI.

The project execution period will be within 25 weeks from the date of signing of contract. This agency will provide services to the State departments who will utilize the data center.

The minimum specified work to be undertaken by the Bidder for setting up and operating WBSDC has been categorized as follows:

Schedule I: Design, Supply, Installation, Integration and Commissioning Phase
Schedule II: Operation & Maintenance phase

Note: The Bidders are requested to submit the Schedule I in the same bid which would be combined for evaluation purposes.

2.1. Schedule – I: Design, Supply, Installation, integration and Commissioning Phase

The Successful Bidder should undertake a complete infrastructure life cycle management for providing the rack space services. This would include:

1) Analyze
2) Design
3) Procure
4) Implement

2.1.1. Schedule I- Analyze

i. Site analysis and requirement

Bidders should analyze the site requirement, its present status, the applications hosting plan, the existing infrastructure and any other relevant details before designing the data center and quoting prices.

ii. Site survey and site preparation report

Bidders will be responsible for site survey to identify the exact situation of the site and then for ensuring site readiness for the implementation of the data center infrastructure. Bidder will submit a detailed site survey report.

2.1.2. Schedule I- Design

The selected Bidder shall implement the Data Center in line with minimum requirements as laid out in TIA 942 specifications for Tier III for Power, Cooling Infrastructure & Security Infrastructure and Tier II for rest of the Data center wherever possible. The implementation should ensure an uptime of 99.749% on a quarterly basis. The broad scope of work during this phase will include the following (but is not limited to):

a. Design of the Expansion Server Area in the Center in line with the following requirements

- A Service Aisle should be provided for maintenance of all cooling and power equipment.
- The Racks should be arranged with the provisioning of cold Aisle Containment.

- The proposed solution should accommodate a minimum of 42 racks of Size 750-800mm*1070-1100mm*42U
- All Power and Data Cabling should be in appropriate cable trays and routed as per EIA/TIA 586 A&B Standards
- Implementation of Physical Infrastructure comprising of Civil, Electrical & Mechanical works required for the expansion.
- Tentative layout is in the RFP. Bidder to visit the existing Data Center, asses the design and propose their solution in line to the tentative layout
- The site needs to be assessed by the bidder and accordingly the SLD has to be prepared by the bidder
- Bidders are requested to visit the existing Data Center to understand the existing equipment's.
- The Scope of DCO is only the migration and management of the Infrastructure and also provides facilitation to the Application owner. Application will be migrated by individual application owner.
- Migration of the Physical Infrastructure is in the scope of the bidder
- The insurance of the existing items is not in the scope of the bidder
- Provisioning of additional electrical LT Panel, UPS, Battery, DG Sync Panels along with cabling from Transformer, DG along with necessary cable trays, trenches, and intelligent circuit breakers in the 1st floor North vacant space.
- Provisioning of entry to Data Center from North Side left staircase through a Security check consisting of Door frame metal detector with provision for X-ray luggage checker, Visitor Management System and Dual HID, Biometric Access System, CCTV Monitoring with visitors waiting space.
- Provisioning of necessary furniture for NOC, SOC and LED lighting arrangements with network infrastructure and provision of Wi-Fi for guest internet access.
- Implementation of Networking & Security Infrastructure and other associated IT Components in the Data Center
- Data Backup, replication, monitoring, assistance to TPA in vulnerability assessment and penetration testing of all infrastructure and applications, mitigation of vulnerability of all infrastructures under SI and user departments.

Some of the key considerations for designing the SDC are given below:

i. Design validation and change

The SI shall prepare detailed deployment design document (both physical and IT) and shall submit the same for approval within 2 weeks from the signing of the contract Agreement with the SIA. However a Solution design has to be provided during the bid process. While preparing the design the Successful Bidder shall keep in mind the existing DC set up in the 1st Floor, scalability requirements and shall plan for less downtime during the implementation.

ii. Structural Soundness to be re-validated

SIA is responsible to undertake site strengthening of the proposed State Data Center. SI will confirm from SIA regarding the details of structural loads.

iii. To finalize Site Layouts and submit Working Diagrams

The site layout as given in the RFP shall be mutually agreed between the SIA and the SI. Subsequently the SI shall refer to the existing layout diagram and could submit the diagrams annexed with the Data Center expansion project. For these purposes the SI shall provide the services of a practicing Architect and all the drawings shall be signed by this architect. The architect would be required to provide his registration number as well and also sign any documents which may be required for legal compliance for the changes that would be undertaken in the building.

a. Basic Layout taking the Data Center set up in the 5000 Sq. ft. approx. area in the 2nd Floor of the building.
b. Layout 2500 Sq. ft. approx. adjacent to the Data Center expansion space
c. 1000 Sq. ft. approx. space for Electrical Infrastructure setup in the 1st Floor
d. Access Control system Layout in the expansion area
e. False Flooring Area of Approximately 3200 Sq. ft. approximate area
f. Cold Aisle Containers
g. Electrical layout (Including PAC and other requirements)
h. Lighting Layout
i. Loose furniture details
j. Fixed furniture details
k. Civil addition and alteration details
l. Internal/ sectional elevation
m. Cabling Layout
n. CCTV Layout
o. Rodent Repellent Layout
p. Fire Extinguisher Layout (including manual switches)
q. Water Leak Detection System layout
r. Other drawings as required by the State

2.1.3. Schedule I-Procure

The SI shall procure the materials and equipment as required and given as part of the SI's response. However, it should be noted that the SI is expected to procure all necessary equipment to install the requirement in the proposed expansion set up. In case, it is identified that certain components are required for required functionality but not included in the Tender BOQ , SI should include such equipment in the bid value , quote for them as "others" including a list for the same with individual item description, unit cost . SI shall procure the same free of cost for the Government. The SI shall note that the specification provided is the minimum requirement and the SI shall procure better equipment if it is required to meet the service levels mentioned the section on SLAs

The SI shall procure and supply all components and sub components (Active as well as passive), as per requirements of the RFP/Contract. The SI shall be responsible for supply/ installation of:

- All active and passive components required for the expansion area of server farm of West Bengal State Data Center

- Physical infrastructure components such as UPS and Air-Conditioning System, Lighting system, UPS power (to draw from WB EB raw power), CCTV Surveillance systems, and Network Cabling etc.
- IT Infrastructure components such as Storage, Networking & Security components and other IT components required at the Data Center
- All Products supplied under the RFP should not reach end of support before 7 years from the date of FAT or start of O & M services
- All the IT / non IT products quoted should be supported by the SI for next 5 years from the start date of O & M services. The SI should also commit support for another 2 years if necessary.

All the software's used for providing data center services shall be licensed to WTL and will be the property of WTL. The SI shall be responsible for end-to-end implementation and shall quote and provide/supply any items not included in the bill of material but required for commissioning of the cloud, network, Non-IT equipment like PAC, UPS, BMS, EMS, Infrastructure Monitoring, including any Compute equipment. WTL shall not pay for any such items, which have not been quoted by the SI in the bid but are required for successful completion of the project.

The SI will be responsible for delivering the equipment at the data center site. The SI shall supply all the installation material/ accessories/ consumables (e.g. screws, clamps, fasteners, ties anchors, supports, grounding strips, wires etc.) necessary for the installation of the systems.

The SI has to prepare and submit a delivery report including details of all components supplied. The delivery report will be validated by the SIA.

Any additional equipment procured by SI, will be supplied by the respective OEM. The Bidder would be responsible for inventory check, testing and installation of the equipment accordingly and coordinating with the supplier as required.

2.1.4. Schedule I-Implement

Bidders shall provide a complete data center solution to SIA as a part of their technical bid. Any activity not mentioned here but required for the implementation of data center shall be taken in note. The solution provided by the Successful Bidder shall meet all the service level requirements. While the basic bill of material will not change, any change in the basic BOM will be done in consultation with the SIA. It is recommended that the SI should thoroughly go through the RFP, to adhere to the service levels as mentioned in the document.

2.1.4.1.Site Strengthening

Selected Bidder shall arrange for necessary clearances which shall enable them to undertake civil, electrical, and mechanical works including false ceiling, partitioning, installation of electrical component, cable laying etc. at the 8000 Sq. ft. expansion of the State Data Center in the 2nd Floor and 1000 Sq. ft. of approximate space in the 1st Floor of the existing Data Center building. The SIA shall support and facilitate the SI in obtaining the clearances.

The Bidders are free to inspect the site prior to submitting their proposals. In case of non-conformance due to the unavoidable building constraints the State and the SI shall agree mutually on alternate arrangements.

2.1.4.2. Supply, Installation, Integration and Commissioning of Non IT Components

The selected Bidder shall procure and supply all Non IT components. The selected Bidder would be required to undertake all the necessary civil, electrical, plumbing and mechanical works including false ceiling/flooring, partitioning, installation of electrical component, cable laying etc. and other infrastructure or services to create the Non- IT / Physical infrastructure.

Installation shall mean to install and configure / integrate every component and subsystem component, required for functioning of the State Data Center.

Based on generic solution design, minimum capacities and specifications for the components have been worked out and described later in this RFP. However, these are only bare minimum requirements and the Bidder is at liberty to suggest better solutions to meet the overall SLA requirements.

2.1.4.3. Supply, Installation, Integration and Commissioning of IT Components

Successful bidder will be expected to bring all the installation equipment's and tools required for the installation of the system. The Successful Bidder shall install, integrate and commission the active network equipment as well as passive network components (Cabling etc.) as per approved deployment design. All the work shall be done in a conscientious manner as per the OEM guidelines and best industry practices. The system shall be subjected to inspection at various stages. Local regulation / codes shall be followed at all times. The Successful Bidder shall follow all Safety Regulations and practices.

The Successful Bidder shall not cause any damage to the existing server farm of WBSDC, Government buildings /other premises and property and will perform restoration if any damage occurs. Trenches, path-cutting, etc. will be back-filled and restored to the original condition immediately after laying of the conduit/cable. The Successful bidder shall plug conduits and entrance holes where the cabling has been installed with suitable sealing material.

2.1.4.4. Acceptance Testing and Commissioning

The SIA shall review the detailed acceptance test plan (FAT) in consultation with the consultant/PMU after taking in to account any comments / suggestions of the stakeholders. State Consultant/PMU will define parameter for testing.

a) The acceptance Testing would include the following
   - Acceptance Testing to ensure that all functions as per requirements, approved designs, hardware equipment and software deployed are of the exact specifications given in the RFP and operates seamlessly in the SDC infrastructure in terms of performance, reliability, security and meets ANSI TIA-942 standards for cooling, Power, Network and Security Infrastructure. The respective OEM must certify the installation of their products in the OEM letter head that the installation has been done as per the standard best practices and for any shortcomings/ defect/ malfunction found in the installation during warranty period will be taken care by the OEM.

b) The technical tasks to be carried out shall be as follows:

- All the functionality of the Software installed by the SI will be checked during Final Acceptance Test.
- Functional Testing: Ensuring that the application functionality as described works adequately in the State Data Center environment. The functional testing of application will necessarily be minimal as this is a core responsibility of the department
- Performance Testing: Ensuring that the application meets expressed performance requirements on the State Data Center equipment by using performance test tools and performance monitoring tools
- Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

The SIA would also conduct audit of the process, plan and results of the Acceptance Test carried out by the System Integrator. The SIA would issue certification of completion for which WTL shall verify availability of all the defined services as per the contract signed between the SI and SIA. The SI shall be required to demonstrate all the services / features / functionalities as mentioned in the agreement.

Commissioning shall involve the completion of the WBSDC site preparation, supply and installation of the required components and making the Data Center available to the SIA for carrying out live Operations and getting the acceptance of the same from the SIA. Testing and Commissioning shall be carried out before the commencement of Operations.

2.1.4.5. Final Acceptance Testing

The final acceptance shall cover 100% of the expansion area scope in West Bengal State Date Center, after successful testing by the SIA or its third party monitoring agency; a Final Acceptance Test Certificate (FAT) shall be issued by the SIA to the SI. The date on which Final FAT certificate is issued shall be deemed to be the date of successful commissioning of the expansion of WBSDC and thereafter the Operation and Maintenance will start from the next date.

Prerequisite for Carrying out FAT activity:

- Detailed test plan shall be defined by the SIA. This shall be submitted by SI before FAT activity to be carried out.
- All documentation related to WBSDC and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the Final Acceptance Test to the client (SIA)

The training requirements as mentioned should be completed before the final acceptance test.

For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the WBSDC supplied components

- **Final Acceptance shall include the following:**
- OEM certification of all the components installed.
- All hardware and software items must be installed at WBSDC site as per the specification.
- Availability of all the defined services shall be verified.

- The SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
- The SI will arrange the test equipment required for performance verification. Successful Bidder will also provide documented test results.
- The SI shall be responsible for the security audit of the network to be carried out by a certified agency other than the successful Bidder.
- SI needs to ensure that all such applications, systems & infrastructure meet the basic standards. This would be also required for compliance purposes such as ISO/IEC 27001:2013, ISO/IEC 20000:2011, or as per SIA or departmental requirements.
- Any delay by the SI in the Final Acceptance Testing shall render the Bidder liable to the imposition of appropriate Penalties, up to a max of 5% of total contract value. In the event the SI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the SI and SIA may mutually agree to redefine the Network so the Bidder can complete installation and conduct the Final Acceptance Test within the specified time.

2.1.4.6. Training

The selected Bidder shall conduct training after installation and commissioning have been completed. Training will be provided by the selected Bidder from the respective OEMs or OEM authorize partners or certified resources to the officials of IT, SIA (West Bengal Electronics Industry Development Corporation Limited), SI and other Departments, for a maximum of 15-20 people to be identified by the SIA, in a phased manner at the expansion SDC premises by the State Government. Non IT training would include training on operation of Precision AC, UPS Systems, electrical systems, BMS systems like access control, fire detection and suppression system, security aspects of the Data Center, education on how the passive network cabling has been done on the overall expansion area build etc.

2.1.4.7. Documentation

Provide documentation, which follows the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation.

Indicative list of documents include:

- Project Commencement: Project Plan in MS Project or equivalent giving out micro level activities with milestones & deadlines
- Delivery of Material: Original Manuals from OEMs.
- Training: Training Material will be provided which will include the presentations used for trainings and also the required relevant documents for the topics being covered.
- Process Documentation: The Bidder shall be responsible for preparing process documentation related to the implementation of each and every component of the expansion server farm area in SDC. The prepared process document shall be formally signed-off by SIA before completion of final acceptance test.

a. The selected Bidder shall document all the installation and commissioning procedures and provide the same to the West Bengal Electronics Industry Development Corporation Limited / Government of West Bengal within one week of the commissioning of SDC.
b. The Selected Bidder shall submit a complete set of Floor Layout Drawings, BMS components, Single Line diagram, a complete cabling system layout (as installed), including cable routing, telecommunication closets and telecommunication outlet/ connector designations. The layout shall detail locations of all components and indicate all wiring pathways.
c. Manuals for configuring cloud platform, servers, switches, routers, and their current setting shall be provided by the selected Bidder.

The SI will prepare the SOP, ISMS Policy through active participation of the Consultant/CT and will be handed over to the DCO. The DCO will operate the Data Center in line to the Policy and process defined by the Consultant/CT and will be also compliant to latest version of ITIL and audited for both process and implementation compliance by auditors every six months.

The selected Bidder shall be responsible for documenting configuration of all devices and keeping backup of all configuration files, so as to enable quick recovery in case of failure of devices. Documentation should be provided by the selected Bidder on a regular basis as and when desired by the SIA.

2.1.4.8. Key Considerations

Some of the key considerations for designing the SDC have been covered in the following:

a. Scalability

All components of the West Bengal State Data Center (WBSDC) must support scalability to provide continuous growth to meet the requirements and demands of various departments. A scalable system is one that can handle increasing numbers of demands and requests without adversely affecting the response time and throughput of the system. The WBSDC should support both vertical (the growth of computational power within one operating environment) and horizontal scalability (leveraging multiple systems to work together on a common problem in parallel). Modular design of the Data Center is an excellent strategy to address growth without major disruptions. A scalable SDC shall easily be expanded or upgraded on demand. Scalability is important because new computing component is constantly being deployed, either to replace legacy component or to support new missions.

b. Availability

All the components of the WBSDC must provide adequate redundancy to ensure availability of the e-Governance applications and the Data Center services. Designing for availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.

c. Interoperability

The entire system/subsystem should be interoperable, in order to support information flow and integration. Operating systems, database and storage technologies from several vendors must interact well with each other. These systems should support the open architecture solutions such as XML, LDAP, SOAP, etc. where information/data can be ported to any system, whenever desired.

d. Security

The WBSDC shall be designed for an end-to-end security blanket to protect applications, services, data and the infrastructure from malicious attacks or theft from external (through internet) and internal (through intranet) hackers. Using Firewalls and Intrusion detection systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worms attacks should be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. WBSDC should be designed to make use of the SSL / VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. SI should be responsible for prevention, alert, mitigation requirements of all Cyber-attacks. The security products quoted should ensure that WBSDC is protected from DDoS layer 4 and 7 attacks. Antimalware, Malicious content infiltration, ransomware attacks, and virus attacks at the host and endpoints.

The SDC layout should be divided into domains such as:

- Trusted Zone –is the secure zone which has a restricted access. This zone will mainly host storage, database and management servers which are not directly accessible to the outside zone. The trusted zone is separated using strong access control and a firewall, which provides an additional level of security to the infrastructure.
- De-militarized Zone – (DMZ) would be a "neutral zone" between SDC's internal network and the outside extranet network. It would prevent extranet users from getting direct access to the servers. In other words, this is a small network that lies between a trusted internal network (SDC LAN), and an un-trusted external network (such as the public Internet). Mostly the DMZ contains devices accessible to Internet traffic, such as Web, FTP, SMTP and DNS servers.

e. Manageability

The SDC must be designed in an efficient way to ensure an ease in maintenance. It must facilitate ease of configuration, ongoing health monitoring, and failure detection that are vital to the goals of scalability, availability, and security. The SDC shall be designed to match the growth of the environment including IT Infrastructure, Government data & information etc.

f. Integration of SDC with SWAN

Another most important aspect which should be taken care while designing the SDC is about seamless integration with SWAN. Provisioning of connectivity between the SDC and SWAN shall be the responsibility of WTL such as laying of OFC, Cabling, etc. However the SI should be responsible for integrating SWAN link from the existing Data Center to newly built Data Center. Planning of terminating SWAN link should at gateway level of the Data Center.

g. IPv6

All the hardware and software (including but not limited to all the routers, switches, firewall, servers, and operating systems) supplied under this tender shall be IPv6 ready from day one. The performance as specified in the specification of each component in the RFP is for IPv6. These components should also be ready to work on IPv4 whenever required. The entire infrastructure should be configured & operational in IPv6 & IPv4 from day one

i.e. in Dual Stack mode. In future, for migrated infrastructure in new DC, IPv6 shall be implemented in dual stack mode.

h. Cloud Services

The proposed Cloud solution should be capable of providing Infrastructure-as-a-Service and Platform-as-a-Service to various line departments within the State (Private Cloud). The detailed specifications of the Cloud is included in the section n on Specification and Compliance requirements.

The selected bidder will be responsible to take a transition of existing cloud solution from the existing Cloud service provider and will provide O&M support on co-ordination with the Cloud service provider. The selected bidder will also be responsible for migrating the existing cloud setup to the new Data Center and integration will be made with the new cloud solution in the Data Center which is proposed to be there. SI will co-ordinate with the cloud service providers (current and new) for migration and integration of existing cloud services and also will be responsible to monitor and manage the new cloud services which will be implemented in new Data Center.

i. DR Integration

The WBSDC is currently integrated with the National DR. The DR site for WBSDC has is at the NIC DC at Shastri Park, New Delhi. The replication is essentially a storage/host based replication from DC to DR. Backend storage has been provided by NIC at the DR site. Additionally, in future SIA shall procure other components including compute and cloud resources as required to setup the DR for existing cloud solution; Application level business continuity planning will also be required to be done by the SI. Testing of DR Management, integration, technical support and O&M of this infrastructure shall be done by the selected bidder for the entire project duration at no additional cost.

j. NIC Services & infrastructure in NDCs

Storage of 25TB at NDC for WBSDC has been provisioned currently and any future Storage and Compute requirements would be worked out between NIC and the State. NDC services, namely Physical space, Core infrastructure and services, Manpower, and Policy, Process & Guidelines support to the State would be provided for an effective DR support. Selected bidder needs to co-ordinate with NIC on behalf of the State to get the available support from NIC as required.

2.2. Schedule- II: Operation and Maintenance Phase

Operation and Management Phase for the WBSDC expansion is planned with 5 years from the date of commissioning /FAT or 18th May 2023, whichever is Later .

The scope of work for the Operations phase can be categorized under two service categories as depicted as Basic Infrastructure Services and Managed Services. Basic Infrastructure Services are mandatory services to be provided by the selected bidder to ensure seamless WBSDC operations. User shall have an option to choose among the services listed under the Managed Services as per their specific requirements.

2.1.5. Pre-requisites for the Services

- The selected bidder and SIA should agree upon the contractual period & service levels for providing the necessary services.
- Servers, necessary OS & other software, Database Licenses and other infrastructure over and above the BoM provided in the RFP, necessary for hosting future application(s) would be provided by SIA and should be supported by the OEM as a part of this contract without any incremental addition to the O & M Costs.
- For Applications added in future , including Servers, storage, networking equipment, software and related Operations jobs , there would be no incremental payment made to the SI in the next 5 years

i) Basic Infrastructure Services

Following services shall be provided by the SIA under the basic infrastructure services:

- Ensure availability of the WBSDC infrastructure (both Non-IT and IT) including but not limited to Power, Cooling, CCTV, Access Control, VESDA, Racks, Network and Security devices, Servers, Storage, and other peripheral equipment installed in WBSDC (existing and new).
- Provision the cloud/physical/virtual environment for the user departments of GoWB to host their application infrastructure (application, databases, etc.)
- Facilitate hosting of applications by user departments of GoWB at the WBSDC:
    - Provide virtual platform (P2V migration) / provide rack space and physical servers (P2P migration) for hosting of applications.
    - Maintain the infrastructure use for hosting of applications inside WBSDC.
    - Provide development, testing / staging infrastructure as required for developing and testing the application before hosting in production environment.
    - Selected bidder will be responsible for ensuring VA and PT of servers or applications before hosting in WBSDC followed by regular VA and PT on half-yearly basis for all IT infrastructure and applications.
    - Ensure availability of other peripheral infrastructure such as CCTV, VESDA, WLD, Access control,Physical security systems, Fire detection, suppression systems, etc., as a part of Intelligent Building Management Systems (IBMS) to maintain the infrastructure.

- Provide intranet and/or internet connectivity for accessibility of applications hosted inside WBSDC.
- Provide adequate storage and on demand provisioning of storage by creating and managing LUNs.
- Provide shared Data Base services and L1 level Database fault reporting required for applications.
- Ensure physical and logical security of infrastructure services provided by SIA.

- Provide access to its hosted infrastructure in WBSDC through secure, two factor authenticated mechanism, with all privileged activity logged for future reference.
- Proactive and reactive maintenance, repair and replacement of defective components (physical and other peripheral IT infrastructure) installed at the Data Center. The cost for repair and replacement shall be borne by the SI. There should be an agreement between the SI and the OEM, a copy of which has to be given to the SIA.
- Proactive monitoring of the entire basic infrastructure installed at the WBSDC through and Integrated BMS.
- Regular Service reporting.
- Provide access card activation service for access to the server farm area in consultation with SIA.
- Any component (Physical & IT installed at the time of WBSDC commissioning) 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).
- Proactive monitoring of the entire basic infrastructure installed at the WBSDC through building management system and EMS
- SI shall maintain records of the maintenance of the basic infrastructure and shall maintain a logbook on-site that may be inspected by the SIA at any time.

ii) Network Monitoring Services

The activities shall include:

- SI shall provide services for management of WBSDC network environment to maintain performance at optimum levels on a 24 x 7 basis.
- SI shall monitor and administer the network within the WBSDC up to the integration points with WBSWAN and other WAN links.
- SI shall create and modify VLAN, assignment of ports to appropriate applications and segmentation of traffic.
- SI shall carry out break fix maintenance of the LAN cabling or maintenance work requiring civil work.

iii) Integration Testing

- Integration testing is essential to ensure that the application to be deployed does not disrupt the WBSDC operations and affect other WBSDC infrastructure in terms of performance and security. The technical tasks to be carried out shall be as follows:
- Functional Testing: Ensuring that the application functionality as described by the department works adequately on the WBSDC environment. The definition and review of the parameters for functional testing shall be the responsibility of the concerned department.
- Performance Testing: Ensuring that the application meets expressed performance requirements on the WBSDC servers by using performance test tools and performance monitoring tools. The user department should submit a test report on performance, based on which the SIA/SI will put the application in the production. The definition and review of the parameters for performance testing shall be the responsibility of the SI and the SIA respectively.
- Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure. The definition and review of the parameters for security testing shall be the responsibility of the TPA and mitigation of applications related vulnerabilities will be the responsibility of SI for infrastructure related security flaws and SIA/user departments for application related issues .

iv) Change Management

- Tracking the changes in hard / soft configurations, changes to policies, applying of upgrades / updates / patches, etc.
- Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.

v) Vendor Management Services

The activities shall include:

- Coordination with all the project stakeholders (SIA, Implementation Committee, TPA/PMU, Departmental users, Vendors, if any) to ensure that all Data Center activities are carried out in a timely manner.
- Coordination with vendors and OEMs to ensure that time and equipment dependencies are optimally managed
- SI shall coordinate and follow-up with all the relevant vendors of the SIA/User Departments to ensure that the user problems and issues are resolved in accordance with the SLAs agreed upon with them.
- SI shall also ensure that unresolved issues related to application which are affecting the SLA of SI are escalated to SIA in accordance with the escalation matrix.

- SI shall also coordinate with vendors of SIA and other user departments of SIA who would host their infrastructure at WBSDC and co-ordinate to ensure that the issues are resolved in accordance with the SLA signed between SIA and the vendor. SI shall maintain a track of SLA performance for such vendors with the help SIA/PMU/CT/TPA.
- SI shall maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.

vi) Visitor Management System

The security requirements of Data Center and infrastructure are challenging and growing increasingly. Visitors shall be screened, registered, signed in quickly and allowed to visit only the relevant areas via integration with access control areas via integration with access control devices. These challenges of the visitor management and lobby management activities are seamlessly and efficiently managed by Visitor Management System.

The activities shall include:

- Provision for storage and use of computerized photo of the visitors
- Each pass has necessary details of the visitor
- List of visitors inside the premises, whenever, required
- Extensive query support
- Duration of stay of each visitors
- Give details of all visitors visited in the past without delays
- Details of visitors vehicles like type and registration number
- Data backup facility
- Data is stored using latest compression techniques
- Data should be available as per backup policy of the SIA

vii) Installation and Configuration of Application Infrastructure

SI shall provide installation and configuration support for the application infrastructure to be hosted by SIA and any Government Department. This service shall be availed by Departments based on their specific requirements. It shall not include application deployment, tuning or any other application related work. The activities shall include:

a. SI shall undertake pre-installation planning at the Data Center including but not limited to Rack planning, structured cabling, SAN cabling, power points, etc.

b. SI shall be responsible for the commissioning of the storage, network & security components, cloud infrastructure and related basic infrastructure at the WBSDC.

c. SI shall carry out the planning and layout design for the placement of equipment in the WBSDC. 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 the WBSDC.

d. The plan and design documents thus developed shall be submitted to the SIA for approval and the acceptance would be obtained prior to commencement of installation.

viii) Network Management

The objective of this service is to ensure continuous operation and upkeep of the LAN & WAN infrastructure at the WBSDC including all active and passive components. *The scope excludes maintenance of WAN links, which shall be the responsibility of respective ISP and WBSWAN Implementation Agency. However, for overall functioning of the Data Center, the selected bidder shall be responsible to coordinate with WBSWAN or ISP team for WAN link related issues and seamless integration with WBSDC & it's operations.*

The services to be provided for Network Management include:

- Ensuring that the network is available 24x7x365 as per the prescribed SLAs
- Attending to and resolving network failures and snags
- Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches. These network equipment may be upgraded to SDN/NFV architecture in the near future.
- Configuration and backup of network devices including documentation of all configurations.
- 24x7x365 monitoring of the network to spot the problems immediately.
- Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.

ix) Physical Infrastructure Management and Maintenance Services

All the devices that will be installed in the Data Center as part of the physical infrastructure should be SNMP or MODBUS TCP/IP enabled or manageable with IBMS and shall be centrally and remotely monitored and managed on a 24 x 7 x 365 basis. Industry leading infrastructure management solution should be deployed to facilitate monitoring and management of the Data Center Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

- Proactive and reactive maintenance, repair and replacement of defective components (IT and Non-IT/ Hardware and Software). The cost for repair and replacement shall be borne by the selected bidder.
- The selected 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.
- To provide this service it is important for the bidder to have back to back arrangement with the OEMs. The bidder needs to provide a copy of the service level agreement signed with the respective OEMs at the time of bid submission.
- 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). In case the selected bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.

- 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 SIA at any time.

x) License Management

In addition to mentioned quantity of software/licenses in RFP, software/license required to run the operations and maintenance of the WBSDC will be arranged by SIA. SI shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the WBSDC. This may be carried out through the use of EMS.

2.1.6. Managed Services

SIA is having very limited resources who are currently working for managing the services of West Bengal State Data Center. Capacity building of the SIA officials will be very important for long run sustainability. So, Managed Services from SI for certain period will be required to maintain international standards and the managed services shall include a range of services related to the IT infrastructure at the Data Center. These services shall not involve any application related work except from assistance in VA/PT, Application Staging , Application security and Load testing , Final UAT .

Following services shall form a part of managed services:

2.1.6.1.Monitoring and Management Services

The SI shall provide monitoring and management services for an agreed service window during the agreed contractual period from the date of final acceptance test. The scope of the services for overall Physical and IT infrastructure management during this period shall include Support for Monitoring, Administration and Management of the entire WBSDC infrastructure, existing infrastructure (including cloud) migration and facilitating infrastructure/cloud services for application migrations. The entire stack of monitoring and management services shall include but is not limited to the following:

- Cloud Monitoring, Server Monitoring, Administration & Management Services
- Database Administration & Management Services
- Storage Administration & Management Services
- Planning existing IT infrastructure/ cloud infrastructure Migration and provides support for Application Migration

It should be noted that migration of applications to the Data Center would be the responsibility of User departments and the DCO would only facilitate the migration of application by providing basic infrastructure/cloud services.

DCO will provide the Server Space, SAN Configuration, Backup in VTL, EMS agents to be deployed in the Servers, Security agents, necessary configuration in cloud etc. All infrastructure facilitation to be provided by the DCO, Application Software will be migrated by the Application owner.

i. Server Monitoring, Administration & Management Services

The activities shall include:

- Configuration of Cloud system, Orchestration layer, monitoring and dashboard, server parameters, operating systems administration and tuning.
- Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of updates & patches to ensure that the system is properly updated.
- Re-installation in the event of system crash/failures.
- Managing and providing maintenance support to all the existing equipment in the Data Center, and migration them to the new hardware as and when appropriate. This hardware may be supplied either as a part of this RFP or can be procured by WTL as a box replacement of an existing equipment in operation.
- Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.
- Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, privilege user access etc., ensuring that the logs are backed up and truncated at regular intervals.
- Periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.
- 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.
- Identification, diagnosis and resolution of problem areas pertaining to the WBSDC infrastructure and application and maintenance of assured SLA levels.
- Implementation and maintenance of standard operating procedures for maintenance of the infrastructure based on the SIA's policies.
- Management of the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc.
- System administration activities shall include tasks including but not limited to setting up the Cloud, servers, executing hardware and software updates when necessary.
- SI shall co-ordinate with existing cloud service provider for knowledge transfer and will migrate the existing cloud infrastructure in new Data Center with the help of exiting cloud service provider.
- SI shall co-ordinate with new cloud service provider for seamless integration of existing cloud services.

- SI shall be responsible for monitoring and managing existing cloud services once the new DC is operational. The selected bidder needs to start the transition with existing cloud service provider prior to FAT as checking functionalities of cloud services will be a part of FAT activities.
- System administration activities shall include tasks including but not limited to setting up the servers, other activities shall include:
    - Configuring and apportioning storage space
    - Configuring virtual machines as request comes
    - Setting up of working e-mail accounts and mailing lists
    - Management and integration of databases
    - Implementing security on the Internet / Intranet
    - Setting up of firewalls and authorization systems
    - Performing periodic backup of data and automating reporting tasks

  Executing hardware and software updates when necessary.
- SI shall be responsible for Integration, Monitoring, Management, Operation & Maintenance support & asset management of all additional servers and devices for the purpose of Cloud enhancement, without any additional cost.
- SI shall be responsible for Integration, Monitoring, Management, asset management, vendor management and notification of Patch upgrades (for Operating system, databases and other softwares)for co-located servers and devices, which will be hosted by SIA/ Government Departments during the O&M phase without any additional cost.The scope excludes server support & maintenance, application/ database support & maintenance and installation of patch upgrades.

ii. <u>Database/ Application Administration & Management Services</u>

- L1 management of database on an ongoing basis to ensure smooth functioning of the same.
- Provide tuning inputs to the SIA/user department in order to improve the application performance or resolve bottlenecks if any.
- Performance monitoring of the databases and applications on a regular basis.
- Provide information to SIA/ User Department regardingoperating system, database and other software upgrades or patch upgrades as and when the same are available.
- Regular backups for all databases/ applications in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions.

iii. <u>Storage Administration & Management Services</u>

The activities shall include but is not limited to:

- Installation and configuration of the storage system at WBSDC. The existing storage will be required to be migrated to an additional or existing storage.
- Management of storage environment to maintain performance at desired optimum levels.

- Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.
- Configuration of SAN whenever a new application will be hosted on the WBSDC. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

iv. <u>Planning existing IT infrastructure/ cloud infrastructure Migration and provide facilitation for Application Migration</u>

The activities shall include:

- As-Is assessment of current infrastructure of existing Data Center.
- Analysis of re-usability of servers, network devices, storages etc.
- Planning and migrating existing reusable IT components in new Data Center
- Checking virtualization compatibility in co-ordination with Application owners or application development vendors
- Planning of application migration in details along with help from Application owners or application development vendors
- Support application vendors for migration of applications in cloud/virtual environment.
- Creating virtual machines and other required infrastructure for application migration.
- Make the physical platform ready if the application does not support virtualization
- Allocation of disk space, RAID configuration, installation of OS, providing network connectivity, security measures shall be taken care of by the SI under requisite approvals from the SIA/CT

It should be noted that migration of applications to the Data Center would be the responsibility of the application owner or application development vendor and the SI would only facilitate the migration of application.

DCO will provide the Server Space, SAN Configuration, Backup in VTL, EMS agents to be deployed in the Servers, Security agents, necessary configuration in cloud etc. All infrastructure facilitation to be provided by the DCO, Application Software will be migrated by the Application owner.

v. <u>Backup and Restore Services</u>

The activities shall include but is not limited to:

- Backup of operating system, database and application as per stipulated policies at the WBSDC.
- SI shall be responsible for all infrastructure, system software, configuration files, configurations of applications, storage data, system images and file level data backup. The integrity of configurations of applications and data related to applications will be the responsibility of respective application owners. SI shall facilitate the restoration services to test the backup.

- 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 SIA 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 and testing.

  (The SI shall provide required chest and access control of offsite media storage & security and will have to bear the expenses of such activities outside location. The SIA will provide a suitable site/place for offsite storage of media and provide security personal for transportation of media as well as at offsite location. The SI will be responsible for all backup of the data stored on the SAN as well as server. For any other backup activity related to application, the primary responsibility will lie with the client. Backup activity will be facilitated by SI).
- Physical security of the media stored in cabinets.
- Ongoing support for file and volume restoration requests at the WBSDC

vi. Network & Security Administration Services

The activities to be carried out under security administration shall include but is not limited to:

- Configuration and management of network devices like routers, switches and designing, creating VLAN
- The SI shall be responsible for the security audit of the Data Center to be carried out by a certified agency other than the successful bidder.
- Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
- Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies etc.
- Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.
- Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.
- Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
- Provide a well-designed access management system, security of physical and digital assets, data and network security, backup and recovery etc.

- Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers, from viruses.
- The SI would be responsible to get the WBSDC certified for ISO 27001 (latest Version) and ISO 20000 (latest version) and sustain and upgrade the same for the next 5 years. Any cost associated with these will be borne by the SI.
- Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO/IEC 27001 and ISO/IEC 20000 guidelines
- Operating system hardening through appropriate configuration and patch updates.
- Periodic reviews of domain level rights and privileges.
- Setting up an authoritative DNS within WBSDC, so that DNS resolution for any newly added servers is never a problem.

vii. Help Desk Services

The help desk service will serve as a single point of contact for all incidents and service requests at the WBSDC. The service will provide a Single Point of Contact (SPOC) and also escalation / closure of incidents for SIA. The activities shall include but is not limited to:

- Provide Help Desk facility during agreed service period window for reporting incidents / issues / problems with the IT infrastructure.
- Provide necessary channels for reporting issues to the help desk. The incident reporting channels could be the following:
  - Specific E-Mail account
  - Telephone Line
  - Portal
- Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls related to WBSDC infrastructure and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
- Creation of knowledge base on frequently asked questions to assist user departments in resolving basic issues themselves
- Track each incident / call to resolution
- Provide feedback to callers.
- Analyze the call statistics
- Creation of knowledge base on frequently asked questions to aid users.
- Continuous monitoring of the physical as well as the IT infrastructure at the WBSDC to ensure availability as per agreed SLAs.

- Monitoring shall be done with the help of BMS and EMS monitoring tools and system logs/counters and therefore the reports and alerts can be auto-generated.
- Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed between the SI and the client. The escalation matrix shall be developed by the SI in discussion with the SIA.
- Coordinate with respective vendors for closure of calls.
- Analyze the incident / call statistics and provide monthly reports including but not limited to:
    - Type of incidents / calls logged
    - Incidents / calls resolved
    - Incidents / calls open

viii. MIS Reports

SI 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 SIA:

a. Daily reports

- Summary of issues / complaints logged at the Help Desk
- Summary of resolved, unresolved and escalated issues / complaints
- Summary of resolved, unresolved and escalated issues / complaints to vendors.
- Log of backup and restoration undertaken.

b. Weekly Reports

- Issues / Complaints Analysis report for virus calls, call trend, call history, etc.
- Summary of systems rebooted.
- Summary of issues / complaints logged with the OEMs.
- Inventory of spare parts in the WBSDC.
- Summary of changes undertaken in the Data Center 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

- Component wise physical as well as IT infrastructure availability and resource utilization
- Consolidated SLA / (non)- conformance report.
- Summary of component wise Data Center uptime.
- Summary of changes in the Data Center.
- Log of preventive / scheduled maintenance undertaken
- Log of break-fix maintenance undertaken

d. Quarterly Reports

- Consolidated component-wise physical and IT infrastructure availability and resource utilization.

- Reports related to consumables
- Reports related to service requests, incidents, problems, change management etc.

e. Half- yearly Reports

- Data Center Security Audit Report
- IT infrastructure Upgrade / Obsolescence Report
- Asset register

f. Incident Reporting

- Detection of security vulnerability with the available solutions / workarounds for fixing.
- Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.
- Software license violations

SIA may ask for additional reports related to Non-IT and IT infrastructure as and when required. SI shall have adequate skilled manpower to implement new modules of EMS and configure those modules as per the requirement of SIA. Resources should have the capability of creating customize reports as per the requirement by SIA. It is mandatory that the initial rollout of the EMS, BMS, and Cloud deployment and monitoring applications are done by the OEM directly.

DCO should agree to provide an automated SOP workflow with web enabled tools, integrated with SMS and email gateways with frontend helpdesk.

The operation & Maintenance phase Service level agreement (SLA) are detailed out in subsequent section.

3. Estimated Timelines

The table below provides the time schedule for implementation of the SDC. '**T',** as referred to in the table, is treated as the date of signing the agreement with the selected bidder by SIA.

Table 1: Tentative Time Schedule for Implementation of SDC

Sr	Activities	Timeline (Start-End) in Weeks	Milestones
'T' as referred to in the table, is treated as the date of signing the agreement with the selected SI by WTL.			
1.	Project Kick-off	T + 0	This would be done after Contract Signing between WTL and Selected Bidder.
2.	Site Survey & Feasibility for Extension area readiness to the server farm build activities.	T + 1	1. Site provisioning needs to be done by WTL. 2. SI to submit a report on the Site Survey & Feasibility.
3.	Preparation & submission of Extension area - Server farm Floor Lay-out, Implementation plan		

Sr	Activities	Timeline (Start-End) in Weeks	Milestones
	by SI		
4.	a. Approval of the SI report b. Design documents of the layouts for various systems (SLD, VESDA, WLD etc.) c. Starting of Civil Works in the 2nd Floor by the bidder	T + 2	To be obtained from WTL
5.	Approval of Layouts of various System	T+3	WTL
6.	Supply, Installation and commissioning of Non IT Infrastructure as per BOM	T + 10	
7.	Acceptance Testing of Non IT Infrastructure	T+11	
8.	Supply , Installation and Commissioning of IT Infrastructure as per BOM	T+17	
9.	Acceptance Testing of IT Infrastructure	T + 20	
10.	Complete Acceptance Testing	T + 23	Complete Acceptance Testing of the DC server farm expansion area.
11.	a. Site - Handover to WTL, Start of O&M phase and b. Submission of design document & manuals handover to end customer and Project Sign-off	T+25	After Project Sign-off, the O & M period shall start.

4. Required Resources

The below mentioned resources are the minimum requirement to maintain O&M of WBSDC and all Level 3 technical resources and Project Manager must be on the payroll of the selected bidder. Selected bidder shall appoint as many team members, over and above the manpower specified, as deemed fit by them, to meet the time Schedule and SLA requirements. SIA would not be liable to pay any additional cost for this. The above resource requirement number is indicative and the SI is required to provide on a timely basis additional resources to meet growing requirements (for e.g. in future if other databases are installed in the SDC, appropriate resources will have to be made available to manage the same or the SI needs to ensure that the already existing Database administrator is capable of managing any database used in SDC). Police verification for all the resources will be provided by the SI. Employee movement by the SI has to be approved by the SIA.

The SI shall post an on-site dedicated Project Manager to look after the entire operation of the Datacenter with his/her on-site team, with no additional responsibility. The project manager shall coordinate with the designated officer of the tendering authority.

4.1. SI will post dedicated support engineers covering 24X7 operations as follows:

Table 2: Resource List

Sr.	Details of resource	Total no. of Resource	Shift	Key Responsibilities	Qualification
1.	Project Manager	1	8 hours per day X 6 days	Complete Ownership of the project. Customer interfacing, Review meetings, OEM interactions, Reporting to customer	B.Tech/ B.E. with MBA & minimum 7 years' experience
2.	Network Expert (L3)	1	8 hours per day X 6 days	Å In charge of actual Configuration and maintenance of network equipment in DC Å Good working knowledge of latest Leaf and spine architecture and SDN /NFV networking, with the latest breed of Networking equipment available . Å Responsible for maintaining all configuration templates for respective equipment Å Should have adequate experience of configuring Firewall, IPS, APT, Deep Security Appliances, Network and Server Load balancers. Å Perform periodic proactive tests on the equipment and systems under their command to ensure compliance to State IT and Security Policy and maximize user satisfaction Å Would be monitoring independent of NMS tools to ensure better network uptime and performance Å Would be responsible for preparing the change management document for approval Å Would be responsible for backing up all	B.Tech/ B.E., with CCNP/ CISSP or equivalent & minimum 5+ years' experience

Sr.	Details of resource	Total no. of Resource	Shift	Key Responsibilities	Qualification
				network related configurations on a regular basis Å Would be upgrading the necessary and recommended IOS on all crucial Network equipment in the DC	
3.	Network Expert (L2)	2(in 2 shifts)	16 Hours Per day X 6 days (will be present during the hours at which the L3 is not present)	• Install and support LANs, WANs, network segments, Internet, and intranet systems. • Install and maintain network hardware and software. • Analyze and isolate issues. • Monitor networks to ensure security and availability to specific users. • Evaluate and modify system's performance. • Identify user needs. • Determine network and system requirements. • Maintain integrity of the network, server deployment, and security. • Ensure network connectivity throughout a SDC's LAN/WAN infrastructure is on par with technical considerations. • Design and deploy networks. • Perform network address assignment. • Assign routing protocols and routing table configuration. • Assign configuration of authentication and authorization of directory services. • Maintain network facilities in individual machines, such as drivers and settings of personal computers as well as printers. • Maintain network servers such as file servers, VPN gateways, and intrusion detection systems. • Administer servers, desktop computers, printers, routers, switches, firewalls, phones, personal digital assistants, smartphones, software deployment, security updates and patches.	B.Tech/ B.E., with CCNA/ CCNP or equivalent & minimum 3+ years' experience
4.	Server and Cloud Expert (L3)	1	8 hours per day X 6 days	Å Microsoft Windows Server 2012 Data center Edition Å RHEL – configuration, administration, monitoring and rollout in Blade Chassis environment. Å OS Patch management using WSUS/SCCM/ CA Client Automation Å Antivirus and Security compliance , Host IPS , MS Proxy, ISA, DHCP, AD , Windows Cluster , Group Domain Policies Å Knowledge of MS Virtualization (Hyper-V) or VMWare and Virtualization	B.E./B.Tech, 5+ Years, MCSE, RHCE, MCP

Sr.	Details of resource	Total no. of Resource	Shift	Key Responsibilities	Qualification
				management software Å Basic Windows scripting Å Basic configuration of Firewall, Routers, Core and Edge switches. Å Knowledge of mailing systems and SMTP and SMS gateway administration Å Knowledge of backup Software e.g. EMC Networker, HP NetBackup etc. Å Will be responsible for OEM interaction for service and spare availability as per SLA Å Troubleshooting and root cause analysis of server hardware and OS Å Monitoring the server logs and critical errors for proactive support Å Will be responsible for tuning various parameters of OS	
5.	Server and Cloud Expert (L2)	2(in 2 shifts)	16 Hours Per day X 6 days (will be present during the hours during which the L3 is not present)	• Ensures server performance and maintains applications on servers; • Problem solving and documentation of current and new servers in both physical and virtual environments; • Performs and oversees continuous system health checks, user administration, and application of patches and upgrades • Performs data management services, server tuning, and directory services maintenance; • Delivers anti-virus software updates and virus protection • Ensures compliance to security standards, policies and guidelines • Provides business continuity through thorough back-up and restore procedures, and periodic testing of outage scenarios; • Administers and maintains a Windows of Linux -based server network, with a combination of physical and virtual servers.	B.E./B.Tech, 3+ Years, with MCSE/Server Certification
6.	Storage Cum Database Administrator	2(2 shifts)	8 hours per day X 6 days	• Manage the Storage Networks • Configuration of the Storage • Creation of Storage Partition • Manage the Database • Configure the Database • Troubleshoot the Database whenever required • Implementation, Support and manage	
7.	Security Expert (L3)	1	8 hours per day X 6 days	• Would be responsible for the information security of the network, and server operating systems , upgrades and patch management	B.E./B.Tech, 5+ Years, Security

Sr.	Details of resource	Total no. of Resource	Shift	Key Responsibilities	Qualification
				• Would be conducting periodic audit on the network equipment, and server operating systems for identifying vulnerabilities using VA/PT tools • Would be monitoring the security reports generated by SIEM and Deep security for immediate mitigation as required • Would be checking the OEMs security alerts and cross verify with the current posture of equipment at DC • Would be responsible for conducting the test run of critical security updates and patches meant for the DC components. • Would be accountable for the roll-out of security updates and patches in the DC • Would be providing necessary security guidelines to other team members on their respective area • Would be reporting and follow-up with OEMs for any security related incidents	Certifications, ISMS, CISA/CISM
8.	Security Expert (L2)	2(in 2 shifts)	16 Hours Per day X 6 days (will be present during the hours during which the L3 is not present)	• Monitor the infrastructure and maintain the security standards • Would be monitoring the security reports generated by SIEM and Deep security • checking the OEMs security alerts • Monitor and alert the owner for security updates and patches meant for the DC components	B.E./B.Tech, 3+Years, Security Certifications, ISMS, CISA/CISM
9.	Technical Specialist – physical infrastructure, BMS & Electrical equipment etc.	3(in 3 shifts)	24 hours per day X 7 days	Responsible for the complete maintenance of the non-IT Physical part of the SDC including the physical security, BMS infrastructure, Power and HVAC systems	Data Center Operation Experience for 5+ Years
10.	Backup administrator	3(in 3 shifts)	24 hours per day X 7 days	• Backup of Data Center Applications • Backup of day to day transactions(Hot and Cold Back)	Experience on Backup and Storage 3 + years' with OEM Certification
11.	Help Desk Support executive	3 (in 2 shifts)	24 hours per day X 7 days	• Receive incident related communication on phone, mail, and web interface • Validate the incident with relevant details and generate trouble ticket • Assign the trouble tickets to relevant engineer or specialist for resolution	Graduate/ Diploma, 2 Years, Relevant, ITIL Knowledge

Sr.	Details of resource	Total no. of Resource	Shift	Key Responsibilities	Qualification
				• respond to requests for technical assistance in person, via phone, electronically • diagnose and resolve technical hardware and software issues • research questions using available information resources • advise user on appropriate action • follow standard help desk procedures, log all help desk interactions	
12.	EMS Expert	2 (in 2 shifts)	16 hrs (1 Nos from 9 Am to 6 PM & 1 for next 8 hr shift	• Receive incident related communication on phone, mail, and web interface • Validate the incident with relevant details and generate trouble ticket • Assign the trouble tickets to relevant engineer or specialist for resolution • respond to requests for technical assistance in person, via phone, electronically • diagnose and resolve technical hardware and software issues • research questions using available information resources • advise user on appropriate action • follow standard help desk procedures, log all help desk interactions	Experience on EMS 3 + years' with OEM Certification
13.	Physical Security	4 (in 3 shifts)	24 hrs(2 Nos from 9 Am to 6 PM & 1 each for next 8 hr shift	• Monitor all the individuals entering and leaving the Operation Area • Maintain a Log register of all activities	Similar experience of 5 + years
14.	House keeping	2 (in 2 shifts)	8 * 6	• sweep, scrub, mop and polish floors outside DC • Only vacuum clean and MOP DC floor • vacuum clean carpets, rugs and draperies • dust and polish furniture and fittings • clean metal fixtures and fittings • empty and clean trash containers	Similar or relevant experience

The resources once placed cannot be replaced without prior approval of CT. Resources must be replacedwith following terms:

i. Not more than 20% of total resources of FMS team is allowed to change other than resignation in ayear by SI of their own. If more than 20% resource is replaced during one year, then for every Additional 10% change in resources, 2% of the QGR will be deducted. This clause will not be applicable if the resource replacement is done as per the directive of SIA/CT.

ii. Whenever there is change in manpower/ resource, SI has to inform CT/SIA in writing with all details of both the person who is leaving and who is joining at least 30 days in advance.

iii. The new resource must meet the qualification criteria as mentioned above as well as should have adequate skillsets to run the operations and management of Data Center infrastructure or upgrading the Data Center infrastructures.

iv. The new resource must be provided training for a minimum period of 21 days to acquire properKnowledge of the domain he/she will look into from the leaving resource and the same will be verifiedby SIA/CT on timely manner. The new resource can take charge only after acquiring entire domainknowledge and upon verification and approval by SIA/CT.

v. After placement of the resource, if CT finds the resource incompetent to perform his/her duties, the same would be communicated to SI in writing and SI will arrange to replace with the suitable resource within 30 days.

- Resources should be trained on periodic basis to make their skillset capable enough to implement new technologies, modules or exploit features of newly added modules of EMS/Databases/Security products etc.
- The SI should not be reluctant in implementing new initiatives taken by SIA pertaining to new features available with the new version/bundle of any Products. Customization of new features available with existing products or upgraded products will not be treated as new implementation by SI and no change request will be considered in such cases.

Bidder shall share costing for all positions separately in an excel sheet

SECTION – B

1. ELIGIBILITY CRITERIA

The Bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements as described in the RFP document. Keeping in view the complexity & volume of the work involved, the following criteria are prescribed as pre-qualification criteria for Bidder interested in undertaking the project. The Bidder must also possess the technical know-how and the financial wherewithal that would be required to successfully provide the Data Center and support services sought by the State for the entire period of the contract. The bids must be complete in all respect and should cover the entire scope of work as stipulated in the tender document. The invitation to bid is open to all Bidders who qualify the eligibility criteria as given below:

1.1. Definition of Consortium Partner:

Consortium shall mean more than one company which joins with other companies of complementing skills to undertake the scope of work defined in this RFP. The consortium can only be formed with the companies dealing in either one of the work stated below:

1.1.1. Data Center Build-up project (NON –IT)

- Planning
- Designing
- Implementation
- Commissioning & Testing

1.1.2. Data Center Build-up project (IT)

- Planning
- Designing
- Implementation
- Commissioning & Testing

1.1.3. Facility Management for IT and Non IT

And should have experience in either one of the fields stated below:

- Design, Supply, Installation and Commissioning
- Facilitation for Application Migration
- Operation and Maintenance of Data Center components and services

1.2. Eligibility Criteria:

Table 3:Eligibility criteria

S. No.	Clause	Documents required
1.	The bidder (prime) should furnish, as part of its bid, an Earnest Money Deposit (EMD) of Rs. 12000000.00.	The EMD should be denominated in Indian Rupees, and should be in the form of Bank Guarantee valid for 6 months from the date of bid submission.
2.	The Bid can be submitted by an individual company or a consortium. In case of consortium applicant, consortia shall submit a valid Memorandum of Understanding (MOU)/agreement.	"Consortium" shall mean more than one company which joins with other companies of complementing skills to undertake the scope of work defined in this RFP. In case of consortium the same shall not consist of more than three companies/ corporations, including the prime bidder. 1. Memorandum of Understanding (MOU)/agreement among the members signed by the Authorized Signatories of the companies dated prior to the submission of the bid to be submitted in original. 2. The MoU/agreement shall clearly specify the prime bidder, stake of each member and outline the roles and responsibilities of each member.
3.	The bidder (prime) should be a company registered under the Companies Act, 1956 since last 3 years as on 31.03.2017	Certificate of incorporation
4.	Bidder (prime) should have experience of IT System Integration/ Information Technology Infrastructure projects including implementation/ operations and should have been in the business for a period exceeding five years as on 31.03.2017. Bidder (prime) who has acquired a company/ division of a company having experience as mentioned above shall also be considered.	A. Work Orders confirming year and area of activity. B. Memorandum and Articles of Associations. C. Relevant legal documentation confirming the acquisition/merger.
5.	Bidder (prime) must have ISO 9001:2015 certification	Valid Copy of Certificate

S. No.	Clause	Documents required
6.	The bidder (prime) should have commissioned and installed at least one Data center project that meets all the below mentioned requirements during the last Five (5) years, i.e. 2012-13, 2013-14, 2014-15 & 2015-16, 2016-17 a. An Order Value (including IT and Non-IT but excluding basic building structure cost) of not less than Rs. 20 crores. b. Valid BS 7799 / ISO 27001 certification Note: • Bidder's in house data centers shall not be considered. • Bidders who have built their own Internet Data Center (IDC), for commercial use will be considered.	a. Copy of work order / client certificates. For IDC bidder, Notarized Certificate from Company Secretary confirming the order value/cost. b. Valid Certification (IDC bidder shall also submit customer work orders)
7.	The bidder (prime) should have experience in providing Facility management services to at least one data center, during the last five years i.e. 2012-13, 2013-14, 2014-15 2015-16 & 2016-17. The facility management services shall include Cloud, IT infrastructure related (e.g. Servers, storage, networks etc.) / non IT related services (Power, cooling, physical security etc.) Note: • Bidder's in house data centers shall not be considered. • Bidders who have built their own Internet Data Center (IDC), for commercial use will be considered.	Copy of work order / client certificates.
8.	The bidder (Prime/ Consortium partner) should have a CMMi level 3 Certificate	Valid CMMi Level -3 certificate
9.	The bidder (prime) should have a turnover of more than Rs. 100 Crores for each of the last three financial years 2014-15, 2015-16 & 2016-17.	Copy of the audited profit and loss account of the company showing turnover of the company for last three years.
10.	a) The bidder (prime) must have on its roll at least 30 technically qualified professionals in, networking, systems integration, and prior experience in providing the Data Center Infrastructure maintenance services as on 31-03-17. b) At least five resources should be ITIL certified and	a) Certificate from bidders HR Department for number of Technically qualified professionals employed by the company. b) Name of the employees along with certified copies of the certifications done, which are ITIL / BS7799/ISO 27001 lead Auditor or Lead

S. No.	Clause	Documents required
	two resources should be BS7799/ISO 27001 lead Auditor or Lead Implementer certified.	Implementer certified to be provided.
11.	The Bidder and/or all/any consortium partners shall not be under a Declaration of Ineligibility for corrupt or fraudulent practices or blacklisted with any of the Government agencies, as on Bid Submission date.	Declaration in this regard by the authorized signatory of the prime bidder
12.	The bidder (prime) should submit valid letter from the OEMs confirming following: • Authorization for bidder • Confirm that the products quoted are not reaching EOL within two years &EOS within 5 years Otherwise the same will be changed with the superior product at no extra cost. • Undertake that the support including spares, patches, and upgrades for the quoted products shall be available for the period of the Project upto 7 years	OEMs include but not limited to: • Compute Infrastructure • Networking Infrastructure • Storage Infrastructure • Cloud services • UPS • HVAC • Generator • Fire detection &Suppression • Surveillance
13.	Each Server and Software OEM is required to submit an undertaking on the horizontal support of its product acrossvarious platforms/processors, as follows: **Server** Each Server OEM is required to submit an undertaking, certifying its product to be supported on Operating Systems (OS), and Databases, with names and version details of the supported OS and Databases, for a period of 6 years, applicable from the date of completion of FAT. In case the said support is terminated for any reason within the required support period for SDC, the OEM shall provide a better server with no additional cost. **Software** Each Software OEM is required to submit an undertaking, certifying its product to be supported on the Server and Databases/ OS, with names and version details of the supported Server and Databases/OS, for a period of 6 years from the date of completion of FAT. In case the said support is terminated for any reason within the required support period for SDC, the OEM shall provide a new version of software as applicable, with no additional cost.	Declaration letter, along with relevant supporting documents

S. No.	Clause	Documents required
	OEM of **each equipment/system** is required to submit an undertaking on support of its product for a period of 6 years, applicable from the date of completion of FAT. In case the said support is terminated for any reason within the required support period for SDC, the OEM shall provide a better equipment/system with no additional cost.	
14.	The bidder (prime) should have an office in the state. However, if the local presence is not there in the state, the bidder should give an undertaking for establishment of an office, within two months of award of the contract and the local office should be equipped with the adequate resource to provide L2/ L3 level support as and when would be required.	Relevant Documents or Undertaking signed by the Authorized Signatory
15.	The bidder should submit an acceptance of Terms and Conditions contained in the RFP document.	Declaration in this regard by the authorized signatory of the prime bidder should be attached. Refer to Section 8.5 of volume-I of this RFP
16.	The bidder should submit valid GST registration certificate and Permanent Account Number (PAN) issued by income Tax department.	Copy of each registration should be provided.
17.	The bidder should submit a copy of the entire RFP document with every page signed by an authorized signatory of the Bidder	Signed RFP copies (both volumes), and **must have court fee stamps of value Rs. 8.25/- affixed on the tender issue page (Page no. 2).**
18.	The bidder should submit power of attorney certifying the authorized signatory.	Power of Attorney executed by the Bidder in favor of the Principal Officer or the duly Authorized Representative, certifying him as an authorized signatory for the purpose of this Tender.

Note: In the event of a consortium, one of the partners shall be designated as a "Prime Bidder". The bidder (prime) of the consortium shall be an Information Technology Company/ IT System Integrator. Every member of the consortium shall be equally responsible and jointly liable for the successful completion of the entire project.

In Consortium all the members shall be equally responsible to complete the project; however prime bidder shall give an undertaking for successful completion of the project. In case of any issues, prime bidder would be responsible for all the penalties.

A bidding company/ corporation cannot be a part of more than one Consortium. Any Member of consortium cannot bid separately as a sole bidder. The bidder (all consortium partners) must have Company registration certificate, Registration under labor laws & contract act, valid VAT/ Sales Tax Registration Certificate, valid

Service Tax Registration Certificate and Income Tax Return with Audit Report from CA. Bidder shall provide an attested copy of all the above mentioned certificates along with this bid document.

1.3. Criteria for Evaluation of Bids

- A three-stage procedure will be adopted for evaluation of proposals, with the pre-qualification being completed before the technical evaluation and thereafter financial proposals being opened and compared. Pursuant to the pre-qualification criterion Bidders will be short-listed for technical bid. Technical bids will be opened only for the Bidders who succeed the pre-qualification criterion. The technical bids for the disqualified Bidders will be returned unopened at the address mentioned on the envelopes containing the technical bid.
- SIA will review the technical bids of the short-listed Bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified.
- SIA will assign points (quality of services score) to the technically qualified Bidders based on the technical evaluation criterion as mentioned in section 6.18.2. The commercial bids for the technically qualified Bidders will then be opened and reviewed to determine whether the commercial bids are substantially responsive.
- The evaluation will be made on the basis of least cost.
- Conditional bids are liable to be rejected.

1.3.1. Criteria for Evaluation and Comparison of Pre-qualification Bids

- The Bidder shall be liable for adherence to all provisions of this Agreement.
  The Pre-Qualification proposal will be evaluated using the checklist given in Section 2

1.3.2. Criteria for Evaluation and Comparison of Technical Bids

- Technical proposal of only those bidders will be opened and evaluated who meet all the pre-qualification criteria.
- The evaluation committee will evaluate the Technical Proposals on the basis of the technical evaluation criterion as provided below.
- Qualifying marks for opening Financial bid is 32 under the category “Organizational strength” out of 40 (80%) and 48 under the category “Technical Solution offered” out of 60 (80%). Firms, scoring less than 80% marks in any one of the category between “Organizational Strength” and “Technical Solution Offered”, will not be eligible for opening financial bid.
- Technical bids will be reviewed for determining the technical capability of the Bidder for the Project and to ascertain Compliance of the Technical bids with the RFP terms and conditions, technical requirements and scope of work as defined in this RFP.

1.3.3. Scoring Criteria and evaluation parameters:

Table 4: Evaluation Parameters

Sr	Technical Score	Marks
A	Organizational Strength	40
B	Technical Solution Offered	60
	Total (A + B)	100

Sr	Evaluation Parameter		Breakup of Marks	Total Marks
A) Organizational strength (40 marks)				
A.1	Bidder's experience in implementation of Data Center projects or Large Scale implementation of IT project in India with a value of Rs. 10 Crore or above;			10
	Slab 1	1 Projects executed	2	
	Slab 2	2 Projects executed	6	
	Slab 3	3 Projects or more executed	10	
A.2	Bidder's experience in providing system integration quantified in terms of number of years will be evaluated; project considered for evaluation should have project cost more than Rs. 5 Crore.			10
	Slab 1	Projects experience of more than 2 years	4	
	Slab 2	Projects experience of more than 4 years	8	
	Slab 3	Projects experience of more than 6 years	10	
A.3	Bidder's experience in providing facility management quantified in terms of number of projects will be evaluated; project considered for evaluation should have project cost more than Rs. 4 Crore.			10
	Slab 1	1 Project under maintenance	2.5	
	Slab 2	2 Projects executed under maintenance	5	
	Slab 3	3 Projects under maintenance	7.5	
	Slab 4	4 Projects or more under maintenance	10	
A.4	Average Turnover of the bidder from Indian Operations for the last 3 financial years;(In Crores)			5
	Slab 1	Avg. turnover > Rs 400 Cr	5	
	Slab 2	Avg. turnover > Rs 350 Cr ≤ Rs 400 Cr	4	
	Slab 3	Avg. turnover > Rs 300 Cr ≤ 350 Rs Cr	3	
	Slab 4	Avg. turnover > Rs 250 Cr ≤ Rs 300 Cr	2	
	Slab 5	Avg. turnover > Rs 200 Cr ≤ 250 Cr	1	
A.5	Bidder's Manpower strength on own payroll			5
	Slab 1	Manpower strength of >100 but <= 150	1	
	Slab 2	Manpower strength of >150 but <= 200	2	
	Slab 3	Manpower strength of >200 but <= 300	3	
	Slab 4	Manpower strength of >300 but <= 400	4	
	Slab 5	Manpower strength of >400	5	

Sr	Evaluation Parameter		Breakup of Marks	Total Marks
B) Technical solution offered (60 marks)				
B.1	Design & Architecture:			15
	Slab 1	Description of the design and technical solution and various components including design diagrams and elaboration of components	5	
	Slab 2	Extent of compliance to technical requirements as per given specifications of RFP Vol-II & for quoting all the products. For mismatch of product specification 1 marks will be deducted for each product. Mismatch of specifications for more than 5 products will be treated as disqualification of the bid. Selected bidder needs to comply with product specification as per RFP and products needs to be replaced by the bidder where technical specification mismatch identified.	5	
	Slab 3	Commissioning of complete data center and adherence to Best practices like ISO, ITIL, BS15000, IPv6 etc.	5	
B.2	Solution document with detailed understanding of the project including:			20
	Slab 1	Approach & Methodology for Installation, Configuration (3 marks maximum on pro-rata basis) & Migration of IT Components with minimal downtime (2 marks maximum on pro-rata basis)	5	
	Slab 2	Approach & Methodology for Installation, Configuration (3 marks maximum on pro-rata basis) & Migration of non-IT Components with minimal downtime (2 marks maximum on pro-rata basis)	5	
	Slab 3	Approach & Methodology - presentation	10	
B.3	Project Plan with timeline and milestones			5
B.4	Resource planning and allocation			20
B.4.1	SI Project Manager – 1 no. (6 marks)			
B.4.1.1	Slab 1	Education: (B.E. / B.Tech) or MBA or its equivalent with PMP/Prince2 certification (2 Marks)	2	
	Slab 2	Education: B.E. / B.Tech or MBA or its equivalent without PMP/Prince2 certification (1 mark)		
B.4.1.2	Slab 1	Overall Experience: 10+ years of experience (2 marks)	2	
	Slab 2	Overall Experience: 8 + years of experience (1 mark)		
B.4.1.3	Slab 1	Data Center implementation & operations experience: With 5+ years (2 marks)	2	
	Slab 2	Data Center implementation & operations experience: With 3+ years (1 mark)		
B.4.2	DC Design and IT Expert -1 no. (4 Marks)			
B.4.2.1	Slab 1	Education: B.E. / B.Tech / MCA with ISO 27001:2013 lead implementer/auditor certification(2 marks)	2	
	Slab 2	Education: B.E. / B.Tech / MCA without ISO 27001:2013 lead implementer/auditor certification (1 mark)		
B.4.2.2	Slab 1	Overall Experience: More than 7 years' experience with 5+ year Data Center implementation with execution of two similar projects (2 marks)	2	
	Slab 2	Overall Experience: More than 7 years' experience with 3+ years, Data Center implementation with execution of two similar projects (1 mark)		
B.4.3	Non IT Solution Expert – 2 nos.(4 Marks, 2 for each expert)			
B.4.3.1	Slab 1	Education: B.E. / B.Tech or above with specialization in Civil Engineering with CDCP certification (1mark) Overall Experience: More than 7 years' experience with 3+ year Data Center Non IT Infrastructure implementation with execution of two similar projects (1 Mark)	2	

Sr	Evaluation Parameter		Breakup of Marks	Total Marks
	Slab 2	Education: B.E. / B.Tech or above with specialization in Electrical/Mechanical Engineering with CDCP certification (1mark) Overall Experience: More than 7 years' experience with 3+ year Data Center Non IT Infrastructure implementation with execution of two similar projects (1 Mark)	2	
B.4.4	Infrastructure Implementation team – 2 no's (6 marks)			
B.4.4.1	Slab 1	5 + Experience in DC implementation but not limited to Storage, Network, Security (2 marks)	2	
	Slab 2	3 + Experience in DC implementation but not limited to Storage, Network, Security (1 mark)		
	Slab 3	Certification – ITIL and CCNA with any security certification (2 Marks)	2	
	Slab 4	Certification – ITIL and CCNA without any security certification (1 Mark)		
B.4.4.2	Slab 1	5 + Experience in DC implementation but not limited to Server, Storage, Network etc. with ITIL and RHCE/MCSE certifications (2 marks)	1	
	Slab 2	5 + Experience in DC implementation but not limited to Server, Storage, Network etc. without ITIL and RHCE/MCSE certifications (1 mark)	1	

1.3.4. Financial Bid Evaluation

- The Financial Bids of technically qualified bidders (i.e. above 80 marks) will be opened on the prescribed date in the presence of bidder representatives.
- Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.
- The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.
- Any conditional bid would be rejected.
- Errors & Rectification: Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail".
- If there is no price quoted for certain material or service, the bid shall be declared as disqualified.
- The lowest quoted price of the financial bid amongst the technically qualified bidders will be declared L1 bid.
- In the event that there are 2 or more bidders having the same value in the financial bid, the bidder securing the highest technical score will be adjudicated as the "Best responsive bid" for award of the Project.

1.4. Appointment of System Integrator

1.4.1. Award Criteria

WTL will award the Contract to the successful bidder whose financial proposal is the lowest and would consider it as substantially responsive as per the process outlined above.

1.4.2. Right to Accept Any Proposal and To Reject Any or All Proposal(s)

WTL reserves the right to accept or reject any proposal, and to annul the tendering process / Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for WTL action.

1.4.3. Notification of Award

Prior to the expiration of the validity period, WTL will notify the successful bidder in writing or by fax or email, that its proposal has been accepted. In case the tendering process / public procurement process has not been completed within the stipulated period, WTL, may like to request the bidders to extend the validity period of the bid.

The notification of award will constitute the formation of the contract. Upon the successful bidder's furnishing of Performance Bank Guarantee, WTL will notify each unsuccessful bidder and return their EMD.

1.4.4. Contract Finalization and Award

The WTL shall reserve the right to negotiate with the bidder(s) whose proposal has been most responsive. On this basis the draft contract agreement would be finalized for award & signing.

WTL may also like to reduce or increase the quantity of any item in the Scope of Work defined in the RFP. Accordingly total contract value may change on the basis of the rates defined in the financial proposal.

1.4.5. Performance Guarantee

The WTL will require the selected bidder to provide a Performance Bank Guarantee, within <15> days from the Notification of award, for a value equivalent to <10%> of the total cost of ownership. The Performance Guarantee should be valid for a period of <months>. The Performance Guarantee shall be kept valid till completion of the project and Warranty period. The Performance Guarantee shall contain a claim period of three months from the last date of validity. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and Warranty period. In case the selected bidder fails to submit performance guarantee within the time stipulated, the WTL at its discretion may cancel the order placed on the selected bidder without giving any notice. WTL shall invoke the performance guarantee in case the selected Vendor fails to discharge their contractual obligations during the period or WTL incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.

1.4.6. Signing of Contract

After the WTL notifies the successful bidder that its proposal has been accepted, WTL shall enter into a contract, incorporating all clauses, pre-bid clarifications and the proposal of the bidder between WTL and the successful bidder. The Draft Legal Agreement is provided as a separate document as a template.

1.4.7. Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful bidder to agree with the Draft Legal Agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event WTL may award the contract to the next best value bidder or call for new proposals from the interested bidders.

In such a case, the WTL shall invoke the PBG of the most responsive bidder.

1.4.8. Confidentiality of the Document

This Tender Document is confidential and the Bidder shall ensure that anything contained in this Tender Document shall not be disclosed in any manner, whatsoever.

1.5. Rejection Criteria

Besides other conditions and terms highlighted in the tender document, bids may be rejected under following circumstances:

1.5.1. Pre-Qualification Rejection Criteria

- Bids submitted without or with improper EMD.
- Bids which do not conform to unconditional validity of the bid as prescribed in the Tender.
- If the information provided by the Bidder is found to be incorrect / misleading at any stage / time during the Tendering Process.
- Any effort on the part of a Bidder to influence the bid evaluation, bid comparison or contract award decisions.

- Bids received by the SIA after the last date prescribed for receipt of bids.
- Bids without signature of person (s) duly authorized on required pages of the bid
- Bids without power of authorization and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder.

1.5.2. Technical Rejection Criteria

- Technical Bid containing commercial details.
- Revelation of Prices in any form or by any reason before opening the Commercial Bid.
- Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to the Tender Document in every respect.
- Bidders not quoting for the complete scope of Work as indicated in the Tender documents, addendum (if any) and any subsequent information given to the Bidder.
- Bidders not complying with the Technical and General Terms and conditions as stated in the RFP Documents.
- The Bidder not conforming to unconditional acceptance of full responsibility of providing services in accordance with Scope of work and Service Level Agreements of this tender.
- If the bid does not confirm to the timelines indicated in the bid.

1.5.3. Commercial Rejection Criteria

- Incomplete Price Bid
- Price Bids that do not conform to the Tender's price bid format.
- Total price quoted by the Bidder does not include all statutory taxes and levies applicable.

1.6. Concessions permissible under statutes

Bidder, while quoting against this tender, must take cognizance of all concessions permissible under the statutes including the benefit under Central Sale Tax Act, 1956, failing which it will have to bear extra cost where Bidder does not avail concessional rates of levies like customs duty, excise duty, sales tax, etc. The SIA will not take any responsibility towards this. However, SIA may provide necessary assistance, wherever possible, in this regard.

1.7. Payment Milestone

Sr. No.	Payment Schedule	Fee Payable	Remarks
1.	Mobilization Advance	10% of the total CAPEX	Payable against Bank Guarantee for an amount equal to 10% of the Contract value on or before 10 days of signing of Contract.
2.	On Delivery of all the Non-IT equipment	50% of the CAPEX value of the delivered Non-IT equipment	Payable on successful check of all / part of the delivered equipment by WTL appointed Nodal Officer.
3.	PAT of Non-IT components	30% of The CAPEX value of the installed Non-IT equipment	Payable on successful PAT of all the installed equipment WTL appointed Nodal Officer, post PAT Certification by Consultant
4.	On Delivery of all the IT equipment	50% of the CAPEX value of the delivered IT equipment	Payable on successful check of all/ part of the equipment by WTL appointed Nodal Officer.
5.	PAT of IT components	30% of The CAPEX value of the installed IT equipment	Payable on successful PAT of all the installed equipment by WTL appointed Nodal Officer, post PAT Certification by

Sr. No.	Payment Schedule	Fee Payable	Remarks
			Consultant
6.	On successful final acceptance test	10% of the CAPEX	Payable on Successful implementation of FAT, in accordance with WTL and concerned department.
7.	Operations and Management for 5 years payable quarterly (as QGR) at the end of each quarter	5% (per quarter) of the OPEX	Payment release subject to Performance.

1.8. Income Tax Liability

The Bidder will have to bear all Income Tax liability both corporate and personal tax.

2. SERVICE LEVEL MANAGEMENT

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the SI to SIA for the duration of this contract.

The SI and SIA shall regularly review the performance of the services being provided by the SI and the effectiveness of this SLA

Note:

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the SI to SIA for the duration of this contract.
The SI and SIA shall regularly review the performance of the services being provided by the SI and the effectiveness of this SLA

2.1. Definitions

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

- "Uptime" shall mean the time period for which the specified services / components with specified technical and service standards are available to the state and user departments. Uptime, in percentage, of any component (Non IT & IT) can be calculated as:

  Uptime = {1- [(Downtime) / (Total Time – Scheduled Maintenance Time)]} * 100

- “Downtime” shall mean the time period for which the specified services / components with specified technical and service standards are not available to the state and user departments and excludes the scheduled outages planned in advance for the West Bengal State Data Center and the link failures that are SWO’s responsibility.

- “Incident” refers to any event / abnormalities in the functioning of the Data Center Equipment / specified services that may lead to disruption in normal operations of the West Bengal State Data Center services.

- “Helpdesk Support" shall mean the 24x7 Center which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.

- “Resolution Time” shall mean the time taken in resolving (diagnosing, troubleshooting and fixing) an incident after it has been reported at the helpdesk. The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:
  a) Critical: Incidents whose resolution shall require additional investment in components or time or shall involve coordination with OEMs. These incidents shall impact the overall functioning of the SDC. For example, purchase of printer, router, software bug fixing etc.
  b) Medium: Incidents, whose resolution shall require replacement of hardware or software parts, requiring significant interruption in working of that individual component. For example, installation of operating system, replacement of switch etc.
  c) Low: Incidents whose resolution shall require changes in configuration of hardware or software, which will not significantly interrupt working of that component. For example, installation of printer on a client etc.

2.2. Category of SLAs

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The SI shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the SI shall be reviewed by the West Bengal Electronics Industry Development Corporation Limited that shall:

- Regularly check performance of the SI against this SLA.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

The SLA has been set on:

2.2.1. Implementation Service levels

The following measurements and targets shall be used to track and report the implementation performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract. All the targets for the completion of the implementation activity are calculated on a weekly basis. Please note that the Bidder should provide comprehensive, end-to-end service to implement the SDC Infrastructure, including replacement of the equipment in case of physical damage. No reason shall be entertained (unless those mentioned in Force Majeure) in case of unavailability of any service given in the scope of work in this RFP and the appropriate penalty shall be levied.

- **Implementation Service Levels**

Table 5: Implementation Service Levels

Measurement	Target	Severity	Penalty
Civil Work	10 weeks from the signing of contract	Critical	A Penalty as 0.5% per week for every week delay in PAT. Subject to a maximum of 5% Penalty will be computed on the remaining milestone activity
Installation of all Non-IT Components including Electrical and BMS	20 weeks from the signing of contract	Critical	A Penalty as 0.5% per week for every week delay in PAT. Subject to a maximum of 5% Penalty will be computed on the remaining milestone activity
Installation of all IT Components	23 weeks from the signing of contract	Critical	A Penalty as 0.5% per week for every week delay in PAT. Subject to a maximum of 5% Penalty will be computed on the remaining milestone activity

Integrated Testing and Final Acceptance test (FAT) completed and handing over.	25 weeks from the signing of contract	Critical	A Penalty as 0.5% per week for every week delay in FAT. Subject to a maximum of 5% Penalty will be computed on the remaining milestone activity

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

- "Uptime" shall mean the time period for which the specified services / components with specified technical and service standards are available to the state and user departments. Uptime, in percentage, of any component (Non IT & IT) can be calculated as:

  Uptime = {1- [(Downtime) / (Total Time – Scheduled Maintenance Time)]} * 100

- "Downtime" shall mean the time period for which the specified services / components with specified technical and service standards are not available to the state and user departments and excludes the scheduled outages planned in advance for the West Bengal State Data Center and the link failures that are SWO's responsibility.
- "Incident" refers to any event / abnormalities in the functioning of the Data Center Equipment / specified services that may lead to disruption in normal operations of the West Bengal State Data Center services.
- "Helpdesk Support" shall mean the 24x7 center which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.
- "Resolution Time" shall mean the time taken in resolving (diagnosing, troubleshooting and fixing) an incident after it has been reported at the helpdesk. The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:
  a) Critical: Incidents whose resolution shall require additional investment in components or time or shall involve coordination with OEMs. These incidents shall impact the overall functioning of the SDC. For example, purchase of printer, router, software bug fixing etc.
  b) Medium: Incidents, whose resolution shall require replacement of hardware or software parts, requiring significant interruption in working of that individual component. For example, installation of operating system, replacement of switch etc.
  c) Low: Incidents whose resolution shall require changes in configuration of hardware or software, which will not significantly interrupt working of that component. For example, installation of printer on a client etc.

2.2.2. Operation & Maintenance Service levels

2.2.2.1. IT Infrastructure Service Levels

Following outlines the service level indicators & and the target performance levels to be maintained by the Agency during the contract period. These SLAs shall be strictly imposed and a third party audit/certification agency shall be deployed for certifying the performance of the Agency against the target performance metrics as outlined in the table below:

Table 6: IT Infrastructure Service Levels

Sr	Measurement	Target	Severity	Penalty

Sr	Measurement	Target	Severity	Penalty
1.	Individual Server Availability (including the OS, database and application running on it)	>= 99.749%	Critical	No Penalty
		>=99 % <99.749%		1% of the QGR
		>=98 % < 99 %		2% of the QGR
		>=95 % < 98%		3% of the QGR
		< 95 %		Maximum of 5 of the QGR can be imposed
2.	Storage Availability	>= 99.749%	Critical	No Penalty
		>=99 % <99.749%		2% of the QGR
		>=98 % < 99 %		5% of the QGR
		>=95 % < 98%		8% of the QGR
		< 95 %		Maximum of 10 % of the QGR can be imposed
3.	Connectivity with SWAN	>= 99.749%	Critical	No Penalty
		>=99 % <99.749%		1% of the QGR
		>=98 % < 99 %		2% of the QGR
		>=95 % < 98%		5% of the QGR
		< 95 %		Maximum of 10 % of the QGR can be imposed
4.	VTL Availability	>= 99.749%	Critical	No Penalty
		>=99 % <99.749%		1% of the QGR
		>=98 % < 99 %		2% of the QGR
		>=95 % < 98%		5% of the QGR
		< 95 %		Maximum of 10 % of the QGR can be imposed
5.	Connectivity to Disaster Recovery Site (With regards to Expanded SDC equipment only)	>= 99.749%	Medium	No Penalty
		>=99 % <99.749%		1% of the QGR
		>=98 % < 99 %		3% of the QGR
		>=95 % < 98%		5% of the QGR
		< 95 %		Maximum of 10 % of the QGR can be imposed
6.	Connectivity with Internet (With regards to equipment only)	>= 99.749%	Critical	No Penalty
		>=99 % <99.749%		1% of the QGR
		>=98 % < 99 %		3% of the QGR
		>=95 % < 98%		5% of the QGR
		< 95 %		Maximum of 10 % of the QGR can be imposed
7.	LAN Availability	>= 99.749%	Critical	No Penalty

Sr	Measurement	Target	Severity	Penalty
	(Active and passive Component, with regards to Expanded SDC equipment only)	>=99 % <99.749%		2% of the QGR
		>=98 % < 99 %		5% of the QGR
		>=95 % < 98%		8% of the QGR
		< 95 %		Maximum of 10 % of the QGR can be imposed
8.	Restore the backed up databases/ applications etc. to be initiated within 2 hours of request	Full Restore	Medium	1% of the QGR for > 5 violations of service parameter on every QGR
9.	Scheduled downtime for Preventive maintenance Per Week • 1am to 3am on Sundays • Any further requirement for scheduled downtime	Notification of >= 7 days in advance	Medium	No Penalty
		Notification of less than 7 days		0.5% of the QGR

Note: Equipment Availability Related penalties shall be governed by the following conditions:

- The Penalty shall be calculated on a quarterly basis.
- If the SLAs drop below the lower limited specified for each component in the table above, it will be governed by the event of default clause as specified under Section VII: General Conditions of the Contract.

2.2.2.2. Physical Infrastructure Service Levels

Table 7: Physical Infrastructure Service Levels

Sr	Measurement	Target	Severity	Penalty
1.	Power Availability (UPS output)	>= 99.749%	Critical	No Penalty
		<99.749% to >= 99 %		2% of the QGR
		>=98% to <99%		5% of the QGR
		>=95% to <98%		8% of the QGR
		<95%		Maximum of 10 % of the QGR can be imposed
2.	PAC system Availability PAC System availability would mean (all PAC's including the standby) temperature and the humidity at the rack	>= 99.749%	Critical	No Penalty
		<99.749% to >= 99 %		2% of the QGR
		>=98% to <99%		5% of the QGR
		>=95% to <98%		8% of the QGR

Sr	Measurement	Target	Severity	Penalty
	level. Temperature to be maintained 20°± 2° at all times Relative humidity to be maintained 50°± 5° at all times	<95%		Maximum of 10 % of the QGR can be imposed
3.	Surveillance: CCTV Availability would include DVR system availability, availability of CCTV recording – 180 days of backup data from the present date	>= 99.749%	Critical	No Penalty
		<99.749% to >= 99 %		0.5% of the QGR
		>=98% to <99%		2% of the QGR
		>=95% to <98%		5% of the QGR
		<95%		Maximum of 10 % of the QGR can be imposed
4.	Complete BMS, system. This parameter applies to any individual component of BMS system, i.e., VESDA, Fire detection, fire suppression, water leak detection, S&EMU, Rodent repellant etc. For any component downtime, the penalty will be applicable	>= 99.749%	Critical	No Penalty
		<99.749% to >= 99 %		2% of the QGR
		>=98% to <99%		5% of the QGR
		>=95% to <98%		8% of the QGR
		<95%		Maximum of 10 % of the QGR can be imposed
5.	Data Center Infrastructure Management (Measure all the components at the end terminal level)	>= 99.749%		No Penalty
		<99.749% to >= 99 %		2% of the QGR
		>=98% to <99%		5% of the QGR
		>=95% to <98%	Critical	8% of the QGR
		<95%		Maximum of 10 % of the QGR can be imposed

2.2.2.3. Civil Work & Minor Works Service Levels

Table 8: Civil Work & Minor Works Service Levels

Sr	Measurement	Target	Severity	Penalty
1	Major Civil Work including the False Flooring, False Ceiling, Doors & Locking, Partitioning, Fire Proofing of all surfaces, Furniture & Fixtures and Painting to be replaced within 2 days of reporting the problem The SI should maintain sufficient inventory to carry out civil and electrical repairs without any disruption to operations.	T days	Critical	No Penalty
		T1 = T + 2 days		0.05% of the QGR for every unresolved call
		T2 = T1 + 2 days		1% of the QGR for every unresolved call
		>T2		2% of the QGR

Sr	Measurement	Target	Severity	Penalty
	For critical items, the Resolution time shall be mutually agreed by the State and the SI at the time of award of contract. T shall be the agreed Resolution (All aspects of the Physical Data Center)			for every unresolved call
2	Minor Civil Work including Cement Concrete Work, Masonry Work, Trench Work, Storage, Glazing and Scaffolding Work to be carried within 4 days of the reporting problem	T= 2 days	Low	No Penalty
		T1 = T + 2 days		0.05% of the QGR for every unresolved call
		T2 = T1 + 2 days		1% of the QGR for every unresolved call
		>T2		2% of the QGR for every unresolved call

2.2.2.4. Helpdesk Service Levels

Time in which a complaint / query is resolved after it has been responded to by the IT service management. In the Help desk Services SLA, if the SI does not resolve any logged incident for more than the allowed resolution time, then the SI is advised to escalate that criticality of the incident to next higher level

Table 9: Helpdesk Parameters for response time

Sr	Type of Incident	Target	Penalty
1.	Critical	T=5 minutes	No Penalty
		T1=T+10 Min	0.5% of the QGR for every unattended call
		T2=T1+15 Min	1% of the QGR for every unattended call
		>T2	2% of the QGR for every unattended call
2.	Medium	1 Hour	No Penalty
		>1 hr and <= 3 hr	1% of the QGR for every unattended call
		>3 hr	2% of the QGR for very unattended call
3.	Low	2 Hour	No Penalty
		>2 hr and <=4 hr	1% of the QGR
		>4hr	2% of the QGR
4.	Application Monitoring Fault Reporting to user departments in case of application unavailability	15 Min	No penalty
		>15 Min and <=30 Min	0.5% of the QGR
		>30 Min	1% of the QGR for every delay

Sr	Type of Incident	Target	Penalty

Table 10: Helpdesk Services SLA for Resolution time

Sr	Type of Incident	Target	Penalty
	Critical	T=30 minutes	No Penalty
		T1=T+ 1 hr	0.5% of the QGR for every unattended call
		T2=T1+1 hr	1% of the QGR for every unattended call
		>T2	2% of the QGR for every unattended call
	Medium	One day from the time of incident logged at the help desk	No Penalty
		>1 day and <= 2 days	1% of the QGR for every unattended call
		>2 days	2% of the QGR for very unattended call
	Low	<= 2days from the time of response logged	No Penalty
		>2 days and <=4 days	0.5% of the QGR for every unattended call
		>4 days	1% of the QGR for every unattended call

2.2.2.5. Compliance and Reporting Process Service Levels

Table 10: Reporting Process Service Levels

Sr	Measurement	Target	Severity	Penalty
1	Submission of MIS reports. The SI shall submit the MIS reports as	Report for previous month to be submitted by 7th of next Month	Medium	1% of the QGR for every 1 day of delay in submission of incremental basis to

	requested by SIA			a maximum of 5%
2	Implementing Change Requests: The SI would implement approved change request within 2 days of its approval	100% of all approved change requests	Medium	1% of QGR for >5 violations of Service Parameter
3	Customization of EMS reports	Customized reports shall be created and submitted within 7 days from date of request submitted by SIA.	Medium	1% of QGR for every 7 days delay in submission of customized reports to a maximum of 10% of QGR.

These SLAs would be calculated for each of the following types of incidences:

- Virus Attack
  Any virus infection and passing of malicious code shall be monitored at the gateway level or user complains of virus infection shall be logged at the help desk system and collated every quarter.
- Denial of Service Attack
  Non availability of any services shall be analyzed and forensic evidence shall be examined to check whether it was due to external DoS attack.
- Intrusion
  Compromise of any kind of data hosted by SDC
  - SPAM statistics on monthly basis shall be monitored through reports generated by Anti-SPAM software.
  - Any other security related threat

Table 11: Security and Incident Management Service Level

Sr	Incidents	Penalty
1	For every virus attack reported and not resolved within 24 hours from the time of patch or virus removal tool/process is available	Rs. 10,000
2	For every incidence of Denial of service attack	Rs. 200,000
3	For every incidence of DataTheft/Destroy/compromised on data Integrity (Compromise of any kind of data hosted by SDC)	Rs. 5,00,000 (In addition to any other penalty, punishment applicable under the legal provisions of the Country and the State prevailing at that point in time.)
4	Host level Intrusion	Rs. 2,00,000

5	Web Defacement	Rs 10,00,000
6	Ransomware Incident	Rs 5,00,000
7	Missing a security incident alert of critical nature	Rs 1,00,000/- per incident

2.2.2.6. Cloud Management Related SLA

Table 12: Virtual infrastructure related Service Levels

S.No	Measurement	Target	Severity	Penalty
1.	Provisioning and De-provisioning of Virtual Machines	Within 30 Minutes after the approval of the request by the concerned Authority	Medium	0.5% of the QGR for every 1 hours or part delay beyond the target time. To the maximum capping of 5 hrs. Beyond 5 hours, 1% of the QGR for every 1 hour.
2.	Uptime of Cloud Solution including the individual Cloud Solution Modules	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR
3.	Overall Cloud Solution Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR Overall Cloud Solution Availability will be measured by following formula: Availability %age = {(Agreed Service Time – Subsystem Down Time)/ (Agreed Service time)*(100%). ** Scheduled downtime will be excluded.

S.No	Measurement	Target	Severity	Penalty
4.	Cloud Network Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service time for the component)*(100%)
5.	Cloud Virtualization Layer Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service time for the component)*(100%)
6.	Cloud Storage Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service time for the component)*(100%)
7.	Virtual Operating System Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR The component availability will be measured by following formula:

S.No	Measurement	Target	Severity	Penalty
				Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service)}
8.	Cloud Orchestration layer Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service time for the component)}*(100%)
9.	Cloud Security layer Availability	99.749%	Critical	99.25% – 99.749% - 1% of QGR 98.75% - 99.25% - 2% of QGR Subsequently, every 0.5% drop in SLA criteria - 2% of QGR The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service time for the component)}*(100%)
10	Data/VM Backup success per day	100% 96-99% 90-95.9%	Critical	No penalty 1% of QGR 5% of QGR

2.2.2.7. Patch Management related SLA

Table 13: Patch Management SLA

Measurement	Target	Severity	Penalty
Patch Management	Critical Patches to be implemented within 10 days of patch release	Medium	0.05% of QGR
	Non Critical Patches to be implemented within 15 days of patch release	Low	0.01% of QGR
	Optional Patches to be implemented within 30 days of patch release	Low	0.01% of QGR

2.2.2.8. Application monitoring Service Levels

These SLAs would be calculated for each of the following types of incidences:

Table 14: **Application monitoring Service Levels**

Sr	Measurement	Target	Severity	Penalty
1	Application monitoring system should alert the system administrator of any application outage within 10 min	<11 minute	Critical	No penalty
		11-30 minutes		0.5% of QGR
		>30 minutes to <=2 hours		1% of QGR
		>2 hours		5% of QGR
2	If a part of the application is non Functional or a service is not running, the system should monitor and alert within 1 hour	< 1 hour	Medium	No penalty
		1 hour to 4 hour		0.1% of QGR
		4 hour to 8 hour		0.5% of QGR
		>8 hours		2% of QGR

2.2.2.9. Non Closure Service Levels

The selected bidder shall be responsible for maintaining CAPA tracker and if any of the issue related to policy implementation or modification or closure of identified issues by TPA/PMU, STQC auditors or ISO/IEC auditors or SIA or SI which are not part of service SLA kept open for more than stipulated time frame as given below penalty will be applicable as below. The criticality of the issue will be determined by external auditors or consultants or after mutual consent between selected bidder and SIA.

Sr	Measurement	Target	Severity	Service Level Down
1	All open issues to be closed within targeted timeline	<7 days	Critical	No penalty
		>7 days to <15 days		0.5% of QGR
		>15 days to <30 days		1% of QGR
		>30 days		5% of QGR
		<30 days	Medium	No penalty
		>30 days to <60 days		0.1% of QGR
		>60 days to <90 days		0.5% of QGR
		>90 days		2% of QGR

2.2.2.10. Manpower Resources Service Levels

In cases where 24x7 man power is not available the support personnel should be available over phone. On critical situations or when directed by SIA, the support personnel must be available on site within 3 hours of request from SIA.

Non availability of the support personnel as stated above will be treated equivalent to single occasion downtime for critical components. The manpower deployed by the SI should be on rolls of the respective SI and not contracted or outsourced personnel.

Table 15: Manpower Service Level

Measurement	Target	Severity	Penalty
Resource availability for all services requested under Operations and Maintenance Resource availability would be calculated as: (No. of shift days for which resource present at the designated location / Total No. of shift days) x 100	>= 99% averaged over all resources designated for System Integration (Data Center Operations) services and calculated on a quarterly basis	Critical	No Penalty
	< 99% to >= 97% averaged over all resources designated for System Integration (Data Center Operations) services and calculated on a quarterly basis		2% of QGR
	< 97% to >= 95% averaged over all resources designated for System Integration (Data Center Operations) services and calculated on a quarterly basis		5% of QGR
	< 95% to >= 90% averaged over all resources designated for System Integration (Data Center Operations) services and calculated on a quarterly basis		8% of QGR
	< 90% averaged over all resources designated for System Integration (Data Center Operations)		Maximum penalty may be imposed i.e. 10% of QGR or on actual

Measurement	Target	Severity	Penalty
	services and calculated on a quarterly basis		whichever is higher

Example: to illustrate the manpower availability in case there are there are 3 shifts per day which will have 2 people in shift 1, 1 in shift 2 and 1 in shift 3.

Total shift per day will be = 4 (2 x 1 + 1 x 1 + 1 x 1) per quarter it would be = 360 shifts

In a quarter if two people were not present in shift 1 for 7 days then 2 x 7 = 14 shifts will be considered for the unavailability of manpower.

Uptime % = (shifts in which manpower was available / total number of shifts) x 100

Uptime c1/0 = (1 — 14/360) x 100

Uptime % = 96.11%

TPA will follow the process mentioned above while calculating manpower availability.

- Maximum penalty on manpower is not limited to maximum of 10% of QGR. Manpower related penalty is additional to the penalty applicable for other services. Manpower related penalty will be either as per the SLA or as per actual rates of manpower absent during the quarter and the highest among these penalty will be applicable to the SI.

2.3. SLA Review Process

- Either SIA or SI may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.
- A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.
- The SIA and the SI shall develop an interim solution, if required, and subsequently the permanent solution for the problem at hand. The SI will then communicate the resolution to all interested parties.
- In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section will be applicable.

2.3.1. Penalties are subject to:

i. Maximum of 20% Penalty will be computed on the value of contract (exclusive of taxes).
ii. In the event of exceeding 20% penalty, it will be deemed to be an event of default and termination.
iii. In the case of maximum Penalty of 10% being imposed on the SI for two consecutive QGR, then the performance of the SI will be reviewed and also may be subjected to cancellation of the order for the FMS Period due failure of service level provided by the SI or higher Penalty of 30% will be imposed on the SI due to non-maintenance of Service levels.

SECTION – C

DATE AND TIME SCHEDULE

Table 16: Time Schedule

Sl. No.	Particulars	Date & Time
1	Date of uploading of N.I.T. & other Documents (online) (Publishing Date)	27.11.2017
2	Documents download/sale start date (Online)	27.11.2017
3	Last Date and time of sending the queries (Offline)	01.12.2017 at 16:00 hrs
4	Pre Bid Meeting at WTL Office (Off Line)	04.12.2017 at 11:30 hrs
5	Corrigendum, if any will be published (On Line)	-
6	Bid Submission start date & time (On line)	12.12.2017 at 14:00 hrs
7	Last Date & time of submission of original Demand Draft/Pay Order for cost of Earnest Money Deposit (Off line)	20.12.2017 at 14:00 hrs
8	Last Date & time of submission of original Demand Draft/Pay Order for cost of Tender Documents, in case the bidder did not attend the Pre Bid Meeting (Off line)	20.12.2017 at 14:00 hrs
9	Bid Submission closing date & time (On line)	18.12.2017 at 15:00 hrs
10	Bid opening date & time for Technical Proposals (Online)	20.12.2017 at 15:00 hrs
11	Date of uploading the final list of Technically Qualified Bidder (online) after disposal of appeals, if any	-
12	Date for opening of Financial Bid (Online)	-

SECTION – D

INSTRUCTION TO BIDDER

1. DEFINITIONS

In this document, the following terms shall have following respective meanings:

"**Acceptance Test Document"** means a document, which defines procedures for testing the functioning of installed system. The document will be finalized with the contractor within 7 days of issuance of the Letter of Award.

"**Agreement**" means the Agreement to be signed between the successful bidder and WTL including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.

"**Bidder**" means any firm offering the solution(s), service(s) and /or materials required in the RFP. The word Bidder when used in the pre award period shall be synonymous with Bidder, and when used after award of the Contract shall mean the successful Bidder with whom WTL signs the agreement for supply, install, commission and render services for the systems.

"**Contract**" is used synonymously with Agreement.

"**Contract Price"** means the price to be paid to the Contractor for providing the Solution, in accordance with the payment terms.

"**Contractor**" means the Bidder whose bid to perform the Contract has been accepted byTender Committee and is named as such in the Letter of Award.

"**Default Notice**" shall mean the written notice of Default of the Agreement issued by one Party to the other.

"Installation" Shall means installation of supplied Hardware, System Software, Software and associated accessories, implementation and integration of achieve functional objective define in the RFP.

"**Fraudulent Practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial noncompetitive levels and to deprive WTL/Department of Par& e-Governance and eventually Gov. of W. Bengal of the benefits of free and open competition.

"**Good Industry Practice**" shall mean the exercise of that degree of skill, diligence and prudence which would reasonably and ordinarily be expected from a reasonably skilled and experienced Operator engaged in the same type of undertaking under the same or similar circumstances.

"Government" / "**Government. of W. Bengal**" means the Government of West Bengal.

"**GoI**" shall stand for the Government of India.

"GoWB" means Government of West Bengal

"Installation" means that the laying down and installation of the Solution in accordance with this Contract.

"Personnel" means persons hired by the Bidder as employees and assigned to the performance of the Infrastructure Solution or any part thereof.

"**Similar Nature of Work"** means job related to Video Conferencing facility and other Networking**.**

"Project" means "Revamping & Physical Expansion of West Bengal State Data Center".

"**Project Plan**" means the document to be developed by the Contractor and approved by WTL., based on the requirements of the Contract and the Preliminary Project Plan included in the Contractor's bid. For the sake of clarity, the Agreed and Finalized Project Plan" refers to the version of the Project Plan submitted by the contractor after receiving the letter of Award and the same approved by Webel Technology Ltd. The project plan may be changed/ modified during the course of the project. Should the Project Plan conflict with the provisions of the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

"Services" means the work to be performed by the Bidder pursuant to this Contract, as described in the detailed Scope of Work.

"**Interest rate**" means "364 days Government of India (GoI) Treasury Bills" rate.

"**Law**" shall mean any Act, notification, bye law, rules and regulations, directive, ordinance, order or instruction having the force of law enacted or issued by the Central Government and/or the Government of West Bengal or any other Government or regulatory authority or political subdivision of government agency.

"LOI" means issuing of Letter of Intent shall constitute the intention of the WTL to place the Purchase Order with the successful bidder.

"**Operator**" means the company providing the services under Agreement.

"**Requirements**" shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Contract.

"**PAR**" mean Department of Par& e-Governance

"Service" means provision of Contracted service viz., operation, maintenance and associated services for DEPLOYED SYSTEMS as per Section titled "Scope of Work"

"Termination Notice" means the written notice of termination of the Agreement issued by WTL.

"Uptime" means the time period when specified services are available with specified technical and service standards as mentioned in section titled WARRANTY SUPPORT" **"%Uptime"** means ratio of 'up time' (in minutes) as mentioned in section titled "Warranty support"

"**Service Down Time**" (SDT) means the time period when specified services with specified technical and operational requirements as mentioned in section titled "WARRANTY SUPPORT"" are not available to Gov. of W. Bengal and its user departments and organizations.

"WTL" means Webel Technology Limited a Government. of W. Bengal undertaking.

2. PRE BID MEETING

Pre Bid Meeting will be held on 04.12.2017 at 11.30 hrs at premises of WTL. Bidder can send their queries as per format (Section - N) to Mr. Sunit Bhattabharya (sunit,bhattacharya@webel-india.com) and copy to Manager (Purchase)(wtlpurchase@gmail.com) and Mr. Birojit Paul (birojit.paul@webel-india.com) . Only the queries received within the stipulated date prior to the Pre Bid Meeting will be answered. The entrance to the Pre Bid Meeting will be limited to two persons per bidder and carrying valid authorization letter on official letter head bearing company seal.

3. COST OF BIDDING

The bidder shall bear all costs associated with the preparation and submission of the bid and WTL will no case be responsible for those costs regardless of the conduct or outcome of the bidding process.

4. BID DOCUMENT

Bidder is expected to examine all instructions, forms, terms and requirement in the bid document. The invitation to bid together with all its attachment thereto shall be considered to be read, understood and accepted by the bidder unless deviations are specifically stated in the seriatim by the bidder. Failure to

furnish all information required by the bid document or a bid not substantially responsive to the bid document in every respect may result of the bid.

5. AMENDMENT OF BID DOCUMENT

At any time prior to the deadline for submission of proposals, WTL reserves the right to add/modify/delete any portion of this document by issuance of an Corrigendum, which would be published on the website and will also be made available to the all the Bidder who have been issued the tender document. The Corrigendum shall be binding on all bidders and will form part of the bid documents.

6. MODIFICATION AND WITHDRAWAL OF BID

As per the bidding process available in the tender.

7. LANGUAGE OF BID & CORRESPONDENCE

The proposal will be prepared by the Bidder in English language only. All the documents relating to the proposal (including brochures) supplied by the firm should also be in English, and the correspondence between the Bidder & WTL will be in English language only. The correspondence by fax/E-mail must be subsequently confirmed by a duly signed formal copy.

8. BIDDER'S SOLUTION

The bidders are requested to study the Bill of Material supplied with this document carefully. While working out the solution the bidder has to work with the broad minimum specification provided in the tender documents, conforming to the model, make and Part number (wherever provided). While submitting the bid the bidder has to detail out all components needed to complete the system BOM. The bidder is required quote for each item retaining all major components/sub system detailed and specified. As the contractor will be responsible for smooth functioning of the system, availability of spares during the tenure of the warranty period have to be take care by the contractor to maintain the guaranteed uptime.

9. EARNEST MONEY DEPOSIT (EMD)

The bidder shall furnish an EMD of Rs. 12000000.00 (Rupees One Crore twenty lakhs only) in the form of a demand draft from a Scheduled Bank payable at Kolkata and in favour of Webel Technology Limited. Any bid not accompanied with the EMD shall be rejected. The validity of EMD instrument will be initially 3 months, have to extend, if required.

10. FORFEITURE OF EMD

EMD made by Bidder may be forfeited under the following conditions:

If Bidder withdraws the proposal before the expiry of validity period.

During the evaluation process, if a Bidder indulges in any such activity as would jeopardize the process, the decision of WTL regarding forfeiture of EMD shall be final and shall not be called upon question under any circumstances.

If Bidder violates any of the provisions of the terms and conditions of the proposal.

In the case of a successful Bidder, if Bidder fails to:

a) Accept the work order along with the terms and conditions.
b) Furnish performance security.
c) Violates any of the work conditions of this proposal or indulges in any such activities as would jeopardize the work.
d) Submitting false/misleading information/declaration/documents/proof/etc.

The decision of WTL regarding forfeiture of EMD shall be final and shall not be called upon to question under any circumstances, besides, forfeiture of EMD even the Bidder will be deferred from participating in any job for a period of one year.

11. FORMS AND FORMATS

The various inputs for the Techno Commercial as Financial Bids are to be submitted in the format specified. The bidder shall use the form, wherever specified, to provide relevant information. If form does not provide space for any required information, space at the end of the form or additional sheets shall be used to convey the said information. For all other cases, the bidder shall design a form to hold the required information.

12. LACK OF INFORMATION TO BIDDER

The bidder shall be deemed to have carefully examined the Bid document to his entire satisfaction. Any lack of information shall not relieve the bidder of his responsibility to fulfill his obligation under the bid. If bidder has any queries relating to bid document then he can send the queries before the Pre Bid Meeting.

13. CONTRACT EXECUTION

On receipt of the Letter of Award the contractor should submit a Performance Bank Guarantee (PBG) equivalent to 10% of the total contract value within three weeks from the date of receipt of Letter of Award/Order. The PBG should be valid for six month more than the warranty period. All delivery of the material will have to be completed within 45 days from the date of acceptance of contract and the contractor has to ensure all activities leading to the commissioning of the contract to be completed within 75 days from the date of award. Subsequent to the award of contract, the contractor will have to arrange for the requisite material as per BOM.

14. TIME SCHEDULE FOR DELIVERY & INSTALLATION

The total delivery, installation & commissioning will have to be completed within 6-8 weeks from the date of Order.

15. LIQUIDATED DAMAGE

The job includes the supply and installation of materials mentioned in the tender document. In the event of failure to meet the job completion in stipulated date/time liquidated damage may be imposed on the contractor for sum not less than 0.5% of the contract value for that item/job for each week or part thereof, subject to a ceiling of 10% of the total contract value (including all taxes & duties and other charges). In the event of LD exceeds 10% of the order value, WTL reserves the right to terminate the contract and WTL will get the job completed by any other competent party. The difference of cost incurred by WTL will be recovered from the contractor and PBG will be invoked.

16. LIABILITY

In case of a default on bidder's part or other liability, WTL shallbe entitled to recover damages fromtheContractor.Ineachsuchinstance,regardlessofthebasisonwhichWTLisentitledtoclaimdamagesfromtheContractor(includingfundamentalbreach,negligence,misrepresentation,orothercontractorclaim),Contractorshallbeliablefornomorethan:

- Payment referred to in the Patents and Copy rights clause.
- Liabilityforbodilyinjury(includingdeath)ordamagetorealpropertyandtangiblepersonalpropertylimitedtothatcausebytheContractor'snegligence.
- As to any other actual damage a rising in any situation involving non-performance by Contractor pursuant to or in any way related to the subject of this Agreement, the charge paid by WTL for the individual product or Service that is the subject of the Claim. However, the contractor shall not be liable for
- Foranyindirect,consequentiallossordamage,lostprofits,thirdpartylossordamagetopropertyorlossofordamagetodata.
- ForanydirectlossordamagethatexceedsthetotalpaymentforContractPricemadeorexpectedtobemadetotheContractorhereunder.

17. PATENTS & COPYRIGHT

If a third party claims that a product delivered by the Contractor to WTL infringes that party's patent or copyright, the Contractor shall defend WTL against that claim at Contractor's expense and pay all costs, damages, and attorney's fees that a court finally awards or that are included in a settlement approved by the Contractor, provided that WTL.

- Promptly notifies Contractor in writing of the claim
- Allows Contractor to control and co-operate with Contractor in the defense and any related settlement negotiations.

Remedies: If such a claim is made or appears likely to be made, WTL would permit Contractor to enable WTL to continue to use the product, or to modify it, or replace it with one that is at least functionally equivalent. If Contractor determines that none of these alternatives is reasonably available, WTL agrees to return the product to Contractor on Contractor's written request. Contractor will then give WTL a credit equal to for a machine. WTL's net book value (provided WTL has followed generally accepted accounting

principles for a generally available software product produced by Contractor (Program) the amount paid by WTL or 12 months charges (whichever is lesser) and for materials the amount paid by WTL for the materials. These will be Contractor's entire obligation regarding any claim of infringement.

18. SUSPENSION OF WORK

WTL shall have the power at any time and from time to time by notice to the Contractor to delay or suspend the progress of the work or any part of the work due to any other adequate reasons and on receipt of such notice the contractor shall forthwith suspend further progress of the work until further notice from WTL. The Contractor shall recommence work immediately after receiving a notice to do so from WTL. The whole or any part of the time lost for such delay or suspension shall, if WTL in its absolute discretion thinks fit, but not otherwise, be added to the time allowed for completion.

19. TERMS OF PAYMENT

Payment terms will be on back-to-back basis, i.e., payment will be made only on receipt of payment from relevant customer, i.e., Department of PAR& e-Governance, Government of West Bengal.

20. GOVERNING LAWS

This contract should be governed by and interpreted by Arbitration clause in accordance with Laws in force in India. The courts at Kolkata shall have exclusive jurisdiction in all matters arising under the contract. The selected vendor shall keep himself fully informed of all current national, state and municipal law and ordinances. The selected vendor shall at their own expense, obtain all necessary permits and license and pay all fees and taxes required by law. These will be selected vendor's entire obligation regarding any claim of infringement. The selected vendor hereto agrees that it shall comply with all applicable union, state and local laws, ordinances, regulations and codes in performing its obligations hereunder, including the procurement of licenses, permits certificates and payment of taxes where required. The selected vendor shall establish and maintain all proper records (particularly, but without limitation, accounting records) required by any law, code/practice of corporate policy applicable to it from time to time including records and returns as applicable under labor legislation.

21. CORRUPT OR FRAUDULENT

The Tender Committee requires that the bidders under this Tender observe the highest standards of ethics during the procurement and execution of such contracts. For this purpose the definition of corrupt and fraudulent practices will follow the provisions of the relevant laws in force. The Tender Committee will reject a proposal for award if it detects that the bidder has engaged in corrupt or fraudulent practices in competing for the contract in question. The Tender Committee will declare a firm ineligible, either indefinitely or for a stated period of time, if it at any time determines that the firm has engaged in corrupt and fraudulent practices in competing for, or in executing, a contract.

22. BIDING CLAUSE

All decisions taken by the Tender Committee regarding the processing of this tender and award of contract shall be final and binding on all parties concerned.

The Tender Committee reserves the right:

- To vary, modify, revise, amend or change any of the terms and conditions mentioned above and,
- To reject any or all the Tender/s without assigning any reason whatsoever thereof or to annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder(s) or any obligation to inform the affected bidder(s) of the grounds for such decision.

23. WORKMEN'S COMPENSATION

In every case in which by virtue of the provision of the workmen's compensation Act 1923 or any other relevant acts and rules, compensation to a workmen employed by the contractor, is payable, then this should be done by the Contractor. If WTL is obliged to make any compensation under the said rules and acts, then the amount shall be recovered without prejudice, from the bills and due of the Contractor. WTL shall not be bound to contest any claim made against the Contractor in respect of workmen's compensation.

24. CONTRACTOR'S EMPLOYEES

The Contractor shall comply with the provision of all labour legislation including the requirement of the payment of Wage Act 1936 and the rules framed there under and modifications thereof in respect of men employed by him in carrying out the contract. The Contractor must ensure that he complies with PF, ESI

regulation for all his deployed employees. The Contractor shall see that all authorized Sub Contractors under him similarly complied with the above requirement.

25. SAFETY MEASURES

The Contractor shall in the course of execution of the work take all necessary precaution for the protection of all persons and property. The Contractor shall take adequate measures to protect the work and present accident during the work. In the event of any accident to any person or persons or damage or injury of any description to any person or property due to failure on the part of the contractor in taking proper precautionary measures the contractor shall be responsible for and must make good the loss the damage at his own cost to the satisfaction of the department and employees of the department shall be indemnified from all claims or liabilities arising there from or any expenses incurred on account thereof.

26. EQUIPMENT

All tools & tackles necessary for the work shall have to be procured by the contractor unless other wise specified elsewhere in these tender documents. The equipment used by the contractor for a particular work must be appropriate for the type of work. The contractor shall maintain the equipment used on the work properly so that they are in good working condition. In no case shall the contractor use defective or imperfect equipment in the work. The contractor shall arrange to replace or repair all defective equipment so that the progress of the work is not hampered. No defective equipment should be left at the site of work and the department shall not be responsible for any loss or damage to any of these equipment during the course of the execution of the work.

27. SUB-CONTRACT

The purchaser (WTL) does not recognize the existence of Sub-Contractors. The Contractor's responsibility is not transferable.

28. TERMINATION FOR DEFAULT

WTL may without prejudice to any other remedy or right of claim for breach of contract by giving not less than 30 days written notice of default sent to the contractor, terminate the order in whole or in part. If the contractor materially fails to render any or all the services within the time period specified in the contract or any extension thereof granted by WTL in writing and fails to remedy its failure within a period of thirty days after receipt of default notice from WTL. If the project (delivery, commissioning as well as warranty maintenance support is not carried out according to specification due to deficiency in service as per terms of the contract. In such case WTL will invoke the amount held back from the contractor as PBG.

29. BANKRUPTCY

If the contractor becomes bankrupt or have a receiving order made against him or compound with his creditors or being a corporation commence to be wound up, not being a voluntary winding up for the purpose only or amalgamation or reconstruction, or carry on their business under a receiver for the benefit of their creditors or any of them, WTL shall be at liberty to terminate the engagement forthwith without any notice in writing to the contractor or to the liquidator or receiver or to any person in whom the contractor may become vested and without any compensation to give such liquidator or receiver or other person the option of carrying out the engagement subject to their providing a guarantee for the due and faithful performance of the engagement up to an amount to be determined by WTL.

30. FORCE MAJEURE

It is hereby defined as any cause, which is beyond the control of the Contractor or WTL as the case may be, which such party could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as

- War, Hostilities or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy and civil war.
- Rebellion, revolution, insurrection, mutiny, usurpation of civil or military, government, conspiracy, riot, civil commotion and terrorist area.
- Confiscation, nationalization, mobilization, commandeering or requisition by or under the order of any government or de facto authority or ruler, or any other act or failure to act of any local state or national government authority.
- Strike, sabotage, lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage of power supply epidemics, quarantine and plague.

- Earthquake, landslide, volcanic activity, fire flood or inundation, tidal wave, typhoon or cyclone, hurricane, nuclear and pressure waves or other natural or physical disaster.

If either party is prevented, hindered or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen days after the occurrence of such event. The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered or delayed.

The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure up to its or their performance of the Contract and to fulfill its or their obligation under the Contract but without prejudice to either party's right to terminate the Contract.

No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall.

- Constitute a default or breach of the contract.
- Give rise to any claim fro damages or additional cost or expense occurred by the delay or nonperformance. If, and to the extent, that such delay or nonperformance is caused by the occurrence of an event of Force Majeure.

31. INSURANCE COVERAGE

Appropriate insurance to cover all solution components for the transit period and until the time of its acceptance at the respective site is to be taken by the contractor. As the contractor will carry the risk for the material in his books during transit, the contractor should arrange insurance for the total system as period from the dispatch till Acceptance Test is successfully achieved. Further the contractor is to take all required insurance coverage in respect of all its personnel who shall be working on this engagement.

32. WARRANTY

The Contractor will warranty that products supplied under the contract are newly made and are free from defect sin the design, engineering and workmanship. The Contractor would be responsible for the up keep and maintenance of the infrastructure and necessary deliverables under the scope of work during the entire warranty period, i.e., 60 months from the date of final acceptance of the system by the customer. The Contractor shall not, without the express prior written consent of WTL, assign any third party of the contractor part thereof. Service support for the entire warranty period will be on site and comprehensive (including spares) and free of cost for the entire warranty period.

33. WARRANTY SUPPORT

All items that will be delivered must be warranted for 5 years and must renewable up to 2 (two) more years through AMC contract. The items must be warranted against bad workmanship and manufacturing defects from the date of acceptance of the system whole or part. Services up port for the entire warranty period will be on site and comprehensive (including spares and all other support) and free of cost for the entire warranty period. The bidder should have a call center in Kolkata. The contact details of the call center must be furnished along with the bid. Any call logged with the service center must be given a running docket number to the person reporting the call. The resolution times should be as per the SLA described in thus EFP.

34. PERFORMANCE BANK GUARANTEE (PBG)

As a guarantee for timely delivery, installation and commissioning of equipment as well as performance of on-site warranty support, as mentioned in Bill of Material, from the date of final acceptance of systems and pertaining to proper running of the systems, the bidder will have to submit 10% of the contract value as security in the form of Performance Bank Guarantee from any nationalized bank as per format enclosed (Section – Q).

35. CONTRACTOR'S RESPONSIBILITIES

Refer Section –A (Scope of Work)

36. NO WAIVER OF RIGHTS

Neither the inspection by WTL or any of their agents nor any order by WTL for payment of money or any payment for or acceptance of the whole or any part of the works by WTL, nor any extension of time, nor any

possession taken by WTL shall operate as a waiver of any provision of the contract or of any power reserved to WTL, or any right to damages here in provided, nor shall any waiver of any breach in the contract be held to be a waiver of any other subsequent breach.

37. ENFORCEMENT OF TERMS

The failure of either party to enforce at any time any of the provision of this contract or any rights in respect thereto or to exercise any option here in provided shall in no way be construed to be a waiver to such provisions, rights or options or in any way to affect the validity of the contract. The exercise by either party of any of its rights herein shall not preclude or prejudice either party from exercising the same or any other right it may have hereunder.

38. PERIOD OF VALIDITY OF OFFER

For the purpose of placing the order, the proposals shall remain valid till 180 days. During the period of validity of proposals, the rates quoted shall not change. In exceptional circumstances, WTL may ask for extension of the period of validity and such a request shall be binding on Bidders. WTL's request and the response to such a request by various Bidders shall be in writing. A Bidder agreeing to such an extension will not be permitted to increase its rates.

39. TAXES & DUTIES

- The prices shall be inclusive of all taxes & levies including GST and other statutory duties as applicable. Rate of taxes should be indicated separately in the Price Bid.
- Contract Price specified in Price Bid should be based on the taxes & duties and charges prevailing at the date one day prior to the last date of Bid submission.
- Statutory deduction, wherever applicable, shall be made from invoice as per government rules. Necessary certificate will be issued for such deductions.
- Bidder submitting a bid shall produce valid statutory documents / certificates with respect to GST, Income Tax, ROC, Prof. Tax, Trade Licence, etc. All such documents / certificates shall remain valid on the last date of tender submission.
- In case of inter-state transaction, WTL will provide "Waybill". However, statutory charges, if any will be borne by the bidder.
- GST component of the invoice of the bidder may be kept on hold in case there ia any mismatch / irregularity in GST return filling on the part of the bidder.

40. DISCREPANCIES IN BID

- Discrepancy between description in words and figures, the rate which corresponds to the words quoted by the bidder shall be taken as correct.
- Discrepancy in the amount quoted by the bidder due to calculation mistake of the unit rate then the unit rate shall be regarded as firm.
- Discrepancy in totaling or carry forward in the amount quoted by the bidder shall be corrected.

41. BID DUE DATE

The online tender has to submitted not later than the due date and time specified in the Important Dates Sheet. WTL may as its discretion on giving reasonable notice by fax, or any other written communication to all prospective bidders who have been issued the bid documents, extend the bid due date, in which case all rights and obligations of the WTL and the bidders, previously subject to the bid due date, shall thereafter be subject to the new bid due date as extended.

42. LATE BID

Any proposal received by WTL after the deadline for submission of proposals may not be accepted.

43. OPENING OF BID BY WTL

Bids shall be opened and downloaded in the presence of Tender Committee and Bidder's representative (maximum 2) may attend, which is not compulsory. The bidder's representatives who are present shall sign a register evidencing their attendance and produce necessary authorization. The bidder's name, Bid modifications or withdrawals, discounts and the presence or absence of relevant Bid Security and such other details as WTL office at his/her discretion, may consider appropriate, shall be announced at the opening. WTL shall open the bid security at mentioned time.

44. CONTACTING WTL

Bidder shall not approach WTL officers beyond office hours and/or outside WTL office premises from the time of the Bid opening to the time of finalization of successful bidder. Any effort by bidder to influence WTL office in the decision on Bid evaluation, Bid comparison or finalization may result in rejection of the Bidder's offer. If the bidder wishes to bring additional information to the notice of WTL, it should be in writing.

45. WTL'S RIGHT TO REJECT ANY OR ALL BIDS

WTL reserves the right to reject any bid and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder(s) or any obligation to inform the affected bidder(s) of the grounds for such decision.

46. BID CURRENCIES

Prices shall be quoted in Indian Rupees, inclusive of all prevailing taxes, levies, duties, cess etc.

47. PRICE

- Price should be quoted in the Price Bid format only. No deviation in any form in the Price Bid sheet is acceptable.
- Price quoted should be firm, inclusive of packing, forwarding, insurance and freight charges.
- Percentage/specified amount of taxes & duties should be clearly mentioned otherwise WTL reserves the right to reject such vague offer.
- Price to be quoted inclusive of supply, installation & commissioning charges.

48. CANVASSING

Canvassing or support in any form for the acceptance of any tender is strictly prohibited. Any bidder doing so will render him liable to penalties, which may include removal of this name from the register of approved Contractors.

49. NON-TRANSFERABILITY OF TENDER

This tender document is not transferable.

50. FORMATS AND SIGNING OF BID

The original and all copies of the proposals shall be neatly typed and shall be signed by an authorized signatory(ies) on behalf of the Bidder. The authorization shall be provided by written Power of Attorney accompanying the proposal. All pages of the proposal, except for un-amended printed literature, shall be initialed by the person or persons signing the proposal. The proposal shall contain no interlineations, erase or overwriting. In order to correct errors made by the Bidder, all corrections shall be done & initialed with date by the authorized signatory after striking out the original words/figures completely.

51. WITHDRAWAL OF BID

Bid cannot be withdrawn during the interval between their submission and expiry of Bid's validity period. Fresh Bid may be called from eligible bidders for any additional item(s) of work not mentioned herein, if so required.

52. INTERPRETATION OF DOCUMENTS

If any bidder should find discrepancies or omission in the specifications or other tender documents, or if he should be in doubt as to the true meaning of any part thereof, he shall make a written request to the tender inviting authority for correction/clarification or interpretation or can put in a separate sheet along with his technical bid document.

53. SPLITTING OF THE CONTRACT AND CURTAILMENT OF WORK

WTL reserve the right to split up and distribute the work among the successful bidders and to curtail any item of work in the schedule partly or fully.

54. PREPARATION OF TENDER

Tender shall be submitted in accordance with the following instructions:

a) Tenders shall be submitted in the prescribed forms. Digital signatures shall be used. Where there is conflict between the words and the figures, the words shall govern.

b) All notations must be in ink or type written. No erasing or overwriting will be permitted. Mistakes may be crossed out and corrections typed or written with ink adjacent thereto and must be initialed in ink by the person or persons signing the tender.
c) Tenders shall not contain any recapitulation of the work to be done. Alternative proposals will not be considered unless called for. No written, oral, telegraphic or telephonic proposals for modifications will be acceptable.
d) Tenders shall be uploaded as notified on or before the date and time set for the opening of tenders in the Notice Inviting Tenders.
e) Tenders subject to any conditions or stipulations imposed by the bidder are liable to be rejected.
f) Each and every page of the tender document must be signed with company seal by the bidder.

55. PRE-DISPATCH INSTRUCTION

All materials / equipment supplied against the purchase order shall be subjected to Inspection, check and /or test by the authorized representative from WTL.

56. FINAL INSPECTION

Final inspection will be carried by the authorized representative from WTL.

57. LOCATION OF DELIVERY, INSTALLATION & COMMISSIONING

WEST BENGAL STATE DATA CENTER, WEBEL BHAVAN, SALT LAKE CITY, KOLKATA - 91.

58. ERASURES OR ALTERNATIONS

The offers with overwriting and erasures may make the tender liable for rejection if each of such overwriting/erasures/manuscript ions is not only signed by the authorized signatory of the bidder. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as “OK”, “accepted”, “noted”, “as given in brochure/manual” is not acceptable. The Customer may treat offers not adhering to these guidelines as unacceptable. The Customer may, at its discretion, waive any minor non-conformity or any minor irregularity in the offer. This shall be binding on all bidders and the Tender Committee reserves the right for such waivers.

59. COMPLIANCE WITH LAW

The contractor hereto agrees that it shall comply with all applicable union, state and local laws, ordinances, regulations and codes in performing its obligations hereunder, including the procurement of licenses, permits certificates and payment of taxes where required.

The contractor shall establish and maintain all proper records (particularly, but without limitation, accounting records) required by any law, code/practice of corporate policy applicable to it from time to time including records and returns as applicable under labor legislation.

60. CLARIFICATION OF BIDS

During evaluation of the bids, the Customer/Tender Committee, at its discretion may ask the bidder for clarification of its bid. The request for the clarification and the response shall be in writing (fax/email) and no change in the substance of the bid shall seek offered or permitted.

61. QUALITY CONTROL

- The contractor is obliged to work closely with WTL act within its authority and abide by directive issued by them on implementation activities.
- The contractor will abide by the safety measures and free WTL from all demands or responsibilities arising from accident/loss of life, the cause of which is due to their negligence. The bidder will pay all indemnities arising from such incidents and will not hold WTL responsible.
- The contractor will treat as confidential all data and information about the system, obtained in the execution of its responsibilities in strict confidence and will not reveal such information to any party without the prior written approval of WTL.
- WTL reserves the right to inspect all phases of contractor’s operation to ensure conformity to the specifications. WTL shall have engineers, inspectors or other duly authorized representatives made known to the contractor, present during the progress of the work and such representatives shall have free access to the work at all times. The presence or absence of representatives of WTL does not relieve the contractor of the responsibility for quality control in all phases.

- The Court of Kolkata only will have the jurisdiction to deal with and decide any legal matters or dispute whatsoever arising out of the contract.

62. DEEMED ACCEPTANCE

Deliverables will be deemed to be fully and finally accepted by WTL/Department of Par& e-Governance in the event WTL/ Department of Par& e-Governance has not submitted such Deliverable Review Statement to Bidder/Implementation Partner before the expiration of the 30-days review period, or when WTL/Department of Par& e-Governance uses the Deliverable in its business, whichever occurs earlier ("Deemed Acceptance").

63. GENERAL TERMS

a) All the pages of the bid document including documents submitted therein must be duly signed and stamped failing which the offer shall be liable to be rejected.
b) All the documents to be submitted by the bidder along with their offer should be duly authenticated by the person signing the offer and if at any point of time during procurement process or subsequently it is detected that documents submitted are forged/tampered/manipulated in any way, the total responsibility lies with the bidder and WTL reserves the full right to take action as may be deemed fit including rejection of the offer and such case is to be kept recorded for any future dealing with them.
c) No Technical/Commercial clarification will be entertained after opening of the tender.
d) Overwriting and erasures may make the tender liable for rejection if each of such overwriting/erasures/manuscription is not only signed by the authorized signatory of the bidder. All overwriting should be separately written and signed by the authorized signatory of the bidder.
e) Quantity mentioned in the tender document is indicative only and orders shall be placed subject to actual requirement. WTL reserve the right to increase or decrease the quantity specified in the tender.
f) WTL reserve the right to reject or accept or withdraw the tender in full or part as the case may be without assigning the reasons thereof. No dispute of any kind can be raised the right of buyer in any court of law or elsewhere.
g) WTL reserve the right to ask for clarification in the bid documents submitted by the bidder. Documents may be taken if decided by the committee.
h) No dispute by the bidders in regard to Technical/Commercial points will be entertained by WTL and decision taken by the Tender Committee will be final.
i) Discrepancy in the amount quoted by the bidder due to calculation mistake, the unit rate shall be regarded as firm and the totaling or carry in the amount quoted by the bidder shall be corrected accordingly.
j) The price offers shall remain firm within the currency of contract and no escalation of price will be allowed.
k) The acceptance of the tender will rest with the accepting authority who is not bound to accept the lowest or any tender and reserves the right to reject in part or in full any or all tender(s) received and to split up the work among participants without assigning any reason thereof.
l) The customer/WTL at its discretion may extend the deadline for the submission of Bids.
m) The Court of Kolkata only will have the jurisdiction to deal with and decide any legal matters or dispute whatsoever arising out of the contract.

SECTION – E

BID FORM

(Bidders are requested to furnish the Bid Form in the Format given in this section, filling the entire Blank and to be submitted on Letter Head in original)

To
Webel Technology Limited
Plot – 5, Block – BP, Sector - V,
Salt Lake City,
Kolkata – 700091.

Sub: Revamping & Physical Expansion of West Bengal State Data Center.

Dear Sir,

1. We the undersigned bidder/(s), having read and examined in details the specifications and other documents of the subject tender no. WTL/PAR/SDC/17-18/030 dated 27.11.2017, do hereby propose to execute the job as per specification as set forth in your Bid documents.

2. The prices of all items stated in the bid are firm during the entire period of job irrespective of date of completion and not subject to any price adjusted as per in line with the bidding documents. All prices and other terms & conditions of this proposal are valid for a period of 180 (one hundred eighty) days from the date of opening of bid. We further declare that prices stated in our proposal are in accordance with your bidding.

3. We confirm that our bid prices include all other taxes and duties and levies applicable on bought out components, materials, equipment and other items and confirm that any such taxes, duties and levies additionally payable shall be to our account.

4. Earnest Money Deposit: We have enclosed EMD in the form of Demand draft for a sum of Rs.12000000/- (DD no. _____ dated _____ drawn on _____).

5. We declare that items shall be executed strictly in accordance with the specifications and documents irrespective of whatever has been stated to the contrary anywhere else in our proposal. Further, we agree that additional conditions, deviations, if any, found in the proposal documents other than those stated in our deviation schedule, save that pertaining to any rebates offered shall not be given effect to.

6. If this proposal is accepted by you, we agree to provide services and complete the entire work, in accordance with schedule indicated in the proposal. We fully understand that the work completion schedule stipulated in the proposal is the essence of the job, if awarded.

7. We further agree that if our proposal is accepted, we shall provide a Performance Bank Guarantee of the value equivalent to ten percent (10%) of the Order value as stipulated in Financial Bid (BOQ).

8. We agree that WTL reserves the right to accept in full/part or reject any or all the bids received or split order within successful bidders without any explanation to bidders and his decision on the subject will be final and binding on Bidder.

Dated, this .....day of 2017

Thanking you, we remain,

Yours faithfully

.....
Signature

.....
Name in full

.....
Designation

Signature & Authorized Verified by

.....
Signature

.....
Name in full

.....
Designation

.....
Company Stamp

SECTION – F

TECHNO COMMERCIAL EVALUATION & AWARDING OF CONTRACT

1. EVALUATION PROCEDURE

- The Eligibility Criteria (Section - B) will be evaluated by Tender Committee and those qualify will be considered for further evaluation.
- The Tender Committee shall verify the Technical Specification (Technical Specification with Compliance Statement, Section – I) Deviation in specification shall not be allowed. Bidder qualified in Technical Specification shall be considered for further evaluation.
- After qualifying in Technical Specification, qualified bidders will only be considered for Financial Bid evaluation.

2. FINAL EVALUATION

Financial Proposal of the bidders qualifying in the evaluation of Technical Specification will be evaluated. The bidder who has qualified in the Technical Specification and returns with lowest quote (L1) in Financial Bid will normally be awarded the contract subject to Post Qualification.

3. AWARDING OF CONTRACT

An affirmative Post Qualification determination will be prerequisite for award of the contract to the most overall responsive bidder. A negative determination will result in rejection of bidder's bid, in which event the WTL will proceed to the next lowest evaluated bidder to make a similar determination of that bidder's capability to perform satisfactorily. WTL will award the contract to the successful bidder whose bid has been determined to be substantially responsive after final negotiation may held with the most responsive bidder, if required. This is a turnkey job in a nature, so bidder(s) to quote all the items mentioned in the tender document, which can ensure single point contact / sole responsibility of the bidder(s) towards project execution. The successful bidder (s) will have to give security deposit in the form of Performance Bank Guarantee.

4. POST QUALIFICATION

The determination will evaluate the Bidder's financial, technical, design, integration, customization, production, management and support capabilities and will be based on an examination of the documentary evidence of the Bidder's qualification, as well as other information WTL deems necessary and appropriate. This determination may include visits or interviews with the Bidder's client's reference in its bid, site inspection, and any other measures. At the time of post-qualification, WTL may also carry out tests to determine that the performance or functionality of the Information System offered meets those stated in the detailed Technical Specification.

SECTION – G

GUIDANCE FOR E-TENDERING

Instructions / Guidelines for electronic submission of the tenders have been annexed for assisting the Bidders to participate in e-Tendering.

1. **Registration of Bidder:**
   Any Bidder willing to take part in the process of e-Tendering will have to be enrolled & registered with the Government e-Procurement System through logging on to **https://wbtenders.gov.in.** The Bidder is to click on the link for e-Tendering site as given on the web portal.

2. **Digital Signature Certificate (DSC):**
   Each Bidder is required to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of tenders from the approved service provider of the National Informatics Center (NIC) on payment of requisite amount. Details are available at the Web Site stated above. DSC is given as a USB e-Token.

3. The Bidder can search & download N.I.T. & BOQ electronically from computer once he logs on to the website mentioned above using the Digital Signature Certificate. This is the only mode of collection of Tender Documents.

4. **Participation in more than one work:**
   A prospective bidder shall be allowed to participate in the job either in the capacity of individual or as a partner of a firm. If, found to be applied severally in a single job all the applications will be rejected.

5. **Submission of Tenders:**
   Tenders are to be submitted through online to the website stated above in two folders at a time, one in Techno Commercial Proposal & the other is Financial Proposal before the prescribed date & time using the Digital Signature Certificate (DSC). The documents are to be uploaded virus scanned copy duly Digitally Signed. The documents will get encrypted (transformed into non readable formats)

The proposal should contain scanned copies of the following in two covers (folders).

Techno Commercial Cover:

Technical Document1 (scanned & join in pdf format then upload)
1. Copy of Demand Draft of Earnest Money Deposit (EMD)
2. Copy of Demand Draft of Tender Fee
3. Bid Form as per format (Section – E)

Technical Document2 (scanned & join in pdf format then upload)
1. N I T Declaration duly stamped & signed in bidder's letter head, Section - Q

Technical Compliance (scanned & join in pdf format then upload)
1. Technical Specification With Compliance Statement (Section – I)
2. Manufacturer Authorisation Form (Section – M)

Financial Cover:
BOQ will be downloaded and same will be uploaded with quoted rates. While uploading BOQ file name shall remain unchanged. Absence of this document shall lead to summary rejection of the bid.

NON-STATUTARY COVER (MY SPACE) CONTAIN FOLLOWING DOCUMENT:
(In each folder, scanned coy will be uploaded with single file having multiple pages)
Table 17: Document List

Sl. No.	Category Name	Sub Category Name	Sub Category Description
A	CERTIFICATES	A1. CERTIFICATES	• GST Registration Certificate • PAN • Document as per Clause no. 5 of Section – B
B	COMPANY DETAILS	B1. COMPANY DETAILS 1	• Document as per Clause – 1 of Section – B
		B2. COMPANY DETAILS 2	• Company Profile (Not more than 3 pages) • ISO Certificate as per Clause no. 12 of Section – B
C	CREDENTIAL	CREDENTIAL 1	• Order copies as per Clause no. 3 & 4 of Section – B
		CREDENTIAL 2	• Product brochure • Other documents, if any
D	DECLARATION	DECLARATION 1	• List of Clients as per format (Section – O) • Financial Capability of Bidder as per format (Section – K)
		DECLARATION 2	• Document as per Clause no. 14 of Section – B • Document as per Clause no. 15 of Section – B
		DECLARATION 3	Bidder's Details as per format (Section – L)
		DECLARATION 4	Technical Capability as per format (Section – J)
		DECLARATION 5	• Declaration as per Clause no.6 of Section – B • Document as per Clause no.8 of Section – B
F	FINANCIAL INFO	P/L & BALANCE SHEET 2014-2015	P/L & BALANCE SHEET 2014-2015
		P/L & BALANCE SHEET 2015-2016	P/L & BALANCE SHEET 2015-2016
		P/L & BALANCE SHEET 2016-2017	P/L & BALANCE SHEET 2016-2017

The hard copy of the total set of documents uploaded in e-Tender site except BOQ to be submitted in sealed envelope to Manager (Purchase), Webel Technology Ltd. before opening of Technical Bid. The envelope superscripted with words "Hard copy of document uploaded against Tender no. WTL/PAR/SDC/17-18/029".

SECTION – H

1. BILL OF MATERIAL

Sr. No.	Components	Qty	Unit
1.00	**Cloud Setup at WBSDC**		
1.01	Cloud compute setup as per requirement along with orchestration layer, cloud management setup & cloud monitoring system with License , O & M and post FAT 24X7 Support for 5 years from software OEM including updates, upgrades and patches for the project period.	1	No.
1.02	Open Hypervisor to create unlimited number of VMs in each the following : 1. Latest DC Edition Windows Based on 2 servers each 2 Pr 14Core or above with support from software OEM including updates, upgrades and patches for the project period. 2. Open source/Openstack Enterprise Linux Virtual Datacenter, based on 10 servers each 2Pr 14Core or above, with support from software OEM including updates, upgrades and patches for the project period.	1	No.
1.03	Automation software with agentless integration capability for 500 no of instances including support for software OEM need to be provided for the project period.	1	Set
1.04	Lifecycle management software for complete updates, upgrades and security patches for the complete OpenStack based Cloud and hypervisor need to be provided. Lifecycle management software for RHEL based instances running on the cloud with 24x7 support from software OEM need to be provided. Lifecycle management software for Microsoft windows server need to be provided.	1	set
1.05	All required licenses of Hypervisor, OS, CALs, orchestration, management, provisioning, monitoring to be included and numbers mentioned clearly explaining the deployment scenario.	1	Lumpsum
1.06	Latest version of Microsoft Windows Server Standard Edition for rack servers as per specification	12	Server
1.07	Latest version of Red Hat Linux Standard Edition for rack servers as per specification	16	Server
2.00	**Server & Server Racks**		
2.01	Server Racks with 2 intelligent PDUs each	28	No.
2.02	Blade servers in minimum two chassis with 100% blade scalability within chassis with converged network connectivity for FC/FCOE/40G connectivity	24	No.
2.03	Two Processor Rack Server for utility service like Backup Server, SMTP gateway, Radius/TACACS+ server, SOC, NOC,EMS, DNS, LDAP/AD, Server Security, AV, AAA server	12	No.
2.04	Four Processor Rack Server	4	No.
2.05	Certificate server for in-house web SSL certificates with latest SSL certificate/ TLS 1.2 for Data Center domain	2	No.

Sr. No.	Components	Qty	Unit
2.06	Open Common Rack	4	No.
3.00	**SAN Storage setup with backup licenses at WBSDC**		
3.01	All Flash Storage Area Network (SAN) - 100 TB	1	No.
3.02	Network backup License for VMs/Servers 40TB File, Database and Archival	150	No.
3.03	SAN Switch	4	No.
3.04	Tape Library with Tapes	1	No.
3.05	Disaster Recovery Management Software (5 licenses for nodes, database and replication)	5	No.
4.00	**Network Setup at WBSDC**		
4.01	Application Switch	4	No.
4.02	Gateway Switch	2	No.
4.03	Data Center Network Management Tool	1	No.
4.04	Spine Switches	2	No.
4.05	DC Access Switch Type 1 - 1/10Gbps Fiber Aggregation for Blade Servers	4	No.
4.06	DC Access Switch Type 2 - 40G Aggregation for Fabric Extender for Fiber and Copper Access Switches for Rack Servers	2	No.
4.07	DC Access Switch Type 3 - 1/10G Copper Access Switches for Rack Server Connections	12	No.
4.08	DC Access Switch Type 4 - 1/10G Fiber Access Switches for Rack Server Connections	12	No.
4.09	10GBASE-SR SFP Module, Enterprise-Class from the same Switch OEM	200	No.
4.10	40GBASE-SR SFP Module, Enterprise-Class from the same Switch OEM	160	No.
4.11	IP KVM Switch	3	No.
4.12	Non IP KVM	15	No.
4.13	Link Load Balancer	2	No.
5.00	**Security Devices for WBSDC**		
5.01	Next Generation Firewall with Intrusion Prevention System	2	No.
5.02	Web Application Firewall & Load Balancer	2	No.
5.03	L7 Anti DDOS setup	2	No.
5.04	URL Filter 100 users	2	No.
5.05	Server Security Solution - 150 Client Licenses	1	No.
5.06	Antivirus for servers -150 licenses	1	No.
5.07	Zero day Protection for Servers-150nos	1	No.
6.00	**EMS Software Licenses as per specifications given**		
6.01	Server, Device & infrastructure health checkup, Device discovery, Monitoring & Management	1	Lumpsum
6.02	Application performance Monitoring (includes Java, .Net and PHP packs)	1	Lumpsum

Sr. No.	Components	Qty	Unit
6.03	Access Management of Server and Network Devices	1	Lumpsum
6.04	Database Performance Monitoring	1	Lumpsum
6.05	Service Desk Management	1	Lumpsum
6.06	Patch Management for windows & Linux	1	Lumpsum
6.07	Asset Management for IT & Non-IT	1	Lumpsum
7.00	**Data Cabling at WBSDC (Data Cable Trays, Conduits, LIUs, Patch Chords, patch panels, CAT6A cabling, Fibre cabling, Termination/Slicing , Junction Boxes, Crimping Tools etc. including all connectors and accessories as necessary)**		
7.01	24 Core Fiber Cassette (MPO) AB/BA Pair Flipped 24 Core fiber MPO LC Cassette, Pair Flipped AB/BA, Multi Mode.	32	No.
7.02	MPO Enclosure 19-inch Rack Mount STRAIGHT patch panel, 1U capacity:- 4MPO Cassette, Multimode UNLOADED Panel to mount MPO/MTP cassettes	24	No.
7.03	24 Core Fiber Cassette (MPO) AB/BA Pair Flipped 24 Core fiber MPO LC Cassette, Pair Flipped AB/BA, Multi Mode.	16	No.
7.04	MPO Enclosure 19-inch Rack Mount STRAIGHT patch panel, 1U capacity:- 4MPO Cassette, Multimode UNLOADED Panel to mount MPO/MTP cassettes	4	No.
7.05	Trunk Cable (MPO-MPO) 5 Meter MPO - MPO Trunk Female cable, 12 Fiber Straight,50./125 , OM4 LSZH Multimode	12	No.
7.06	Trunk Cable (MPO-MPO) 7 Meter MPO - MPO Trunk Female cable, 12 Fiber Straight,50./125 , OM4 LSZH Multimode	8	No.
7.07	Trunk Cable (MPO-MPO) 10 Meter MPO - MPO Trunk Female cable, 12 Fiber Straight,50./125 , OM4 LSZH Multimode	8	No.
7.08	Trunk Cable (MPO-MPO) 15 Meter MPO - MPO Trunk Female cable, 12 Fiber Straight,50./125 , OM4 LSZH Multimode	2	No.
7.09	LC-LC Fiber Duplex Patch Cord OM4 Multimode-2 Meter	40	No.
7.10	LC-LC Fiber Duplex Patch Cord OM4 Multimode-3 Meter	40	No.
7.11	Trunk Cable (MPO-MPO) 15Meter MPO-MPO Trunk Female cable, 12 Fiber straight, 50.125 OM4 LSZH Multimode	4	No.
7.12	Trunk Cable (MPO-MPO) 20Meter MPO-MPO Trunk Female cable, 12 Fiber straight, 50.125 OM4 LSZH Multimode	8	No.
7.13	Trunk Cable (MPO-MPO) 25Meter MPO-MPO Trunk Female cable, 12 Fiber straight, 50.125 OM4 LSZH Multimode	8	No.
7.14	Trunk Cable (MPO-MPO) 30Meter MPO-MPO Trunk Female cable, 12 Fiber straight, 50.125 OM4 LSZH Multimode	8	No.
7.15	Trunk Cable (MPO-MPO) 35Meter MPO-MPO Trunk Female cable, 12 Fiber straight, 50.125 OM4 LSZH Multimode	4	No.
7.16	24 Core Fiber Cassette (MPO) AB/BA Pair Flipped 24 Core fiber MPO LC Cassette, Pair Flipped AB/BA, Multi Mode.	28	No.

Sr. No.	Components	Qty	Unit
7.17	MPO Enclosure 19-inch Rack Mount STRAIGHT patch panel, 1U capacity:- 4MPO Cassette, Multimode UNLOADED Panel to mount MPO/MTP cassettes	28	No.
7.18	Fan-out Cable MTP to LC 6port 15Meter	24	No.
7.19	LC-LC Fiber Duplex Patch Cord OM4 Multimode-1 Meter	200	No.
7.20	LC-LC Fiber Duplex Patch Cord OM4 Multimode-3 Meter	200	No.
7.21	LC-LC Fiber Duplex Patch Cord OM4 Multimode-5 Meter	200	No.
7.22	Cat-6A Patch Cord 3meter 10G supported	200	No.
7.23	Cat-6A Patch Cord 5meter 10G Supported	200	No.
7.24	Cable Management Panel for FOC	24	No.
7.25	Cat-6A Unshielded 48-Ports Patch Panel is fully loaded with Category 6A Keystone Modular Jacks. 10G supported	4	No.
7.26	Cat-6 Patch Cord 2meter 1G Supported	20	No.
7.27	Cat-6A Patch Cord 3meter 10G Supported	96	No.
7.28	Cat-6A Information Outlet with Back Box	10	No.
7.29	Cat-6A UTP Cable Roll of 305 Mtrs	8	Box
7.30	Twinax Cable – 5 Mtr.	50	No.
7.31	Twinax Cable – 10 Mtr.	50	No.
8.00	**IT Setup at Disaster Recovery site at Delhi- NDC**		
8.01	Compute setup as per requirement along with orchestration layer, cloud management setup & cloud monitoring system with License, O & M and Support for 5 years pots FAT. Open Hypervisor to create unlimited number of VMs in each the following: 1. Latest DC Edition Windows Based on 1 servers each 2 Pr 14 Core or above 2. Open source/Open stack Enterprise Linux based on 5 servers each 2Pr 20Core or above All required licenses of Hypervisor, OS, CALs, orchestration, management, provisioning , monitoring to be included and numbers mentioned clearly explaining the deployment scenario. Necessary Blade Chassis to be included.	1	No.
8.02	All Flash Storage Area Network – 120TB	1	No.
9.00	**Civil and Interiors**		
9.01	Civil (Brick Work covering with wall across all the edges, Plaster, Painting, Epoxy Painting, Fire proofing, 1 hour fire rated, Gypsum Partition)	5000	Sq.ft.
9.02	Active tile for High density racks to deliver 1500CFM	8	No.
9.03	Cold Aisle Containment	3	Set
9.04	Vitrified Tiles	1800	Sq.ft.
9.05	False Flooring	3200	Sq.ft.
9.06	Supplying and fixing Double leaf metal doors of Size 1200 mm X 2100 mm with 2 hour Metal fire rating, along with the required framework, Vision Panel, handle, locking system, top patch and bottom patch, hardware, etc. as per the specifications etc. complete.	2	No.

Sr. No.	Components	Qty	Unit
9.07	Single Fire Proof Metal Door min4"	4	No.
9.08	Double Fire Proof Metal Door min 5"	5	No.
9.09	Double Aluminium Door	2	No.
9.10	Single Aluminium Door	2	No.
9.11	Ramp for server room (1500mmX3450mm)	1	Lumpsum
9.12	Civil works - existing Water sprinkler system seal and removal	1	Lumpsum
10.00	**Furniture (NOC, BMS)**		
10.01	Providing and fixing Long back hydraulic gas lift chair for workstations with comfortable arms rest of size 650 mm (L) x 650 mm (D). The height of the chair should be adjustable from 1190 mm to 1300 mm with seat height adjustable from 420 mm to 540 mm. The long back chairs should have aesthetically pleasing and ergonomic design with revolving mechanism	40	No.
10.02	Reception Table	1	No.
10.03	Sofa set three seater	1	No.
10.04	Four set three seater	1	No.
10.05	Center Table	1	No.
10.06	Luggage Scanner	1	No.
10.07	Metal Door Scanner	1	No.
10.08	Manager's Room table	1	No.
10.09	Workstation with cabinet for desktop for NOC each to accommodate 2 no's of 22" inch display	9	No.
10.10	Under table desktop with two display adapter with required cables & accessories for 24/7 operations. Desktop configuration(Intel Core i5 Gen 5, CPU- Min 3GHz, Memory - 8GB, HDD - 1Tb and must have one dual HDMI port)	9	No.
10.11	22" LED displays for NOC tables	18	No.
10.12	dual socket IO points fully wired, for NOC	14	No.
10.13	Commercial Lift upto 2nd floor from ground floor with all civil construction	1	No.
11.00	**IBMS/CCTV : Supply, Installation, Testing and Commissioning of**		
11.01	BMS - adequate IO/connections for required connectivity for all	1	Set
11.02	Indoor Dome camera with power supply & accessories as per specifications	25	No.
11.03	16Ch NVR as per specifications	2	No.
11.04	Mounting Rack for NVR etc.	1	Lumpsum
11.05	Cabling for Camera	1	Lumpsum
11.06	48 port unmanaged switch 100/1000 mbps (Make Cisco/Juniper/HP)	1	Lumpsum
11.07	24" LCD/TFT Monitor for monitoring cameras	1	Lumpsum
11.08	Temperature Sensors	9	No.

Sr. No.	Components	Qty	Unit
11.09	Video Display Wall 3x2 46"/47"	1	No.
11.10	46" /47" LED TV	6	No.
12.00	**Access Control System: Supply, Installation, Testing and Commissioning**		
12.01	TCP/IP based 2 Reader Access Door Controller with Power supply and housing	12	No.
12.02	Finger print biometric reader with smart card reader with accessories for Server room entry	1	No.
12.03	Smart Card reader with Pin for UPS room entry	1	No.
12.04	Smart Card reader with accessories for Server room exit	22	No.
12.05	Exit Push button with accessories for UPS room exit	1	No.
12.06	Smart Cards	25	No.
12.07	Dual leaf 600 lbs electromagnetic lock with inbuilt magnetic contact & Power Supply	8	No.
12.08	Emergency break glass unit with accessories	12	No.
12.09	Access Control with Time & Attendance Software	1	No.
12.10	PC for Access Control Software	1	No.
12.11	6 core x 0.75 sq.mm. shielded armoured cable with accessories	600	Mtrs.
12.12	4 core x 0.75 sq.mm. shielded armoured cable with accessories	700	Mtrs.
13.00	**Water Leak Detection System: Supply, Installation, Testing and Commissioning of**		
13.01	4 Zone Water Leak Detection Panel with Modbus connectivity	3	Lot
13.02	Water Leak detection Cable Sensor – 20 mtrs	1	No.
13.03	Electronic Hooter	3	No.
13.04	2 core x 1.5 Sq. mm FRLS armoured copper cable along with accessories	50	Mtrs.
14.00	**Rodent Repellent System: Supply, Installation, Testing and Commissioning of**		
14.01	Microprocessor based Ultrasonic Rodent Repellent System with stands	3	No.
14.02	Rodent Transducer	49	No.
14.03	Rodent Wire (Connecting Cable) in PVC Conduit	3	Lot
14.04	2 core x 1.5 Sq. mm FRLS armoured copper cable along with accessories	60	Mtrs.
15.00	**Public Address system**		
15.01	6W RMS ceiling mount Speakers	12	No.
15.02	6 zone selection system controller along with microphones	1	No.
15.03	1 CD / DVD Player	1	No.
15.04	12W Volume Controller Unit	1	No.
15.05	Suitable U Rack for housing 1 no. Amplifier, 1 no. main Console, CD Player.	1	No.
15.06	2 core x 1.5 Sq. mm FRLS armoured copper cable along with accessories	250	Mtrs.

Sr. No.	Components	Qty	Unit
16.00	**Fire Alarm System**		
16.01	Addressable fire alarm control panel with 1 loop card and battery backup of 24 hrs in normal condition and 30 min in alarm condition with necessary accessories & BMS implementation/ integration	1	No.
16.02	Addressable Multi sensor type Photo-thermal smoke detector with mounting based LED, Address Switch to program the detectors with accessories	66	No.
16.03	Response Indicator with accessories	29	No.
16.04	Addressable Fault Isolators module with accessories.	5	Lumpsum
16.05	Addressable Control relay modules. (for GRP, ACS, Hooters, PAC, PAS) with accessories	17	No.
16.06	Addressable Manual Call Points with accessories	8	No.
16.07	Addressable monitor modules with accessories (monitoring VESDA, WLD & GRP)	18	No.
16.08	Sounders with strobes with accessories.	12	No.
16.09	2 core x 1.5 Sq. mm FRLS armoured copper cable along with accessories	1600	Mtrs.
16.10	20 mm MS conduit of 2 mm thickness complete with all joints, elbows, fixing accessories etc. as required.	80	Mtrs.
16.11	PC Modulator Controller for setting Alarm temperature.	1	No.
16.12	Analogue Type LHS Cable with dual alarm setting and temperature setting from 70 to 130 Degree C along with restorable feature	2	Mtrs.
17.00	**Fire Suppression System**		
17.01	80 Ltr seamless cylinder with valve	9	No.
17.02	NOVEC 1230 Agent	549	Kgs.
17.03	Master Cylinder Kit with following items: i) Pr. Gauge + Low Pr. Supervisory Switch ii) Electromagnetic Actuator iii) Manual Actuator iv) Pneumatic Actuator v) Flexible Discharge Hose vi) Flexible Actuation Hose	3	No.
17.04	Slave Cylinder Comprising Below Items: i) Pr. Gauge + Low Pr. Supervisory Switch ii) Pneumatic Actuator iii) Flexible Discharge Hose iv) Flexible Actuation Hose	6	No.
17.05	Gas Discharge Nozzles	15	No.
17.06	Seamless Piping with manifold	2	Lot
17.07	Pressure Test Charges	2	Lot
17.08	Gas Release Panel with accessories	3	No.
17.09	Abort Switch	3	No.
17.10	Release Switch	3	No.
17.11	Hooter with Power Supply	3	No.

Sr. No.	Components	Qty	Unit
18.00	**VESDA For Server Farm Area**		
18.01	Aspiration Detector for Server Room	2	Lot
18.02	Power Supply Unit with battery backup	3	No.
18.03	Air Termination nozzles & Capillary tubes	12	Lot
18.04	Piping for Aspiration System	167	Mtrs.
18.05	2 core x 1.5 Sq. mm FRLS armoured copper cable along with accessories	80	Mtrs.
18.06	Items required for integrating the new BMS items with existing BMS system or implementation of separate BMS system	1	lumpsum
19.00	**HVAC**		
19.01	Precision AC (N+1)	6	No.
19.02	Supply and Return Air Grill	1	Lump sum
19.03	Comfort AC (inclusive of Outdoor unit)	10	No.
20.00	**Supply & Installation of Non- IT Infrastructure including warranty cost**		
20.01	200kVA Modular UPS system scalable up to 250 kVA	2	No.
20.02	300 KVA Input Isolation Transformer for UPS	2	No.
20.03	Battery System with 30 minute back up	1	Lumpsum
20.04	20 kVA UPS system with Battery with 30 minute back up.And Cabling with accessories as required	2	No.
21.00	**INTERNAL ELECTRICAL WORKS- New LT DB - 1 no comprising the following**		
21.01	800 Amps 4P 50 kA Incomer MCCB with Microprocessor Based Trip Unit, Under voltage Release for Interlock	3	No.
21.02	400 Amps 4P 50 kA Outgoing MCCB with Microprocessor Based Trip Unit	4	No.
21.03	100 Amps 4P 50 kA Outgoing MCCB with Microprocessor Based Trip Unit	3	No.
21.04	PLC for Changeover and Interlock Logic with Battery Backed SMPS	1	Set
21.05	Wired Floor Standing IP54 Cabinet with i. Copper Busbar/Cable/Wires ii. Type 1 Surge Arresters for Incomer iii. Digital Voltmeter & Ammeter for Incomers iv. RYB Indication	1	Set
22.00	**INTERNAL ELECTRICAL WORKS -Distribution Cabinet for New UPS - 1 no comprising the following**		
22.01	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	3	No.
22.02	160 Amps 4P 25 kA Outgoing MCCB with Microprocessor Based Trip Unit	6	No.
22.03	32 Amps 4P 10 kA MCB	6	No.

Sr. No.	Components	Qty	Unit
22.04	Wired Floor Standing IP54 Cabinet with i. Copper Busbar/Cable/Wires ii. Type 1 Surge Arresters iii. RYB Indication	1	set
23.00	**INTERNAL ELECTRICAL WORKS -Distribution Cabinet for Existing UPS - 1 no comprising the following**		
23.01	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	2	No.
23.02	160 Amps 4P 25 kA Outgoing MCCB with Microprocessor Based Trip Unit	6	No.
23.03	Wired Floor Standing IP54 Cabinet with i. Copper Busbar/Cable/Wires ii. Type 1 Surge Arresters iii. RYB Indication	1	set
24.00	**INTERNAL ELECTRICAL WORKS -Distribution Cabinet for Raw Power - 1 no comprising the following**		
24.01	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	1	No.
24.02	100 Amps 4P 25 kA Outgoing MCCB with Microprocessor Based Trip Unit	9	No.
24.03	Wired Floor Standing IP54 Cabinet with i. Copper Busbar/Cable/Wires ii. Type 1 Surge Arresters iii. RYB Indication	1	set
25.00	**INTERNAL ELECTRICAL WORKS -Distribution Cabinet for Auxiliary UPS - 1 no comprising the following**		
25.01	100 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	2	No.
25.02	32 Amps 4P 10 kA MCB	8	No.
25.03	Wired Floor Standing IP54 Cabinet with i. Copper Busbar/Cable/Wires ii. Type 1 Surge Arresters iii. RYB Indication	1	set
26.00	**INTERNAL ELECTRICAL WORKS -Server DB**		
26.01	160 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	8	No.
26.02	63A 10 kA 3P MCB	24	No.
26.03	32A 10 kA 1P MCB	120	No.
26.04	Wired Floor Standing IP54 Cabinet with i. Copper Busbar/Cable/Wires ii. Type 1 Surge Arresters iii. RYB Indication	8	set
27.00	**INTERNAL ELECTRICAL WORKS -Modification in Existing UPS OP Cabinet**		

Sr. No.	Components	Qty	Unit
27.01	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	1	No.
27.02	Additional Cabinet Section with Copper Busbar/Cable/Wires	1	lumpsum
28.00	**INDUSTRIAL TYPE SOCKETS AND PLUG TOPS: Supply, installation, testing and commissioning of factory made metal clad totally enclosed with cast aluminium housing with industrial socket and socket with scrapping earth connection and plug top. In case of interlocked socket, the interlocking should ensure that the plug cannot be inserted or withdrawn while the switch is in 'ON' position. (all switches & sockets shall be housed in painted MS boxes). The erection rate shall include supply of angle iron frame work and fixing accessories such as grip bolts/grouting/ welding to steel structures etc.,**		
28.01	32A, 230V, 2P+E, IP 44 Male top with socket, Plastic moulded industrial socket with suitable straight plug, Surface mounted / Raceway mounted type. The pricing shall include to make the required supports on the floor/Raceway along with required accessories.	126	No.
28.02	32A, 415V, 3P+E+N, IP 44 Male top with socket, Plastic moulded industrial socket with suitable straight plug, Surface mounted / Raceway mounted type. The pricing shall include to make the required supports on the floor/Raceway along with required accessories.	24	No.
28.03	63A, 230V, 2P+E, IP 44 Male top with socket, Plastic moulded industrial socket with suitable straight plug, Surface mounted / Raceway mounted type. The pricing shall include to make the required supports on the floor/Raceway along with required accessories.	12	No.
28.04	63A, 415V, 3P+E+N, IP 44 Male top with socket, Plastic moulded industrial socket with suitable straight plug, Surface mounted / Raceway mounted type. The pricing shall include to make the required supports on the floor/Raceway along with required accessories.	12	No.
28.05	MODULAR TYPE Supply, erection, testing and commissioning of power points by providing following switches/sockets mounted on suitable size metal coated boxes fixed flush/surface on to the wall with all fixing and wiring accessories -6/16 Amps, 5-pin (230 Volts) single phase universal socket with 16 Amps single pole switch with indicating lamp. The pin configuration shall be round type. Plug tops are included	65	No.
28.06	MODULAR TYPE Supply, erection, testing and commissioning of power points by providing following switches/sockets mounted on suitable size metal coated boxes fixed flush/surface on to the wall with all fixing and wiring accessories -6/16 Amps, 5-pin (230 Volts) single phase universal socket with 16 Amps single pole switch with indicating lamp. The pin configuration shall be round type. Plug tops are included	65	No.
29.00	**SUB-MAINS/CIRCUIT MAINS/POWER WIRING: Supply and running of 1100 V grade FRLS PVC insulated copper conductor wires in 2 mm thick FRLS PVC/ MS conduits as per Technical specification. The rate shall include all wiring & conduit accessories as applicable.**		
29.01	Supply and running of 3Rx1.5 Sqmm FRLS PVC insulated multistrand copper conductor wire in 20mm diameter FRLS PVC conduits for	950	Mtrs.

Sr. No.	Components	Qty	Unit
	lighting circuits from DB to switch boards & emergency lighting circuits from MCB DBs to SBs and light fixtures.		
29.02	Supply and running of 2Rx2.5 Sq. mm + 1Rx1.5 Sq. mm FRLS PVC insulated multistrand copper conductor wire in 25mm diameter FRLS PVC conduits for Raw power circuits (1x6/16A) from DB to Sockets and looping between the sockets	720	Mtrs.
29.03	Supply, running and termination of 1C x 6 Sq. mm Flexible FRLS PVC insulated multistrand copper conductor wire in existing conduits/ raceways.	210	Mtrs.
30.00	**POINT WIRING: FOR LIGHT FIXTURES: POINT WIRING WITH FRLS PVC CONDUITS: (False/Non-False Ceiling Area): Wiring with 2 x 1.5 Sq. mm FRLS PVC insulated 1100V grade copper conductor wires and 1 x 1.5 Sq. mm PVC insulated earth wire up to first light point and 2 x 1.5 Sq. mm FRLS PVC insulated 1100V grade copper conductor wires and 1 x 1.5 Sq. mm PVC insulated earth wire for looping with multiple light fixtures in 2mm thick, 20mm diameter FRLS PVC conduits as per specification. The rate shall include necessary accessories. (SWITCHES & SOCKETS SHALL BE OF MODULAR TYPE)**		
30.01	Single light point controlled by 6A switch (conduit / wires / switches)	21	No.
30.02	2/3/4 light point controlled by 6A switch (combined rate for 2/3 points)	44	No.
31.00	**LT CABLES: Supply, Unloading, Laying, testing & Commissioning of 1.1 KV Grade XLPE insulated & PVC sheathed Copper conductor steel armoured FRLS power cables as per specification. The rates quoted shall be for laying in trays, cable trenches (indoor and outdoor), pipes**		
31.01	Raw power to New LT Panel - 4 C X 400 SQ MM	250	Mtrs.
31.02	4C X 300 sq. mm	800	Mtrs.
31.03	DG Sync panel to New LT panel -4 C X 400 SQ MM	280	Mtrs.
31.04	New LT panel to RPDB (Lighting arrangement) - 4C X 25 Sq mm	150	Mtrs.
31.05	4C x 6Sq mm for LPDB & Utility incoming	150	Mtrs.
32.00	**1.1kV, Copper Conductor, PVC Insulated, Unarmoured, flexible LT Cable. The rates quoted shall be for laying in trays, cable trenches (indoor and outdoor), pipes, end terminations etc.**		
32.01	1C X 185 Sq. mm	570	Mtrs.
32.02	LT Panel to Modular UPS DB incoming - 1C X 150 Sq. mm	2280	Mtrs.
32.03	UPS O/G to SDB - 1C X 150 Sq. mm	250	Mtrs.
32.04	1C X 25 Sq. mm from PAC to earth	210	Mtrs.
32.05	4C X 25 Sq. mm from existing PAC panel to PAC / Existing LT Panel to PAC	900	Mtrs.
32.06	3C X 6 Sq. mm for SDB to Server racks of proposed setup	2940	Mtrs.
32.07	4C X 10 Sq. mm for HD racks	650	Mtrs.
32.08	1C X 6 Sq. mm for racks & pedestal earthing	540	Mtrs.
32.09	4C x 6Sq mm for LPDB & Utility incoming	950	Mtrs.

Sr. No.	Components	Qty	Unit
32.10	4C x 16Sq mm	80	Mtrs.
32.11	1C x 16Sq mm	260	Mtrs.
33.00	**Installation of New DG Sync Panel with Intelligent Breakers with communication at DG Sync Cabinets, to run 3 DG sets in N+1 mode**		
33.01	MCCB 4P/800A/2.0, Motorized, total number to be provided as per requirement for connecting two LT panels	1	Lot
33.02	Breaker ULP chord 1.3 M as per requirement	1	Lot
33.03	IFM (ULP to modbus interface module) as per requirement	1	Lot
33.04	10 Stacking connectors for COM interface as per requirement	1	Lot
34.00	**DG Sync Panel Bypass System & Communication system**		
34.01	GPRS connectivity with Co-map Make, Model RM for SMS alert to operator and also for monitoring through on laptop /PC	3	No.
34.02	By pass System for DG Sync Panel auto system with manual system in case of Controller failure	1	Lot
34.03	Auto synchronization controller make co-map for emergency in case of controller non function.	2	No.
35.00	**EARTHING: Supply & installation of the following with clamps, inspection chambers, excavation, refill with soil, charcoal, sand and salt, compound as per technical specifications & IS: 3043 standards. Complete. The cost shall include excavation, backfilling, compaction, construction of chambers, tools and tackles for excavation & all required civil works. Testing earth resistivity and electrode resistance**		
35.01	40x6 mm GI Strip	270	Mtrs.
35.02	40x6 mm CU Strip with sleeves	270	Mtrs.
35.03	6 SWG CU wires for pedestals	100	Mtrs.
35.04	25x3 mm GI Strip	100	Mtrs.
35.05	25x3 mm CU Strip for SRG	300	Mtrs.
35.06	3 mtrs long 50 mm dia. G.I pipe electrode earth station. The chamber size shall be 450x 450 mm with C.I. cover plate. The identification number shall be provided both inside and outside.	4	No.
35.07	600x600x3.15mm Copper plate electrode earth station. The chamber size shall be 450 x450 mm with C.I. cover plate. The identification number shall be provided both inside and outside.	4	No.
36.00	**SUPPLY & INSTALLATION OF INDOOR LIGHTING FIXTURES - Supply, Erection, Testing & Commissioning of the following light fixtures complete with Energy Efficient Electronic Ballast, Control gear and all the other standard accessories. The light fixtures given in this tender are only indicative of the types required. The Electrical Contractor shall submit samples for final selection and approval.**		

Sr. No.	Components	Qty	Unit
36.01	2x18W Recess mounted indirect /direct LED luminaire, 2x18w LED Tube lamps, having high efficiency diffuser giving more efficiency with duly wired electronic ballast/Power Supply. The cost shall include the lamp and all required mounting & required accessories and other accessories. (Make: Philips/Thorns/Wipro/Syska or Approved equivalent)	40	No.
36.02	2x28W surface mounted type decorative mirror optic luminaire with louvers suitable for 2x28W LED Tube Lamps. The cost shall include the lamp and all required accessories.	20	No.
37.00	**MISCELLANEOUS**		
37.01	**Data Center Infrastructure Management System (DCIM) with accessories**	1	Lumpsum
37.02	**STEEL ITEMS :**Supply, fabrication, erection & epoxy painting of steel items as required as per specification complete, Generally steel items include cable tray, cable tray supporting arrangements, MS Channels-(ISMC), Angles, Plates and any other steel items not covered in other items of schedule of quantities. The cable trays shall be of ladder made of angles and flats / sheet steel folded type. The rate shall also include painting with two coats of red oxide and primer and two coats of synthetic enamel paint of approved shade.	1	Lumpsum
37.03	**PERFORATED TYPE CABLE TRAYS(GI TRAYS)/ WIREWAYS:**Supply, erection, testing & commissioning of the following sizes prefabricated perforated type cable tray made of 14 SWG GI sheet with two coats of red oxide primer and finished with good quality paint with necessary supports, brackets, angle iron, suspension are measured separately the heading "Steel Items"	1.2	M.T.
38.00	**LADDER TYPE CABLE TRAYS(GI TRAYS)**		
38.01	Supply & erection of the following sizes ladder type cable tray, Hot dip galvanized made of 14 SWG GI sheet with two coats of red oxide primer and finished with good quality paint with necessary supports. Brackets, angle iron, suspension are measured separately the heading "Steel Items".	1	Lumpsum
38.02	50X50X300 mm wide	250	Mtrs.
38.03	50X50X600 mm wide	175	Mtrs.
39.00	**PERFORATED TYPE CABLE TRAYS(GI TRAYS)**		
39.01	Supply, erection, testing & commissioning of the following sizes prefabricated perforated type cable tray made of 14 SWG GI sheet with two coats of red oxide primer and finished with good quality paint with necessary supports, brackets, angle iron, suspension are measured separately the heading "Steel Items".	1	Lumpsum
39.02	150(W) x 50 (H) x 2mm (T)	120	Mtrs.
39.03	300(W) x 50 (H) x 2mm (T)	290	Mtrs.
39.04	450(W) x 50 (H) x 2mm (T)	70	Mtrs.
40.00	**Supply and fixing of the following charts / drawings duly Laminated**		
40.01	Single line diagram & Escalation Matrix	3	No.
40.02	Rubber Mating 1M x 1M X 12mm	30	No.

Sr. No.	Components	Qty	Unit
40.03	Media Safe - 300 ltr	2	No.
40.04	Multi-Function Printer	2	No.
40.05	LCDprojectorwith Hi Life LED Lamps , HDMI/SVGA - 3000 Lumen	1	No.
41.00	**Installation Charges**		
41.01	Installation charges for IT Infrastructure	1	lumpsum
41.02	Installation charges for Non- IT Infrastructure, including BMS, Electrical equipment, CIVIL works etc.	1	lumpsum
42.00	**Support Cost**		
42.01	FM Cost for 5 Years as per requirement mentioned in RFP	1	No.
42.02	AMC/ Support Cost for IT (software and hardware) equipment for 5 years.	1	No.
42.03	AMC/ Support Cost for Non-IT equipment for 5 years.	1	No.
43.00	**Any other component (Hardware, Software or otherwise) required for implementation, commissioning of the above items.**	1	No.

Note:

- **Bill of quantity may change at the time of ordering.**
- **Cable charge will be raised on basis of at actual laying of cable.**
- **Detailed Technical Specifications are given in Section–I**

2. TECHNICAL SPECIFICATION WITH COMPLIANCE STATEMENT

(Tender No. WTL/PAR/SDC/17-18/030)

2.1. Proposed Technical Solution

2.1.1. Architecture

The bidder should follow the below architecture for WBSDC expansion set up architecture is derived from the existing architecture of WBSDC and with the envisaged requirements highlighted with IT system. The architecture depicts the broad functions WBSDC, the various system and inter-linkages between them. System Integrator will Supply, install, integrate and Commission the new expansion server farm area and at the end of the contract tenure, will hand over the DC set up to WTL.

Both existing and new infra setup on the second floor will use the EMS and BMS components comprises of the CCTV surveillance, Access control, Fire detection and Suppression control, Integration with DG, UPS and the other standalone devices, VESDA, Water leak detection, Rodent repellent etc. It is required to integrate all the existing EMS and BMS systems in the new expanded Data Center to that of the existing Data Center in the 1st Floor. Finally the existing setup has to get migrated with applications and data to the new setup seamlessly with minimum possible planned downtime.

The detailed technical requirements of IT and Non IT infrastructure, interfaces with other systems/stakeholders and data exchange requirements are covered in the subsequent sections.

2.1.2. Technical Requirements

2.1.2.1. Brief description

As a part of this project, SI would be required to undertake the following IT Infrastructural upgrade at WTL. The requirements have been classified as follows:-

- Procurement and deployment of IT and Non IT devices
- Installation and commissioning of the IT and Non IT Infrastructure including Civil modifications as per requirement of the site.

2.1.2.2. Supply of IT Components

The bidder will supply the required IT Infrastructure components as per but not limited to the BOM along with technical specifications of which are given below.

2.1.2.2.1. Storage

The shortlisted bidder to provide SAN of 120 TB usable capacity after RAID 6 Configuration. The functionalities of the configuration are detailed in the technical specifications below in the document

2.1.2.2.2. Racks

The bidder should supply the racks with uniform and compact sizes leverage to optimized floor space usage. Each of the server racks should be supplied with intelligent PDUs as per the specification given in subsequent sections. The required rack details given below:

Server Racks 750-800mmX1070-1100mmX 42U- 28 units

2.1.2.2.3. Enterprise Management System

The bidder should supply and install the Monitoring software licenses as per the requirement given in the Bill of material.

2.1.2.2.4. Building Management System

The bidder should supply the below listed BMS items as per the BoM.

- VESDA
- CCTV Dome Camera
- Video streamer
- Gas Based Fire Suppression System integration
- Access control – Pin and biometric reader (two factor authentication)
- Temperature Sensors
- Public Addressing System
- Water leak detection system
- Rodent repellent and pest control system

2.1.2.2.5. Power Systems:

The bidder needs to provide a separate L.T panel as per specification with all accessories, which will provide supply to the systems at Data Center and this new L.T Panel (in the 1st floor expansion area) will work together with the existing L.T. Panel (in the 1st floor) to have a redundant power supply system. The input of the same will have to be taken from raw power source/ transformer of the building (in the Ground floor) and output of the same will be given to UPS systems, PAC systems and other equipment as required.

The power distribution units at the rack level also need to have real time remote monitoring capability.
A separate electrical room (in the 1st floor expansion area) will have to be setup with New LT Panel, New modular UPS system along with batteries. There will be redundant i-PDU which will be responsible for supply of power to the racks and devices. The redundant i-PDU will have power from 2 different LT Panels and UPS System. The bidder need to asses and design the electrical layout for the same for better resiliency and redundancy. The Data Center Infrastructure management tool will be responsible for analyzing the power at the PDU Level.

2.1.2.2.6. Data Center Infrastructure Management Tool

The Tool used to monitor all the Non IT Components of the Data Center infrastructure including the electrical Infrastructure. It should provide a comprehensive report on the Power Usage effectiveness, monitoring the power distribution at the PDU level.

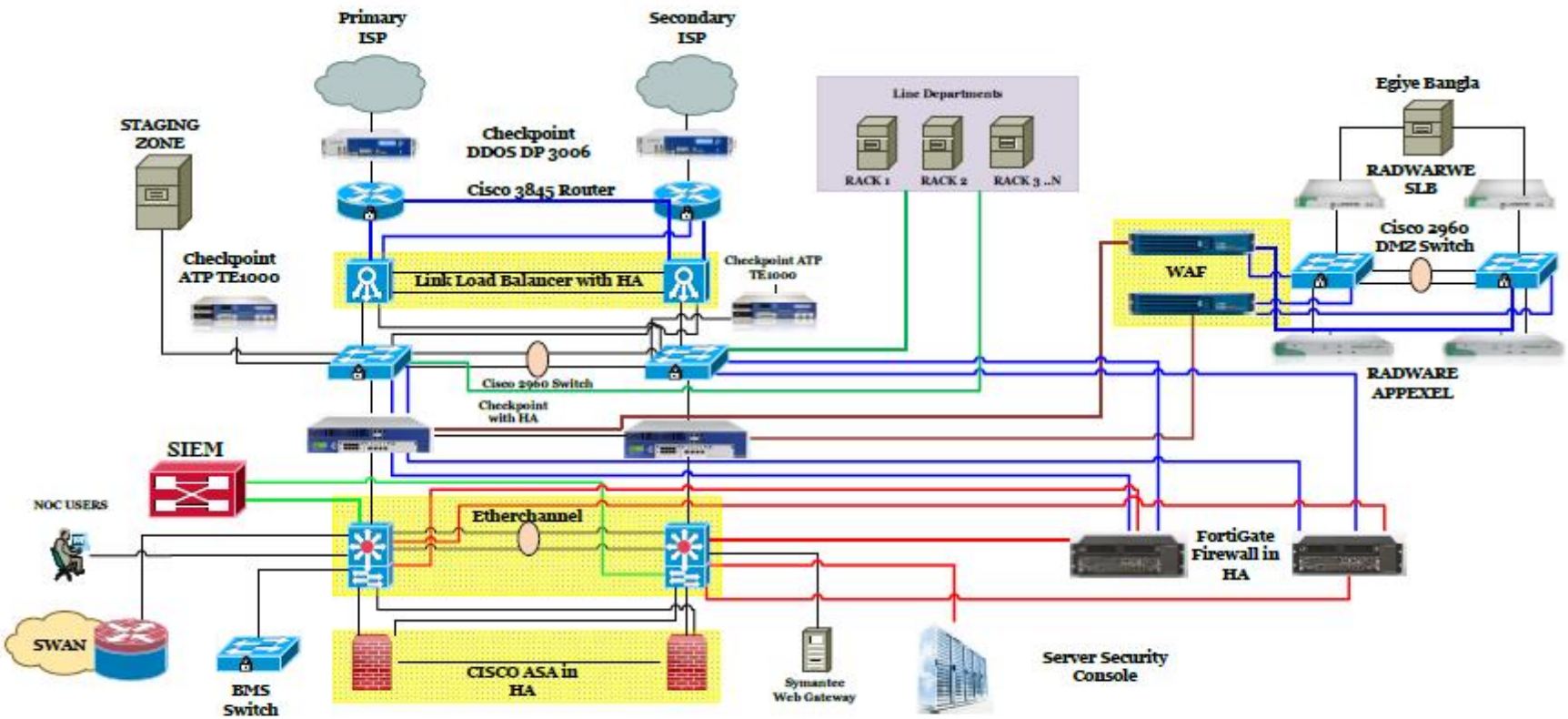
At a high level, DCIM shall be used for many purposes such as it should support data center availability and reliability requirements, it should identify and eliminate sources of risk to increase availability of critical IT systems, it should be used to identify interdependencies between facility and IT infrastructures to alert the facility manager to gaps in system redundancy, and it should assist in modeling the costs structures of building and maintaining the huge accumulation of assets which form the data center, over long periods of time.

DCIM shall be enabled to measure energy use, enabling safe operation at higher densities.

3. Proposed Physical Layout

Tentative Layput for the xxpansion phase. Detail Layout will be freezed during Implementation period.

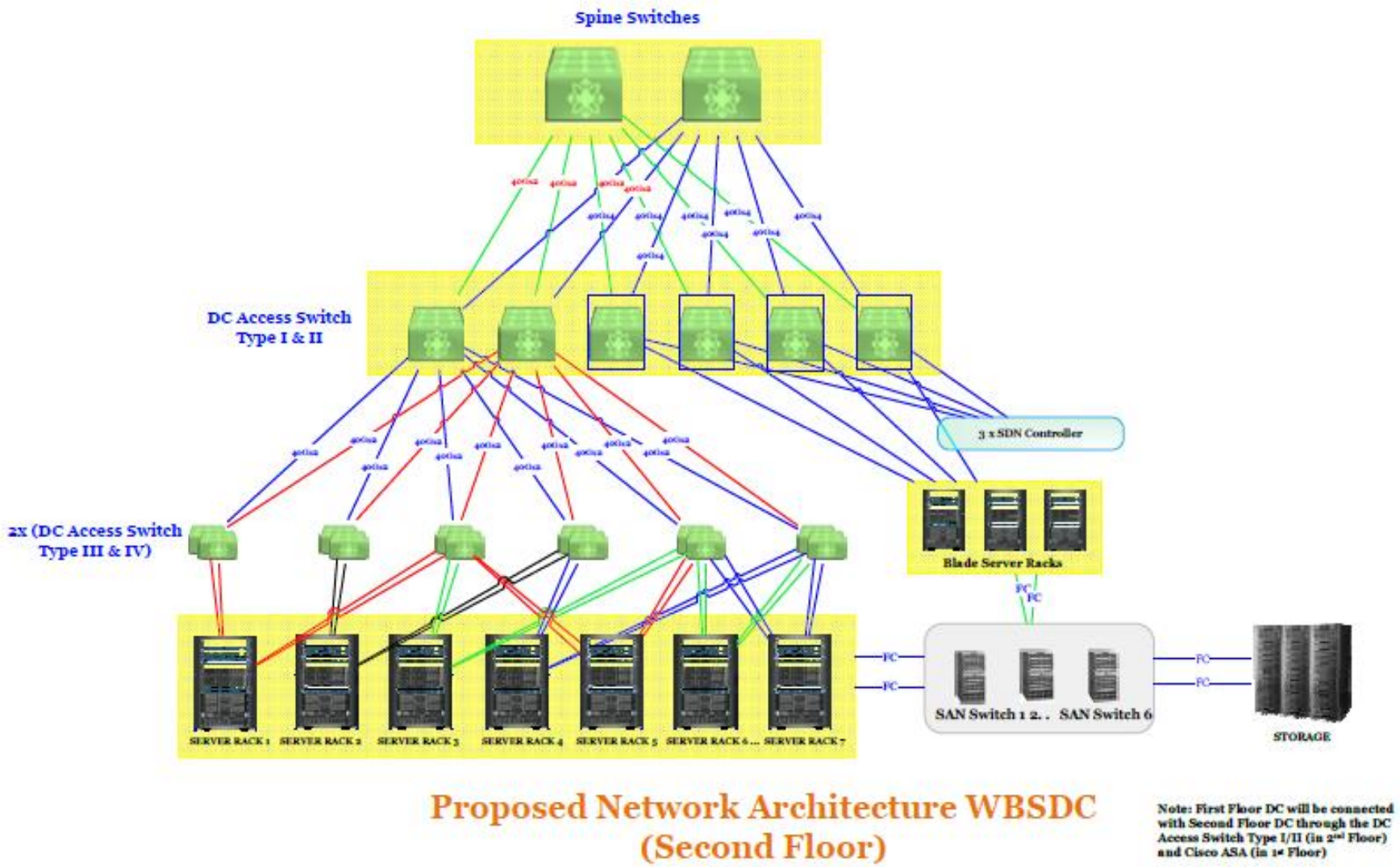
4. Proposed Network Layout



Proposed Network Architecture WBSDC (First Floor) with Existing setup

Note: Second Floor DC will be connected with First Floor DC through the Cisco ASA (in 1st Floor) and DC Access Switch Type I/II (in 2nd Floor)

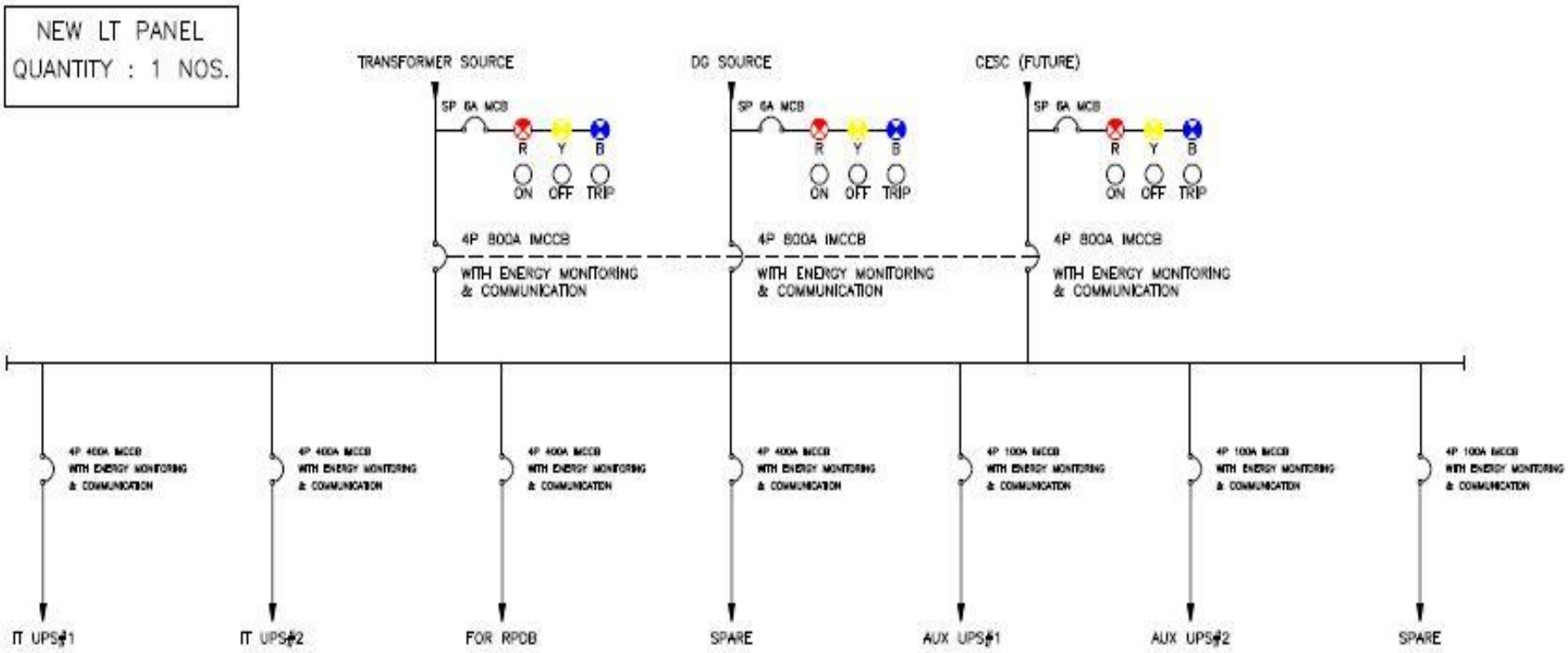
4.1. The Logical Architecture with distribution from the Server Farm Switch



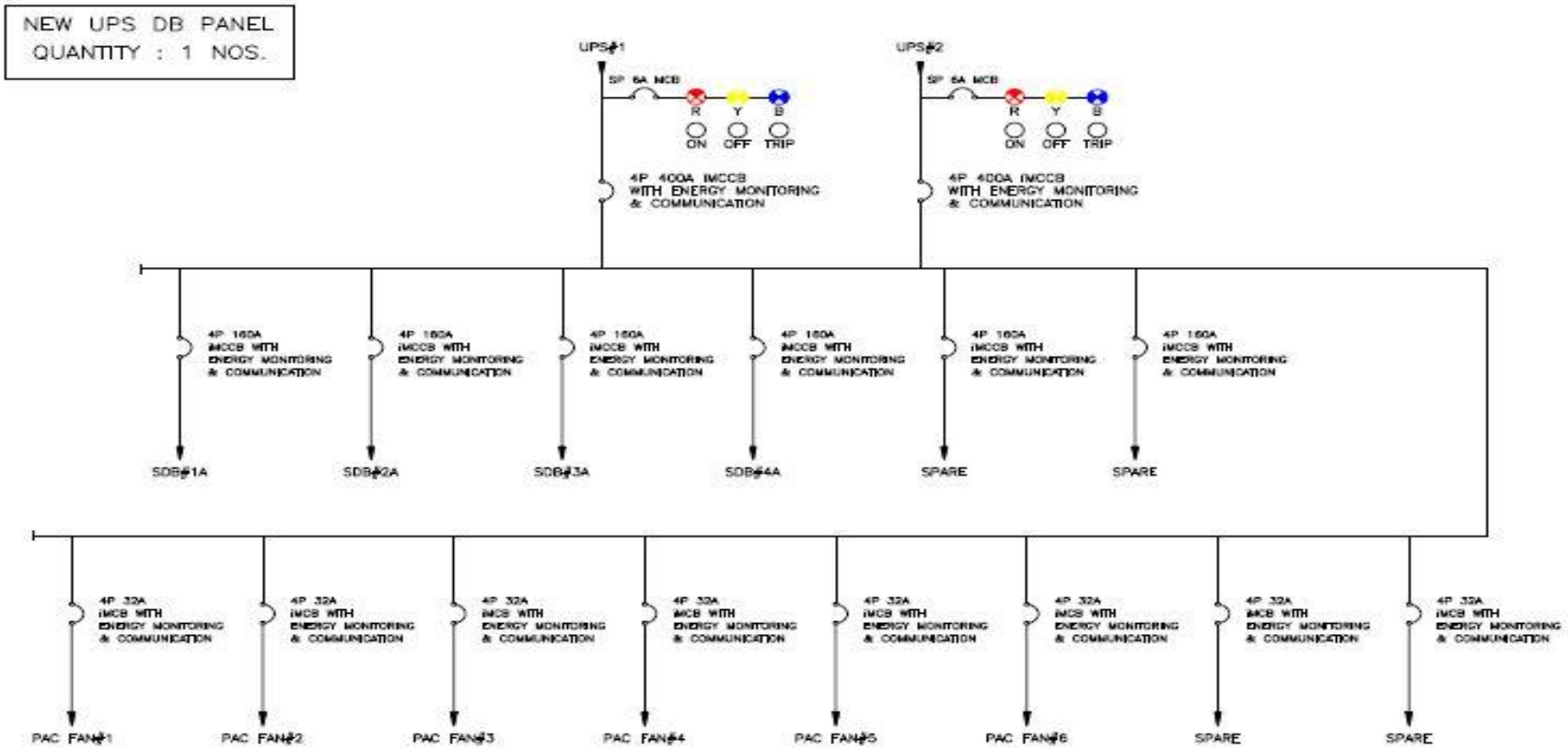
Note: Tentative Network Architecture for the expansion phase. Detail architecture will be freezed with the shorlisted bidder during Implementation period.

5. Electrical Setup Single Line Diagram

5.1. New LT Panel for 2nd Floor

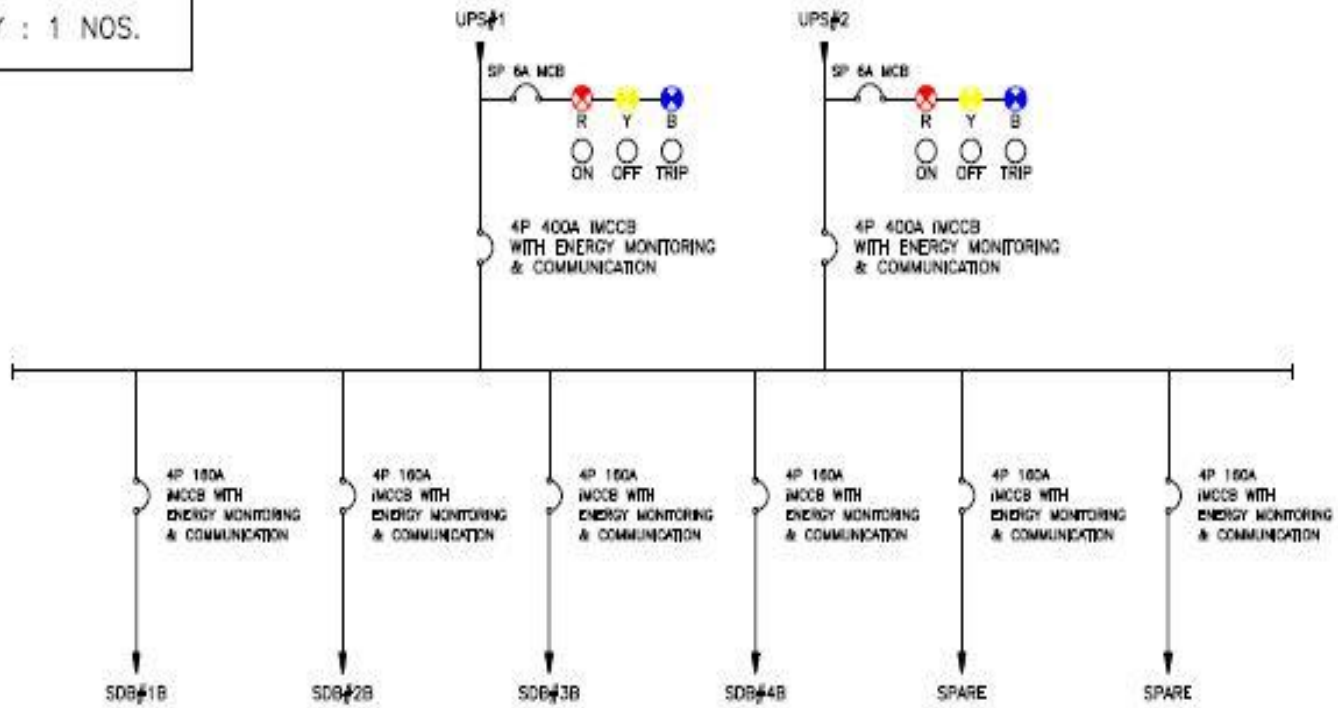


5.2. New UPS DB Panel

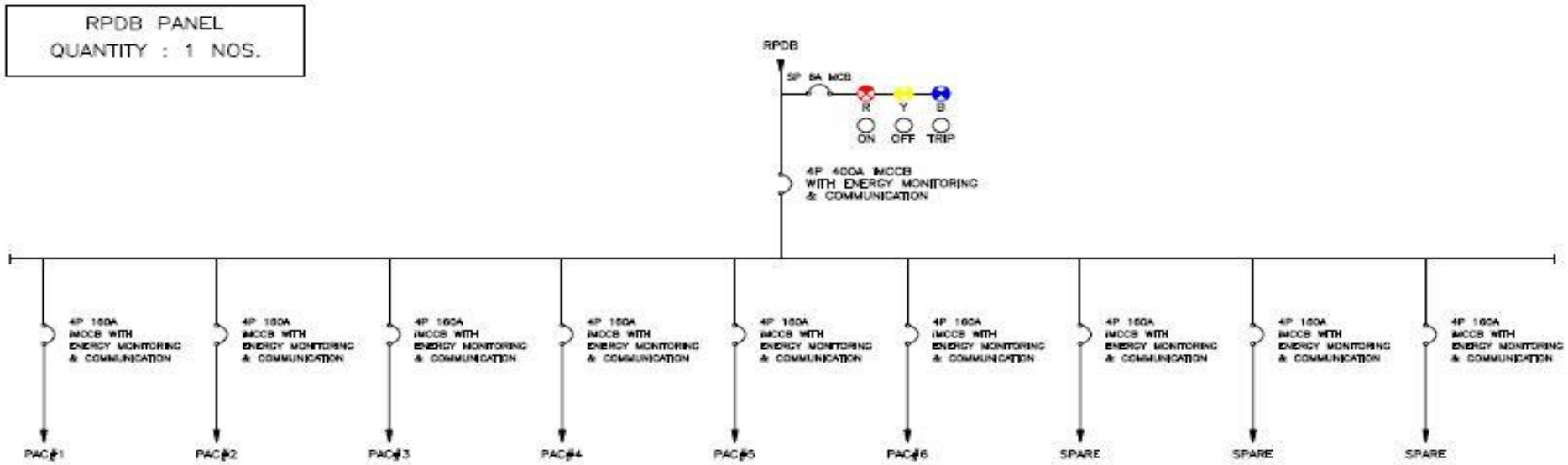


5.3. Existing UPS DB Panel

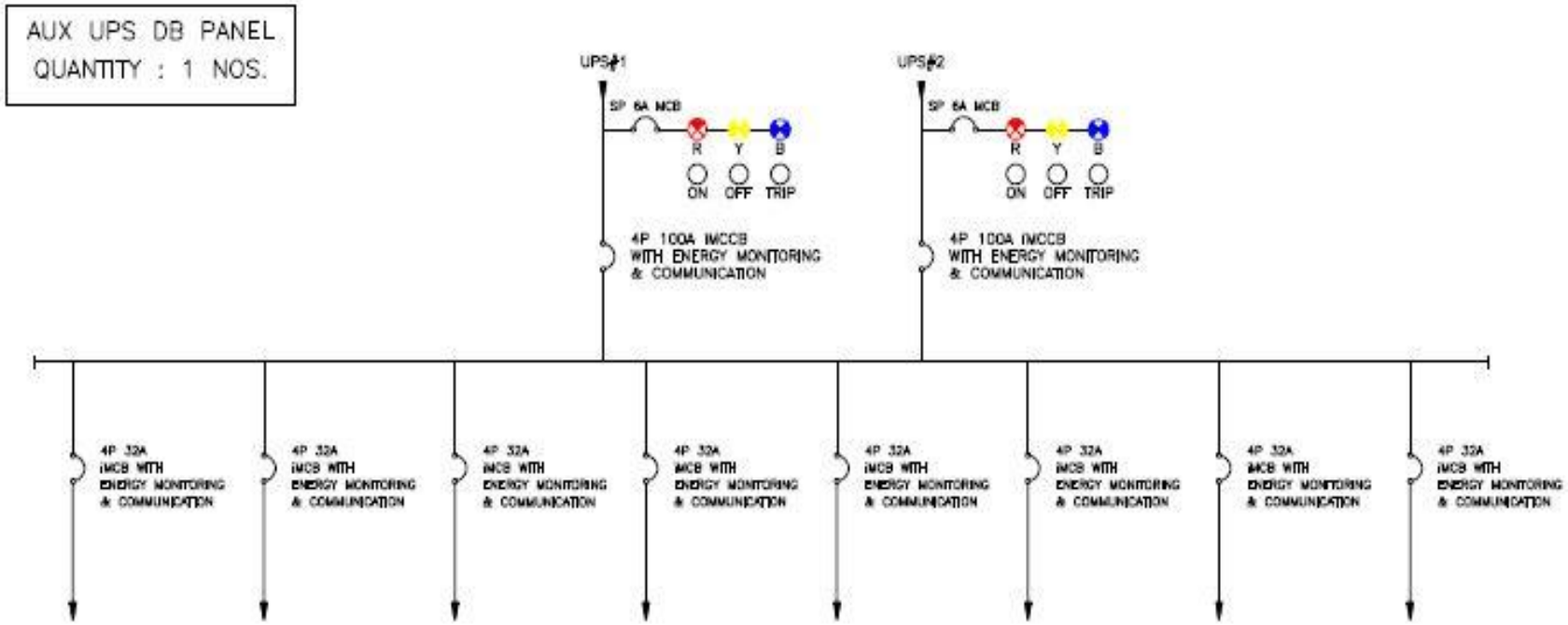
EXISTING UPS DB PANEL
QUANTITY : 1 NOS.



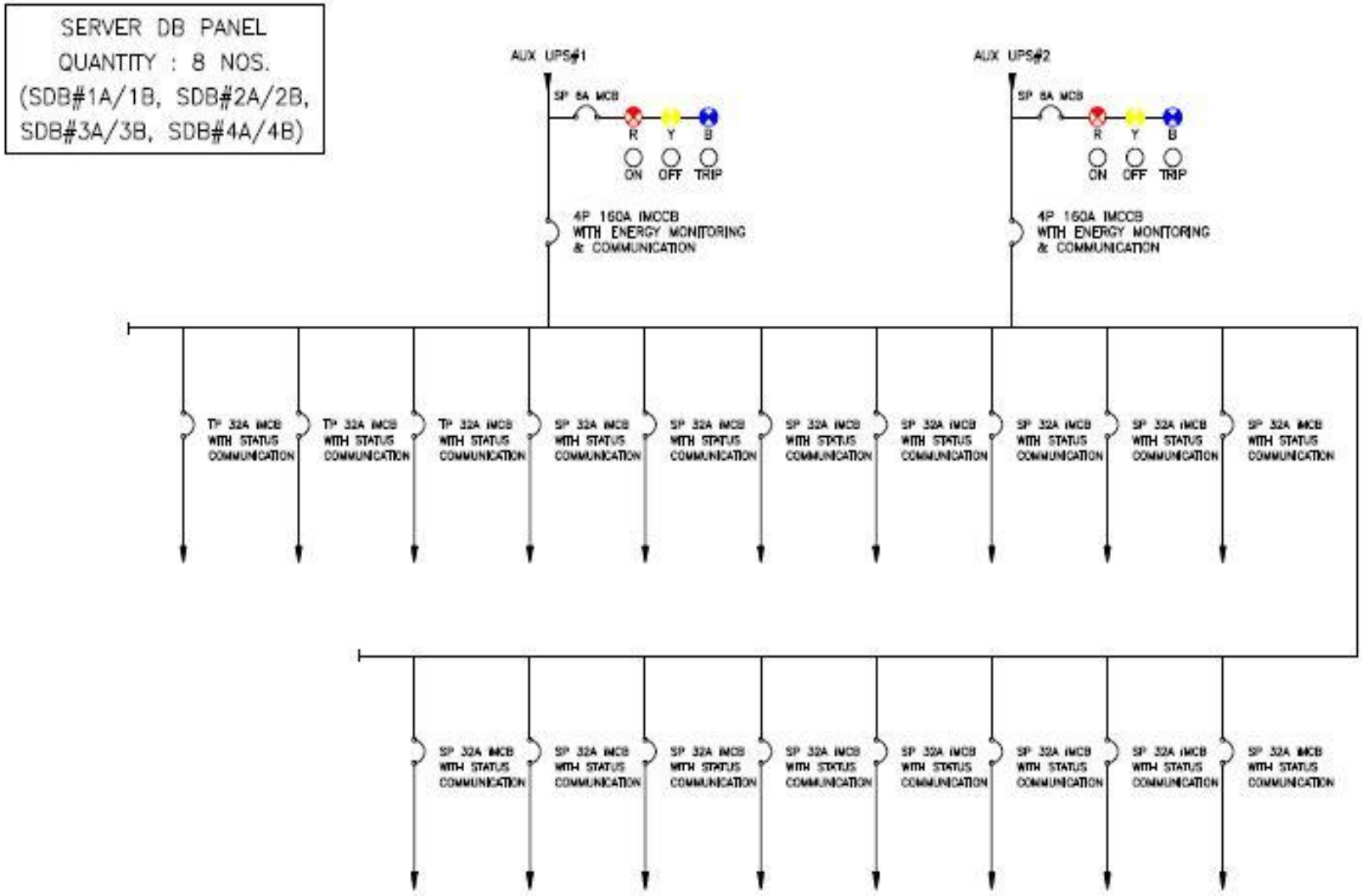
5.4. Raw Power DB



5.5. Aux UPS DB Panel



5.6. Server DB Panel



6. Un-priced BOM Compliance:

Bidder needs to quote all the items as specified in the BOM and needs to fulfill the following conditions, otherwise the bid will be summarily rejected.

i. For all the items, make and model must be specified.
ii. All the items must be covered for 5 years of on-site warranty and the same must be specified in the OEM authorization forms.
iii. No Downward deviation from the mentioned specification is allowed. If any downward deviation found, bidder shall be provided with a chance to rectify the same by complying with the minimum requirement but no additional cost will be considered.
iv. All products must have a road map for support for a minimum period of 7 years includes 5 years warranty
v. Bidder should submit all relevant data sheet/brochure of all quoted items and should also available in respective OEM's official website.
vi. Bidder should indicate items mentioned in the OEM data sheet / brochure by marketing the serial no. as mentioned in minimum specification in the RFP

7. Technical Parameters for the IT components under BOM

7.1. Cloud Specification:

Sr.No.	Opensource-Openstack based Cloud platform Specifications	Complied (Yes/No)
1.	**Specifications**	
1.1	The entire cloud solution should be offered with end to end mapping of the complete requirement mentioned in the BOQ, and 24x7 support from OEM for next 5 Years	
1.2	The solution should support x86 hardware from hardware vendors who are in or the topmost 4 OEMS for Data Center Servers (eg Cisco, Dell, HP, IBM/Lenovo). It should also support standard storage options from different OEM's and native storage for object mapping.	
1.3	The offered solution should be open-standard and open-source based with 24 x7 enterprise life cycle and support.	
1.4	The offered solution should be able to scale to additional nodes, automating the whole hardware lifecycle, including blade chassis from another OEM , and Rack servers	
1.5	The solution should be offered with complete feature functionality available with the OEM related to OpenStack, Open source, SINGLE Hypervisor and cloud Orchestration/management platform.	
1.6	Proposed solution should be offered with updates and upgrades to the latest versions available during the project period as required.	
1.7	Proposed solution should support software defined storage as well as storage virtualization with traditional storage.	
1.8	Certified Security certification of Common Criteria, (ISO/IEC 15408), FIPS or equivalent.(not mandatory)	
1.9	Should be supported for at least lifecycle of 5 years and extendable support up-to two more years.	
1.10	Platform Should Certified with multiple Industry leading Storage OEMS	
1.11	The solution should support HA and should support external and/or internal load balancer.	
1.12	It should able to creates a network file share, NFS and CIFS	
1.13	Offered solution should support ready state configuration for selected hardware, that automatically configures RAID, BIOS, Network bonding, etc.	

Sr.No.	Opensource-Openstack based Cloud platform Specifications	Complied (Yes/No)
1.14	The solution should be able to get backed up with Industry standard backup software like Commvault, Networkar, Semantec, etc	
1.15	The Solution shall deliver Hypervisor capabilities using any standard blade/ rack/ tower server infrastructure from HPE, DELL, IBM, Cisco, Oracle, etc.	
1.16	The Solution shall be able to run various operating systems like windows server, linux (RedHat, Suze Linux etc) KVM, Xen and any other open source	
2.	**Cloud Orchestration attributes**	
2.1	Cloud service Orchestration System should enable to provision cloud resources through self service provisioning interface, subject to approvals through workflows customized for the SDC.This self service capabilities should be available through a web interface, to be designed/ customized as per WBSDC requirement. This web interface should be user friendly and should have separate screens/ dashboards/ work flows for SDC Cloud Administrator and User Departments. The self-service portal for users should provide facilities to order and manage all possible services. The solution should be open source in nature with enterprise class 24x7 support from OEM.	
2.2	Cloud Service should support IaaS and capable of expanding it to PaaS model by adding relevant software layers and deployment models. Relevant open stack based solution need to be offered for complete cloud framework to be deployed alongside of hypervisors and operating systems.	
2.3	The Solution shall offer User Registration, Signup, Forgot Password and other standard pages (Profile, Billing or Contact information). The solution should provide Role Based authentication for all users.	
2.4	The Solution shall allow creation of library hosting various Operating System, Databases and middleware that can be selected while creating new virtual servers	
2.5	The Solution shall allow for implementing workflows for provisioning, deployment, decommissioning all virtual and physical assets in the cloud datacenter	
2.6	Cloud Orchestration System should enable to provision cloud resources from application programming interface (API), subject to approvals through workflows customized for the SDC	
2.7	Cloud Orchestration System should be accessible via secure method using SSL certificate. The solution should be offered with agentless automation and communication using simple SSH to run repeated tasks in automated manners to different instances. Minimum 500 instances need to be factored with the solution for automation purpose. Proposed automation tool should able to discover how a machine has changed over time or compare machines in your cluster to see how they are different.	
2.8	Should be able to crate, delete, shutdown, online VM migration from any segment with auto IP release, reboot virtual machines from Cloud Orchestration System as per the processes defined in the SDC	
2.9	Should be able to take snapshot of virtual machines and internal daily backup facility with third party backup solution	
2.10	Should be able to size virtual machine and select require operating system when provisioning any virtual machines. The solution should support physical provisioning also.	
2.11	Choice to place VM to any physical server. Container based deployment landscape should also be supported.	
2.12	Auto de- provision of service offering without disturbing the VM.	

Sr.No.	Opensource-Openstack based Cloud platform Specifications	Complied (Yes/No)
2.13	Should be able to predict billing/ Charge Back of resources before provisioning any cloud resources if integrated with a third party billing system. The charge back model should include following: - The Solution shall support different cost models - The Solution shall allow mixing of different cost model/ policies - The Solution shall have the ability to charge differently for different level of services - The Solution shall support cost calculation of shared/ multi-tenant application	
2.14	Should be able to set threshold of cloud resources of all types of scalability.	
2.15	Should be able to provision any kind of resources either static or elastic resources like Physical, Virtual or container types.	
2.16	Should be able to take console of cloud virtual machines from portal or as required to perform any operations.	
2.17	Should get list of all cloud resources irrespective of geographical locations from Cloud Orchestration System. System should display aggregate compute, storage capacity.	
2.18	Should be able to set the scaling parameters like in case of horizontal scaling a. Should be able to set percentage / quantity of RAM consumption to trigger new virtual machines. b. Should be able to set percentage / quantity of CPU consumption to trigger new virtual machines. c. Should be able to set percentage / quantity of network bandwidth to trigger new virtual machines. d. The above rules for containers based deployment also will be followed and in case of any container deployment the same should be achievable.	
2.19	Should be able to set port on which horizontal scaling will work.	
2.20	Should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.	
2.21	The virtual machine should have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic.	
2.22	Should ensure that the virtual machine format is compatible with other cloud systems. Also the cloud management platform should able to manage physical, multiple type of hypervisors like VMware, Hyper-V, RHV, OpenStack Based private cloud deployments, Container based deployment and also multiple public cloud like Amazon, Google and Azure.	
2.23	Cloud Orchestration System should support provisioning from self-Cloud Orchestration System to add more storage as and when require by VM.	
2.24	Orchestration System should give provision to attached new block disk, CEPH based object storage to any cloud VM from self-service portal.	
2.25	The cloud virtual machines should be auto-scalable in terms of RAM and CPU automatically without reboot.	
2.26	Cloud Orchestration System must support multi-tenancy for management perspective. Different department or group company should be able to access allocated resources only.	
2.27	The Solution should provide a simple to use intuitive web end experience for Cloud Administrator and User Departments.	
2.28	The Solution should provide comprehensive service catalog with capabilities for service design and lifecycle management, a web-based self-service portal for users to order and manage services.	

Sr.No.	Opensource-Openstack based Cloud platform Specifications	Complied (Yes/No)
2.29	The Solution should enforce password policies with the help of LDAP and AD integration (complex password, change password in specific number of days etc.).	
2.30	The Solution shall be capable of supporting separate templates/views of OS images and bundle of packages and VMs.	
2.31	The tool shall provide image library, where Software and server images can be maintained. Facilities shall be there to import new server templates to the library and registering, so as to use the same for provisioning the new virtual servers. It should capable to provision physical servers and containers also.	
2.32	The Solution shall be able to isolate and allow secure authenticated access to infrastructure services	
2.33	The Solution shall be able to abstract compute, network, and storage resources for the application and user self-service regardless of different type of hypervisor like VMware, Hyper-V, RHV etc., x86 based servers, network and storage hardware	
2.34	The Solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources.	
2.35	The Solution shall cater for the fact that if one server fails all the resources running on that server shall be able to migrate to another set of virtual servers as available	
2.36	The Solution shall provide support for cluster services between Virtual Machines	
2.37	Cloud should be support container based solutions	
2.38	Cloud Orchestration System should have provision to ensure that cloud virtual machine is into separate network tenant and virtual LAN.	
2.39	Cloud Orchestration System must ensure that cloud virtual machines are having private IP network assigned to cloud VM	
2.40	Should ensure that cloud VM network is IPV4 or IPV6 compatible.	
2.41	Should support use of appropriate load balancers for network request distribution across multiple cloud VMs.	
2.42	Cloud Orchestration System should provide network information of cloud virtual resources from OpenStack based deployed landscape	
2.43	Cloud Orchestration System should have built-in user-level controls and administrator logs for transparency and audit control for OpenStack based deployed landscape.	
2.44	Cloud Orchestration System should support policy based provisioning of virtual machines. Based on granted permission, users should be able to perform the operations. For example if any users doesn't have permission to delete VM, he should not be able to do it.	
2.45	Cloud Orchestration System should support quota based system. Users should not be able to provision resources beyond allocated quota in the Openstack infrastructure.	
2.46	The Admin should be able to define Access Control to Permit or Deny operation per Group or per User.	
2.47	Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.	
2.48	The Solution should allow for implementing workflows for provisioning, deployment, Decommissioning all virtual and physical assets in the cloud datacenter.	
2.49	User Management: The solution shall provide comprehensive user management	
2.50	Individual users shall be able to manage their own profile and individual preferences. The solution administrator shall have the rights to all User Management functions.	
2.51	Cloud Orchestration System should provide facility to make template from virtual machines.	
2.52	Cloud Orchestration System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.	

Sr.No.	Opensource-Openstack based Cloud platform Specifications	Complied (Yes/No)
2.53	Cloud Orchestration System should have provision to live migration of virtual machine to another physical servers.	
2.54	Cloud Orchestration System should have provision to migration of virtual machine from one hypervisor platform to a similar hypervisor platform	
2.55	Cloud Orchestration System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.	
2.56	The Cloud Orchestration System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.	
2.57	Cloud solution should support detecting, in real time, resource requirements of a system in openstack environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.	
2.58	Cloud Orchestration System should give provision to monitor the network traffic of cloud virtual machine.	
2.59	Cloud Orchestration System must offer provision to monitor uptime of each cloud virtual machine	
2.60	Cloud Orchestration System must make provision of resource utilization graph i.e. RAM of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.	
2.61	Cloud Orchestration System must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.	
2.62	Cloud Orchestration System must make provision of resource utilization graph i.e. disk of each cloud virtual machine. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.	
2.63	Cloud Orchestration System must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.	
2.64	Cloud Orchestration System must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity, Support Visualization capabilities, Change Alerts, to enable the quick identification and context of performance availability problems.	
2.65	The Solution shall provide the capability to migrate the live Virtual Machine files from one storage array to another storage	
2.66	The Solution shall allow provision of security on the hypervisor, as well as guest VMs. It shall provide the ability to apply security to virtual machines and security policies that can follow the machines as they move in the cloud.	
2.67	The Solution shall also integrate with SAS,SSD,FC,FCoE and iSCSI SAN and infrastructure from leading Vendors so as to leverage high performance shared storage to centralize Virtual Machine file storage for greater manageability, flexibility and availability	
2.68	The Solution shall allow configuring each Virtual Machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address	
2.69	The Solution shall allow means for connect virtual machines with related applications	
2.70	The Solution shall support configurations with standard VLAN implementations from all vendors	
2.71	The Solution shall offer Automated and Approval based Upgrades for Virtual Machines delivered through cloud infrastructure	
2.72	The Solution shall be able to Integrate existing malware protection solution in SDC for Virtual Machine	
2.73	The Solution must offer Identity, Authentication and Role based access to User Departments Infrastructure - Machines (Virtual or Physical), Application or Common Services.	

Sr.No.	Opensource-Openstack based Cloud platform Specifications	Complied (Yes/No)
2.74	The Solution must offer Policy based administration by putting User Departments Machines (Virtual or Physical) in logical groups and apply relevant policies.	
2.75	The Solution shall have the ability to not just enforce policies but also track and report non-conformance	
2.76	The Solution shall support VLAN isolation by supporting multiple networks per resource pool	
2.77	The Solution shall support secure communication between guest VMs and Hypervisor and intra-VMs.	
2.78	The Solution shall have the ability generate standard & customized report as well as the native ability to export to common formats	
3.	**User Department Requirements**	
3.1	The User Departments shall be able to view Department's infrastructure as Services e.g. : group his servers by- application LOB servers, All web servers, all Small servers etc	
3.2	The User Departments shall be able to select between a managed infrastructure or an unmanaged infrastructure. (e.g. who will manage the PatchUpdating on virtual machines)	
3.3	The Solution shall allow User Departments to delegate user services to others on their team	
3.4	The User Department shall be able to allocate, monitor, report and upgrade allocated capacity as required within allocated capacity.	
3.5	The Solution shall allow selecting various Operating System as well as option of Installing additional software's on the provisioned Containers, Virtual Machines and physical machines to User Department while Requesting for provisioning of new virtual servers from Self service GUI	
3.6	The User Department shall be able to report Department's allocated Quota, Used Quota and balance Quota of infrastructure capacity	
3.7	The User Department shall be able to view consumption reports for Department's cloud infrastructure (Virtual, Physical, Containers, Application or Common Services)	
4	**SDC Cloud Administrator Requirement**	
4.1	Administrators shall be able to automatically scale and/or manage resources unilaterally	
4.2	Administrators shall be able to easily configure, deploy, and manage services through a highly intuitive service-centric interface, while using a library of standard templates. The solution should be capable to provision compute, network and storage as required automatically or manually on an enterprise class OpenStack based private cloud landscape.	
4.3	Administrators shall easily be able to commission & decommission VMs	

7.2. Servers:

1. Centralized Management Solution for Managing Blade and Rack Servers from the same Management Dashboard must be available.
2. Management Solution must be in Redundant Mode
3. Blade Server Network Switch must be provisioned from Day -1 with scalability.

7.2.1. Rack Servers:

Sl. No	Features	Minimum Specifications Required	Complied (Yes/No)
1	CPU	4 x Intel Xeon Processor E5 20Core Min 2.4GHz	
2	Cache L3	Min 35MB	
3	Chipset	Intel C612 or Better	
4	Memory	8 x 64GB DDR4 Memory with Min 2400Mhz speed	
5	Memory Slots	24 DIMM sockets	
6	Memory Upgradability	Up to 1.5 TB with 24x 64 GB LRDIMMs and two processors	
7	Memory protection support	ECC, Memory Mirroring, Memory Sparing	
8	SCSI Controllers	Integrated 12 Gbps SAS Hardware Raid Controller supports Hardware RAID 0, 1, 5.The onboard controller should support self-encrypting drives.	
9	Disk Drives	6x1200GB 10K 12Gbps SAS 2.5in G3HS HDD	
10	Graphics Controller	16MB SDRAM	
11	I/O Adapter	The server should have redundant dual Port 10G/FC/FCOE adapters (2 Nos of Dual Port or 2 Nos of Quad Port 10G NICs) to provide adapter level redundancy. The adapters should be enabled with FCoE or iSCSI hardware offload	
13	Ports	One external USB 3.0 Port.	
14	Operating System Support	Microsoft Windows Server 2012 and 2012 R2, Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 11 and 12, VMware vSphere 5.5 and 6.0	
15	Management	Integrated management module with remote presence enablement (graphics, keyboard, mouse and virtual media)	
16	Security features	Power-on password, administrator's password, Trusted Platform Module 1.2.	
17	Failure Alerting Mechanism	The server should be able to alert impending failures on maximum number of components. (Processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs), fans, power supplies & RAID controllers.	
18	Warranty	5 Years Onsite Comprehensive Warranty	

7.2.2. Blade Servers

Srl No	Features	Minimum Specifications Required	Complied (Yes/No)
1	CPU	2 x Intel Xeon Processor E5-2680 v4 14C 2.4GHz 2400MHz 120W or better	
2	Cache L3	Min 35MB	
3	Chipset	Intel C612 or Better	
4	Memory	8 x 64GB DDR4 Memory with Min 2400Mhz speed	
5	Memory Slots	24 DIMM sockets	
6	Memory Maximum	Up to 1.5 TB with 24x 64 GB LRDIMMs and two processors	
7	Memory protection support	ECC, Memory Mirroring, Memory Sparing	
8	SCSI Controllers	Integrated 12 Gbps SAS Hardware Raid Controller supports Hardware RAID 0, 1. The onboard controller should support self-encrypting drives.	
9	Disk Drives	2 x 600GB 10K 12Gbps SAS 2.5in G3HS HDD	
10	Graphics Controller	Min 16MB SDRAM	
11	I/O Adapter	The server should have redundant dual Port 10G adapters (2 Nos of Dual Port or 2 Nos of Quad Port 10G NICs) to provide adapter level redundancy. The adapters should be enabled with FCoE or iSCSI hardware offload	
12	Ports	One external USB 3.0 Port.	
13	Operating System Support	Microsoft Windows Server 2012 and 2012 R2, Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 11 and 12, VMware vSphere 5.5 and 6.0	
14	Management	Integrated management module with remote diagnostics (graphics, keyboard, mouse and virtual media)	
15	Security features	Power-on password, administrator's password,	
16	Failure Alerting Mechanism	The server should be able to alert impending failures on maximum number of components. (Processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs), fans, power supplies & RAID controllers.	
17	Warranty	5 Years Onsite Comprehensive Warranty	

7.2.3. Specifications for Blade Chassis

Sl. No	Features	Minimum Specifications Required	Complied (Yes/No)
1	Form Factor	Max 12U Rack mounted chassis to house at least 14 half height/width OR 7 full height/width compute blades. The Bidder should not quote for a blade chassis which is likely to be declared end of support within 5 years period. Bidder to attach the letter from OEM stating the same.	
2	IO Bays	Min Four high-speed switch bays capable of supporting I/O architectures in Ethernet 1GbE, 10GbE and 40GbE, Fiber Channel, FCoE and InfiniBand	
3	Switch Modules	The Chassis should have minimum of 2 x 10G converged switches. The switches should be enabled with adequate number of downlink ports to support 4 x 10G ports per blade server for the full capacity of offered blade chassis. Each switch should have a minimum of 4 x 16Gbps FC uplinks for storage connectivity, 2 x 10G SR and 2 x 1G RJ 45 uplinks for LAN connectivity. The switch should be designed to support both LAN and SAN environments, offering Layer 2 and Layer 3 features for the LAN and support for connectivity to SAN including FCoE, Fiber Channel, iSCSI, and NAS storage.	
		Each switch should deliver non-blocking architecture with minimum 1.28 Tbps throughput and full line write performance.	
		The proposed converged switches should be capable of supporting 16G FC transceivers for SAN connectivity and 40G transceivers for LAN environment.	
		The switches should deliver a highly efficient In-Service Software Upgrade to deliver enterprise-class business continuity during a software upgrade/downgrade process. The software change process should be non-disruptive to Layer 2, Layer 3, Fiber Channel, and FCoE traffic	
		The switch should support : Border Gateway Protocol (BGP4+), Layer 3 ACLs , Multicast: PIM-SIM, IGMPv2, OSPF, Static Routes, IPv4/v6 ACL, Policy-Based Routing (PBR), Bidirectional Forwarding Detection (BFD), 16-way ECMP, VRF Lite, VRF-aware OSPF, BGP, VRRP, static routes , VRRP v2 and v3, IPv4/IPv6 dual stack, IPv6 ACL packet filtering, IPv6 routing, Wire-speed routing for IPv4 and IPv6 using any routing protocol, Data Center Bridging eXchange (DCBX), FCoE to Fibre Channel Bridging,End-to-end FCoE (initiator to target),VM-Aware Network Automation,ACL-based QoS,Class of Service (CoS) IEEE 802.1p,Per-port QoS configuration,Flow-based QoS,IPv4/IPv6 management,Port-based Network Access Control 802.1X,TACACS+,Secure FTP (sFTP)	
		The switches should be VM-aware (should support Automatic Migration of Port Profiles) and should support SDN/NFV features and capabilities. The switches should support administration through Open Flow 1.3, OpenStack, Puppet, Python and standard CLI.	
4	Mid plane	Chassis should have a highly reliable mid plane for providing connectivity of the shared resources to the compute nodes in a highly reliable manner.	
5	Power Modules	Redundant power modules to provide N+1 redundancy. Vendor to quote for the PDUs along with blade chassis	

Sl. No	Features	Minimum Specifications Required	Complied (Yes/No)
6	Chassis Management Module	Integrated chassis Management Module providing IP based management of the blades and vital elements like FC and Ethernet Switches. Should also provide for controlling Power, Fan management, Chassis and compute node initialization, Switch management, Resource discovery and inventory management, Resource alerts and monitoring management, Chassis and blade power management and diagnostics for elements including Chassis, I/O options and compute nodes.	
7	Chassis Management Network	The management network connection to individual server nodes and I/O modules should be minimum 1Gbps to provide faster throughput for remote connections, deploying operating systems, and updating firmware.	
8	System Panel	LEDs on the front information panel that can be used to obtain the status of the chassis Identify, Check log and the Fault LED	
9	Management Software	The blade chassis should be supplied with management software for the full capacity. The management software should be from the same OEM.	
10	Operating Temperature	Chassis must have an operating temperature of at least 5 degrees centigrade to 40 degrees centigrade.	
11	Warranty	5 Years Onsite Comprehensive Warranty	

7.2.4. AAA server

Sr. No.	AAA Feature	Complied (Yes/No)
1	The AAA solution should be available as both hardware based appliance or software based solution	
2	The AAA Server should provide authentication services to all the users connecting to the network, should enforce security policies on the end stations	
3	The AAA Server should offer centralized command and control for all user authentication, authorization and accounting from a Web- based, graphical interface and distribute those controls to hundreds or thousands of access gateways in the network	
4	The AAA Server should provide the manageability and administration of user access for routers VPNs, firewalls, dialup and DSL connections, cable access, storage, content, voice over IP (VoIP), wireless solutions and switches using IEEE 802.1x access control	
5	The same AAA Server should leverage access framework to control administrator access and configuration for all RADIUS enabled network devices in the network	
6	It should support Authentication by validating any user's login credentials against a central security database to ensure that only individuals with valid credentials will be granted network access	
7	The proposed solution should be able to integrate with industry leading Directory server like but not limited to LDAP server, Microsoft Active Directory, RSA Secure ID server	
8	The AAA server should support the following authentication methods Native User Authentication Pass Through Authentication Proxy RADIUS Authentication External Authentication Directed Authentication HTTP Digest Access Authentication	
9	The AAA server should support the following authentication protocols EAP-TTLS EAP-PEAP EAP-TLS EAP-MD5 PAP CHAP MS-CHAP and MS-CHAPv2	
10	Device command set authorization Network access restrictions and administrative access reporting. Restrictions such as time of day, day of week and session time limits . User and device group profiles. Should have a Web-based user interface to simplify and distribute configuration for user group profiles	
11	The AAA Server should be able to support large networked environments and support for redundant servers, remote databases, and user database backup services. Lightweight Directory Access Protocol (LDAP) authentication forwarding support for authentication of user profiles stored in directories from leading vendors	
12	Different access levels for each AAA Server administrator- and the ability to group network devices- enable easier control and maximum flexibility to facilitate enforcement and changes ofsecurity policy administration over all the devices in a networks	
13	The AAA server should be compatible with all the components of SIEM, FLOW and Networking solutions quoted for this RFP	
14	The AAA server should support LDAP Configuration Interface (LCI) to allow scripting	
15	The AAA server should support Java scripting for LDAP	
16	The AAA server should support JavaScript Realm Selection and Filter Selection	
17	The AAA server should support directed realms to provide virtualized instances of the server, allowing requests to be managed according to their nature	

Sr. No.	AAA Feature	Complied (Yes/No)
18	The AAA server should support Location-based profiles for groups	
19	The AAA server should support Account lockout and account blacklisting	
20	The AAA server should support Proxy filtering	
21	The AAA server should support IP address assignment via locally managed IP or Dynamic Host Configuration Protocol (DHCP) pool	
22	The AAA server should support directed realms to provide virtualized instances of the server, allowing requests to be managed according to their nature.	
23	The AAA server should support IPv6	
24	The AAA server should support Attribute translation and mapping to translate from one type of network access equipment to another	

7.2.5. Server Racks

Sr. No.	Specifications	Complied (Yes/No)
1	Server Rack Enclosure	
2	Supply, Assembly and Installation of UL listed Server Racks	
3	Size - Minimum. 750-800 mm (W) x 1070 -1100mm (D)	
4	Height - 42 U	
5	Rack should include following	
6	a. Single Perforated Front Door with profile which shall have better air flow, MINIMUM 85% of Open Perforated area of Front Door. b. Split Perforated Rear Door for better clearance at rear side c. Removable side panel split in to two for easy removal with lock. Side Panel should be of pass-through type in front and rear side, with preinstalled wire brush. This shall allow to pass the cables to side enclosure directly without mixing the air between. d. Castor Wheels and adjustable leveling feet from underneath or above. e. Roof includes two large cable access slots for high density cabling and brush strips for air containment. Roof to have spring loaded pints for easy roof removal and installation with cable in place. f. Rack should be supplied with accessories mounting channels - 04 no's in rear (2 in left and 2 in right) to mount zero U rack PDUs. Each channel should be capable to mount 2 Rack PDUs of 32A, Single Phase g. Vendor-neutral EIA-310, 19" Rack Mounting Rail with option of adjustment in 1/4 in (6.4 mm) increments, U position numbered in front and rear. h. Baying Kit to join enclosures i. Hardware Kit with M6 x 16 Phillips slot screws and cage nuts. j. Vertical Manager - 02, pre-installed in front side of rack, 01 in left and 01 in right. The vertical cable manager should have smooth plastic cable guides at 1 U increments to allow patch cords to enter and exit in an organized manner. k. Static Load Capacity of minimum 1300 kgs and rolling load of not less than 1000 kgs	
7	8 no's of Racks to have 3 phase PDU's	

7.2.5. Rack PDU for Server and Storage Racks

Sr. No.	Specifications	Complied (Yes/No)
1	Supply, Installation, Testing and Commissioning of 2 Intelligent Rack PDUs in each Rack of 32A, 1Ph for Medium Density Racks and 32A, 3Ph for Hi density Racks	
2	Single Phase Rack PDU should be with input cable length of minimum 2.5 meters IEC 309 32 A P+N+E connector to connect from floor mount PDU power extension cable. Three Phase Rack PDU should be with input cable length of minimum 1.5 meters IEC 309 32 A 3P+N+E connector to connect from floor mount PDU power extension cable.	
3	PDU should have IEC C13 X 16 & IEC C19 X 6 outlets that support the IT devices allocated in the Rack	
4	Acceptable input voltage: 220–240 VAC; Maximum input current (phase): 32 A VDE; Overload protection (internal): Two (2) 16 A, 1-pole hydraulic-magnetic circuit breakers. PDU should provide real-time remote monitoring (Volts, Amps, total Power-kilowatt and Total Energy- kWh) of connected loads. User-defined alarms warning system. Locally it should be able to display the Volt, Amps and Power on the LCD display affixed on the Power strip itself.	

7.2.6. Open Common Racks

Sr. No.	Components	Specifications	Complied (Yes/No)
1	Features	Should be available in 2-Post Configurations	
		Option of 84" height	
		Should be available with an option of Rail Widths: 3", 6", 12" (2-Post)	
		EIA-310-E Compliance	
		UL Listed, Certification - Information Technology and Communications equipment	
		Load Capacity: 1000 lb (2 and 4-Post Al)	
		EIA Standard Hole Pattern: 12-24 Threads @ 5/8" (127mm), 1/2" (25.4mm) centers	
		2-Post Configuration Material: Al: 6061-T6 Aluminium Extrusion (3" Rail), Al: 6061-T6 0.125" Thick, (6" and 12" Rail), Steel: 16 Gauge, CRS	
		Finish: Durable black epoxy powder-coat	
		Easily assembled, hardware included	
2	Cable Management	Ergonomically designed and aesthetically pleasing, Lightweight, but sturdy	
		Should have dual hinge latching door & can be opened right or left.	
		Cable fingers spaced at 1RMU increments for exact alignment with EIA standard	
		Rack spacing	
		Cable fingers support up to 48 cables per RMU	
		Should be available in 6", 8" & 12" vertical trough widths both single sided or double sided.	
		In case of Horizontal cable management the cable manager should be covered	
		Horizontal cable management troughs should be available in 1 & 2 RMU	
		Open back on 2U and 3U horizontal troughs for easy pass through of cables	
		Easy one point removal and installation process for door	
		Handle should be recessed to eliminate snag potential for clothes and arms	
		Cable fingers are specially designed with smooth surface for cable routing from High Density Cable Manager to Cable manager and vice versa	
		Provision for Tool-less installation of Cable Spool	

7.3. SAN Storage &Backup Solution:

Backup server at SDC is responsible to take online backup for all application servers, DB servers including VMWare infrastructure with existing backup software to the proposed backup appliance with inline deduplication technology.

7.3.1. Specification for All flash/FMD 100 TB storage (For WBSDC) and 120TB (For NDC)

S.No.	Storage	Compliance (Yes/No)
1	The Storage OEM should be positioned as a leader in the latest Gartner Magic Quadrant for Solid-State Arrays in the last year	
2	The proposed storage system should be of Enterprise class All SSD/ Flash /FMD storage.	
3	The storage should be able to scale to 2 PB capacity or higher using Flash Disks and FMDs of capacity less than 8TB and 4 TB each respectively.	
4	The storage system must support intermixing of all SSD/FMD sizes in a same drive enclosure/chassis/shelf.The supported disks should be dual ported with minimum 6Gbps/12Gbps full-duplex data transfer capability.	
5	Offered Storage Array shall be supplied with minimum of two controller/VSDs with scalability to minimum 6 controllers/VSDs & should be supporting all Block and File protocols for flexibility & ease of management	
6	The storage system should be true scale-out/scale-up system by allowing creation of virtual storage system from the resources spanning across multi-controllers.	
7	The storage must provide non-disruptive firmware/microcode upgrade, device reallocation and configuration changes	
8	The proposed storage system should support more than 20000 LUNs /Volumes	
9	The storage system should support Clusters of MS-SQL , My SQL , PostgreSQL , and Windows and Linux server clusters .	
10	The storage system should have TOTAL minimum 1 TB Global Shared Cache extendible to 2 TB across all controllers (usable cache memory after cache protection overheads) with an ability to protect data on cache if there is a controller failure or power outage. The usable cache should only be used for reads & writes of workloads. SSDs will not be considered as cache memory.	
11	The cache on the storage should have minimum 48 hrs or more battery backup or should have de-staging capability to either flash/disk.	
12	The storage should be supplied with iSCSI, NFS, CIFS, FC protocols for use with different applications. All protocol licenses should be provided for entire capacity of the storage. Any hardware/software required for this functionality shall be supplied along with it in No Single Point of Failure.	
13	Should support various RAID levels like Single Parity RAID, Dual Parity RAID & Mirrored RAID.	
14	The architecture should be designed as a NSPOF architecture.	
15	Proposed storage should support both block and File level Data Reduction methods , otherwise extra usable storage capacity needs to be factored as per below clause.	
16	The storage should be supplied with rack mount kit. The storage system should be supplied with all the necessary SFP+ modules & patch cords as required. Storage Solution Should be accommodated in a standard 42U 19" rack.	
17	The storage array shall have the ability to expand LUNS/Volumes on the storage online and instantly.	
18	The Storage array must provide capability for thin provisioning of capacity. Vendor should provide the licenses for maximum supported capacity of the proposed storage.	

S.No.	Storage	Compliance (Yes/No)
19	The storage should have Quality of Service features.	
20	The proposed storage should have capability to do storage based replication with another storage at DR/DC. Replication should be storage based and integrated with storage system. Otherwise, the solution should include all the hardware like FC-IP routers, either built-in or supplied separately, if required to fulfil the replication solution. For maintaining Zero Data Loss in future, the required software capabilities should be included now and the hardware (ports, switches) required to achieve the same should be proposed now but will be procured later. The solution shall support replication for the full supported capacity of the system for at least 3000 volume pairs . Vendor should provide the licenses for maximum supported capacity of the proposed storage for both synchronous and asynchronous replication.	
21	The storage system should support remote replication for both file and block. For optimal usage of bandwidth and to reduce operating expenses remote replication should provide “data reduction”. Any additional hardware or software required to achieve the same should be provided along with replication solution.	
22	The proposed storage system should have redundant hot swappable components like controllers, disks, power supplies, fans etc.The proposed storage must support non-disruptive replacement of hardware component. Architecture shall support isolation of failed components automatically without rebooting/failing the entire controller for sub-component failures like CPU, cache DIMMs, ports etc	
23	The solution shall support replication in one to many and many-to-one mode . The replication solution on storage shall support failover to BCP/DR storage and failback as and when required using DC, DR and Near DR .	
24	The array should support controller-based functionality for pointer based snapshot. The storage should support minimum 250 snapshots per volume/LUN. Vendor should provide the licenses for maximum supported capacity of the proposed storage.	
25	It should be possible to switch storage resources from storage system in one site to storage system in another site in case of any outage. All required hardware, software & licenses components required to provide the above functionality in the secondary site should be included as part of the proposal from day one.	
26	The system should support instant creation of clones of active data, with near zero performance impact for both block and file. Necessary license to clone & restore from clone to be provided. Vendor should provide the licenses for maximum supported capacity of the proposed storage.	
27	Easy to use GUI based and web enabled administration interface for configuration (Create/delete/configure Luns/Tiering/ Alerts / Cloud configuration)	
28	Friendly GUI Based Storage Administration tools for role based access control ,monitoring , even management and closure , threshold setting, LUN mapping , deallocation , space reclaim etc	
29	GUI Based Storage Monitoring tools to obtain Storage performance statistics like Total IOPs performance , Read/write percentages, Store historical data , Management Dashboard etc.	
30	The storage shall support logical/Virtual partitioning of controllers in future such that each partition appears as a separate storage in itself. Vendor should provide the licenses for maximum supported capacity of the proposed storage.	
31	The proposed storage should support industry-leading Operating System platforms including: Suse and Red Hat LINUX, Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc. It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multi-pathing/Equivalent software, if required, with the solution for unlimited host connectivity.	
32	All the licenses on the storage system must be provided for maximum capacity supplied with the system from day one.	

S.No.	Storage	Compliance (Yes/No)
33	Any hardware & software components required to enable the replication/DR solution will need to be provided, in requisite quantities of each, by the vendor.	
34	The storage system must be supplied with Data-at rest encryption and key management solution (for Storage), drive based encryption shall not be accepted	
35	The storage should be supplied with **100TB(SDC)** and **120TB (NDC)**usable capacity (Excluding any RAID overhead, Hot spare, Controller OS overhead, Snapshots and Clone overheads etc.) in dual disk failure protection with Data Reduction enabled. The SSD/FMD disks should not be greater than 4 TB for controllers with 6Gbps SAS Lanes and not greater than 8 TB for controllers with 12 Gbps SAS Lanes . One Global spare should be provided for every 15 SSD/FMD . OEMs that do not support data reduction capability should provide a physical usable capacity of **120TB(SDC) and 150TB (NDC)** to compensate for benefits of Data reduction , other than the Global spares and overheads indicated above .	
36	The designed IOPs for 30:70 Write:Read for the above systems for Raid 6 should be minimum 1,30.000 . The design document should be shared in the proposal .	
37	Front-End Ports – Minimum 32 Nos. FC ports of 16Gbps each scalable to 64 ports , + 4 Nos. 10GbE Ports + 2 nos 1GbE ports + 4 ports 10GbpE for replication . Back-End ports –Minimum 384 Gbps of aggregate bandwidth for disk drive connectivity scalable to 768Gbps across all controllers .	
38	The Hardware and software quoted should have 5 years warranty and should have OEM support for 5 years from date of commissioning and acceptance, however it should not later than 2 weeks from delivery . 24X7 Support with 2 hrs resolution for faults not requiring any spares, 6 hours resolution for faults requiring spares . Total downtime should not exceed 8 hrs in an year.	

7.3.2. Backup Software:

The Backup software must be provided along with required licenses to take backup of source data to Virtual Tape Library, as per following specifications:

Sr.No.	Specification	Complied (Yes/No)
1	OEM should be in the Gartner's Leaders Quadrant for Enterprise Backup Software and should be available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup/ restores from various platforms including Windows, UNIX, HP-UX, IBM AIX, Linux. Both Server and Client software should be capable of running on all these platforms.	
2	Ability to backup data from one server platform and restore it from another server platform to eliminate dependence on a particular machine and for disaster recovery purposes.	
3	Should support various level of backups including full, incremental, differential, synthetic and virtual synthetic backups	
4	The backup software should be able to encrypt the backed up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.	
5	Should be able to recover data using wizard based recovery, backed up by existing backup software to proposed backup appliance and replicated to Near site and DR site.	
6	Should have single pane of glass management for backup software and proposed backup appliance	
7	Should support parallel save streams for Unix, Linux and windows systems to achieve parallelism till the end of the backup, enabling backups to complete much quicker than standard scripted solutions	
8	Must support wizard-driven configuration and modifications for backups and devices	
9	Should have firewall support and single management pane to manage backup/restores and all backup target storage devices.	
10	Must support P2V, P2P, V2V backup of all standard Virtualisation platforms and Cloud Orchestration software .	
11	Should able to break up large save sets into smaller save sets to be backed up in parallel to allow backups to complete faster for Unix & Linux clients	
12	Should have in-built calendar based scheduling system and also support checkpoint restart able backups to preserve the integrity of the backup window	
13	Should have integrated snapshot management for existing and proposed storage arrays from end-to-end within the backup software including configuration of snapshot backup to recovery.	
14	Should support block based backup for Windows systems to speed up the backup of workloads such as high density file systems or very large files.	
15	Should support immediate clone controlled replication to enable replication to begin as soon as a saveset as part of a group has finished.	
16	The Backup software should have the ability to report inactive files, which will help the customer decide what to backup/archive.	
17	Should support backups for clustered servers and support industry popular clusters like Sun cluster, HP service guar, HACMP i.e. should have the ability to backup data from clustered servers from the virtual client.	
18	The software should support virtual platform like VMWare, KVM, Citrix Xen Server and Hyper V, licensing of such environments should be based on physical hosts not on the number of virtual instances.	
19	Must support backup / recovery of raw SCSI volumes	
20	Licensing of the software should not to be dependent on the number of CPUs of the client machines.	
21	Should support advanced backup to disk backups where backups and restores from	

Sr.No.	Specification	Complied (Yes/No)
	the backup media (disk in this case) can be done simultaneously.	
22	The solution must support client-direct backup feature to reduce extra hop for backup data at backup/media server to cater stringent backup window	
23	Backup clients should be updated automatically using the client push feature	
24	Should integrate with third party VTL which has data deduplication capabilities.	
25	Should be able to restore data already backed up to tape media.	
26	License for Backup Software to be quoted for (i) 30TB Backup with additional increments for 5 TB (ii) 10 TB Archive with incremental cost for 5 TB (iii) Server based license for 2 nos	
27	Should support online backup Agent/Modules for Databases such as MS SQL, Oracle, Exchange (DAG), Lotus, DB2, Informix, Sybase, MySQL, SAP, PostgreSQL and should be per host and not dependent on number of CPUs	
28	Must support Hardware and storage array based snapshot backup with zero downtime and zero load on the primary backup client.	
29	Must support bandwidth optimize open storage technology for backup to purpose built backup appliances for optimum utilization of network bandwidth during backup	
30	Should have bare metal recovery from physical servers to both Hyper-V and VMware vSphere virtual machines for Windows 8.1 and Windows 2012 or latest	
31	Should support centralized proxy-based image backup with load-balancing, multi-streaming and change block tracking	
32	The backup software should support data movement directly from the backup client to the disk target without passing through the backup server.	
33	Backup Solution must support multi tenancy feature for creation of distinct data zones where the end users have access without being able to view data, backups, recoveries, or modify in other data zones.	
34	The proposed solution should have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats.	
35	The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.	

7.3.3. Tape Library

Sl.No.	PARAMETER	Specification	Complied (Yes/No)
1	Architecture & Future Scalability	The offered Automated tape Library should be supplied with min 15 LTO7 FC Tape drives and 240 Slots with Redundant Power Supply . The Tape Library must be further scalable to more than 40 LTO7 drives& 500+ Slots , as and when required by the SDC by stacking expansion modules for drives and slots for future growth within the same library.	
2	HARDWARE PARTITION	The offered Automated tape Library must support partitioning so that each drive can be configured in a separate partition thus providing the ability to utilize a single library in a variety of applications.. All the necessary License or hardware for min 10 partitions scalable to 20 Partitions must be provided along with the library.	
3	Tape Drive technology & Consumables	Offered LTO7 drive in the Library shall conform to the Continuous and Data rate matching technique for higher reliability. 200 LTO7 DATA CARTRIDGES & 10 CLEANING CARTRIDGES, with Colored Barcode labels must be provided as a part of supply. SDC will procure more consumables- as and when required.	
4	Data Transfer rate & backward compatibility	Each of the LTO7 drive shall support 300 MB/sec in Native mode and 750MB/sec in 2.5:1 Compressed mode. The drives must be able to restore old LTO6/LTO5 media.	
5	Encryption	The offered Automated tape Library must support encryption . The overall solution offered with the Tape Library should provide either AME or LME encryption key management. The necessary tools/License required must be provided by the System integrator, to keep the Encrypted keys in a Redundant and safe location.	
6	Connectivity & Integration	Offered Tape Library should be integrated with the other Servers and storage to back up all the data from the SAN to The Tape library using the required back up S/w via LAN or LAN Free. The Bidder needs to supply the necessary Back up s/w to integrate this functionality.	
7	RELIABILITY	RELIABILITY: The offered tape library must have a high reliabilityie MCBF (mean cycles between failures) more than 3,000,000 cycles.	
8	Management	Tape Library shall provide web based remote management.	
9	INTELLIGENT MONITORING:	The overall solution with Tape Library and the backup s/w integration should have features like Intelligent monitoring management and diagnostics	
10	Barcode Reader and Mail slots	Tape library shall support Barcode reader and min 10 mail slots- to deliver easy, secure access to individual tape cartridges without interrupting library operations. Mail slots must be scalable to min 30 once the Library is Fully scaled up.	
11	Other Features	1. Tape Library shall have GUI Panel 2. Shall be rack mountable. 3. The Tape library must Set alerts for backup and archive events. 4. LCD front panel. 5. The TL should have support for minimum 7 Years , and must be quoted with 5 YEARS 24x7 ONSITE SUPPORT & warranty back to back with OEM- MAF to be submitted.	
12	Tapes for backup	Minimum 200 Latest generation LTO Tapes is to be provided.	

7.3.4. DR Management Software

SL No.	Requirements	Complied (Yes/No)
1	The proposed solution should be in the form of a software which is rated/mentioned in independent analyst reports from either Gartner or IDC for at least 5 years running and the OEM of the solution should be in the market for at least 10 years	
2	The proposed solution must offer a workflow based management & monitoring capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts on any deviations.	
3	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR.	
4	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness and facilitate policy based actions for events with ability to cancel out polar events.	
5	The proposed should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions.	
6	The DR Management solution should have a managed lifecycle for all workflows from draft to final published version with version control and time stamp to ensure proper testing and troubleshooting of drill/recovery procedure.	
7	The proposed solution should be capable of executing DR drill and recovery workflows in simulation mode, without any changes to DR to ensure conditions are met to ensure a successful execution.	
8	The proposed solution should have granular, role based administration and should use existing Active Directory/LDAP for identity management without the need of its own, separate identity management database and facilitate role based administration based on attributes defined in AD/LDAP	
9	The proposed solution should be capable of generating reports and email/SMS alerts on RPO deviation, RTO deviation and DR Drills from a centralized location.	
10	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should seamlessly integrate with existing environment without the need to replace/change configuration including existing clusters.	
11	The proposed solution must support all major platforms including Linux, Windows, Solaris, HPUX, and AIX with native high availability options. It must support both physical and virtual platforms.	
12	The proposed solution should have file level replication for associated application servers and DB log replication which is supported on the commonly used OS platforms and has inbuilt bandwidth compression.	
13	The proposed solution should have a file system analytics tool to give total file/directory count, typical scan time, number of open files, time of last replication for a file, file size & time stamp.	
14	The DR Monitoring and Management software must be running successfully in at least 30 large organizations.	
15	The DR Monitoring and Management software must be available in India market for more than 5 years and running in at least 15 large PSU/government organizations	
16	The main management server of the proposed should have a mechanism to have a local HA and remote, real time replica to eliminate any single point of failure and should not have any impact on the production in case the main management server fails.	
17	The DR Management solution should be tested and certified by an A2LA Accredited Organization to ensure that there are no security vulnerabilities which can be exploited.	
18	The DR management solution should have inbuilt debugging and log capture with facility to view the logs from the web based GUI itself.	
19	The DR Management solution should have a validation tool to verify DC-DR equivalence for OS, databases and applications with both out-of-box and custom templates.	
20	The DR Management solution should be cloud ready with at least 15 cloud customers and should be listed with a public cloud service provider like AWS.	
21	The DR management solution should be managing 3-way DR in at least 5 organisations	

7.4. Networking components

7.4.1. SAN Switch

Sr.No.	SAN Switch Specification	Complied Yes/No
1.	The fiber channel SAN switch must be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fiber channel switch'	
2.	The switch should be 48 ports and must be configured with license for 48ports , with license if necessary for ISL trunking	
3.	All 48* FC Ports for device connectivity should be 8/16 Gbps auto sensing Fiber Channel Ports loaded with 16 Gbps FC modules (Short Range)	
4.	The switch must have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.	
5.	The switch must be able to support non-disruptive software upgrade.	
6.	The switch must be able to support stateful process restart.	
7.	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience. Should offer built-in storage network management tool and SAN plug-and-play capabilities. This tool should simplify management of single or multiple switches and fabrics. For virtual infrastructure, it manages the entire path: from the virtual machine and switch to the physical storage.	
8.	Should support Power On Auto Provisioning (POAP) to automate software image upgrades and configuration file installation on newly deployed switches. Additionally, it should provide intelligent diagnostics, protocol decoding, network analysis tools	
9.	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances.	
10.	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.	
11.	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.	
12.	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), Port Zoning and LUN Zoning	
13.	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.	
14.	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.	
15.	The switch shall support the following Management Access Control	
	SSHv2	
	SNMPv3	
	IP ACLs	
16.	The switch must support the following fabric services:	
	Name server	
	Registered State Change Notification (RSCN)	
	Login services	

Sr.No.	SAN Switch Specification	Complied Yes/No
	Public loop	
	Broadcast	
	In-order delivery	
	Name server zoning	
17.	The switch must comply with the following FC standards: -	
	FC-PH, Revision 4.3	
	FC-PH-2, Revision 7.4	
	FC-PH-3, Revision 9.4	
	FC-GS-2, Revision 5.3	
	FC-GS-3, Revision 7.01	
	FC-FLA, Revision 2.7	
	FC-FG, Revision 3.5	
	FC-SW-2, Revision 5.3	
	FC-AL, Revision 4.5	
	FC-AL-2, Revision 7.0	
	FC-PLDA, Revision 2.1	
	FC-VI, Revision 1.61	
	FCP, Revision 12	
	FCP-2, Revision 7	
	FC-SB-2, Revision 2.1	
	FC-BB, Revision 4.7	
	FC-FS, Revision 1.9	
	FC-PI, Revision 13	
	FC-MI, Revision 1.99	
	FC-Tape, Revision 1.17	
	IP over Fiber Channel (RFC 2625)	
	Extensive IETF-standards-based TCP/IP, SNMPv3, and Remote Monitoring (RMON) MIBs	
	Class of service: Class 2, Class 3, Class F	
	Fiber Channel standard port types: E, F, FL	
	Fiber Channel enhanced port types: SD, TE	
18.	The switch must support port mirroring for both Fiber Channel and Gigabit Ethernet (802.3z), such that traffic going to a specific port can be mirrored and forwarded to another port for analyzing.	
19.	The switch must be able to immediately recover in the event of a failed forwarding path going via an alternative path.	
20.	The switch must also support load balancing across multiple paths through the fabric via Fabric Shortest Path First (FSPF).	
21.	Using FSPF, the switch must be able to load balance up to 16 equal cost paths across the SAN network.	

Sr.No.	SAN Switch Specification	Complied Yes/No
22.	The aggregated ports can reside across line-cards and chassis giving true distributed forwarding architecture	
23.	The switch must support the aggregation of any ports from any module.	
24.	Forwarding traffic must not be impacted when an individual ISL within an aggregated link goes down.	
25.	FSPF must not re-converge when an individual ISL within an aggregated link goes down.	
26.	The switch must be able to load balance traffic through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.	
27.	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.	
28.	The switch must be capable of discovering neighboring switches and identify the neighboring Fiber Channel or Ethernet switches.	
29.	The switch must support TACACS+ or RADIUS authentication when managing from GUI, console or telnet to prevent unauthorized access	
30.	The switch must support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch.	
31.	The switch must support multilevel security on console access prevents unauthorized users from altering the switch configuration.	
32.	The switch must support role-based administration by allowing different administrators different access rights to the switch. Role-based access control will use RADIUS or TACACS+ AAA functions.	
33.	The switch must support SNMPv3 for secured management.	
34.	Switch must support Fiber Channel Trace route and Fiber Channel Ping for ease of troubleshooting and fault isolation. In addition, the switch must also support the following diagnostics.	
	Power-on-self-test (POST) diagnostics	
	Online diagnostics	
	Internal loopbacks	
	Fabric Analyzer	
	SPAN	
	FC Debug	
	Syslog	
	Port level statistics	
35.	Switch must support out-band management protocols like SNMP, SNMPv3, SMI-S, Telnet, FTP and TFTP.	
36.	The switch must support the use of an external port analyzer, which is able to convert Fiber Channel frames to Ethernet frames so as to use a conventional Ethernet based packet analyzer to capture the traffic and analyze it as Fiber Channel.	
37.	For switch management, the management software must support both Fabric wide and Device level management without the additional purchase of software.	
38.	The switch must support SNMPv3—via Ethernet port and in-band IP-over-FC access	
39.	The Fabric Manager software must be able to perform	
	GUI based management, configuration and diagnostics.	

Sr.No.	SAN Switch Specification	Complied Yes/No
	Discovery and Topology Mapping	
	• Fabric View	
	• Summary View	
	• Physical View	
	• Configuration	
	• Monitoring and Alerts	
	• Network Diagnostics	
	• Configuration Wizards	
40.	The switch should support IPv6.	

7.4.2. Switching Fabric Architecture: Fabric Network Solution functional requirement & Specification:

Sr. No.	Feature Set	Complied (Yes/No)
1	**Fabric Definition**	
2	Fabric is an Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol, capable of adaption of SDN/NFV architecture in future.	
3	Fabric should have following functionalities to be achieved:	
4	**Flexibility :** allows workload mobility anywhere in the DC	
5	**Robustness :** while dynamic mobility is allowed on any authorised location of the DC, the failure domain is contained to its smallest zone	
6	**Performance:** full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active	
7	**Deterministic Latency :** fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale	
8	**Scalability :** add as many Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.	
9	Fabric should have Switch and Optics from same OEM.	
10	**Hardware and Interface Requirement**	
11	Fabric Connectivity should have the following properties:	
13	All switches including SPINE and leafs should be of line rate including access and uplink ports non-blocking	
1	**Fabric Features**	
2	In the fabric the oversubscription ratio of the connectivity between each leaf to SPINE switches should not be less than 4:1	
3	Fabric must support various Hypervisor encapsulation including VXLAN, NVGRE and 802.1q natively without any additional hardware/software or design change.	
4	Fabric must auto discover all the hardware and auto provision the fabric based on the policy.	
5	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.	
6	Fabric must provide open programmable interface using phython SDK, Jason SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.	
7	Fabric must provide open scripting interface from the central management appliance / SDN Controller for configuring the entire fabric.	
8	Fabric must support Role Based Access Control in order to support Multi - Tenant environment.	
9	Fabric must integrate with different virtual machine manager and manage virtualise networking from the single pane of Glass - NFV Fabric Controller/SDN Controller	
10	Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass –NFV Fabric Controller / SDN Controller	
11	Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between VM to VM, VM to Physical server and vise versa, Leaf to another leaf etc.	
12	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc	
13	Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation &Orchestration software.	
14	**Fabric Layer 2, Layer 3 and Misc. Features**	

Sr. No.	Feature Set	Complied (Yes/No)
15	Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc	
16	Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host	
17	Fabric must support Jumbo Frame upto 9K Bytes on 1G/10G/25G/40G/100G ports	
18	Fabric must support Layer 2 Multicast i.e. IGMP v1, v2 and v3	
19	Fabric must support IP v4 and IP v6 FHRP using HSRP or VRRP	
20	Fabric Must support IP v4 and IP v6 Layer 3 routing protocol OSPF and BGP	
21	Fabric must support IP v6 dual stack	
22	Fabric must support traffic redistribution between different routing protocol	
23	Fabric must support IP v4 and IP v6 management tools like - Ping, Traceroute, VTY, SSH, TFTP and DNS Lookup	
24	Fabric must support IP v4 and IP v6 SNMP V1 / V2 / V3	
25	Fabric must support integration with the centralised Syslog server for monitoring and audit trail	
26	Fabric must support NTP	
27	**Fabric Security Features**	
28	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service	
29	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD	
30	Fabric must support VM attribute based zoning and policy	
31	Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment	
32	Fabric must support true multi - tenancy	
33	Fabric must be accessible using CLI over SSH and GUI using HTTP/HTTPS	
34	Fabric must support SNMP v2/3 with HMAC-MD5 or HMAC-SHA authentication and DES encryption.	
35	Fabric must act as a State-less distributed firewall with the logging capability	
36	**Fabric Service Features**	
37	Fabric must be capable to provide services of L 4 - L7 services using physical or virual appliances i.e. Firewall, ADC, IPS etc.	
38	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service	
39	**Fabric Scale and Performance**	
40	Fabric should support scale up and scale out without any service disruption	
41	Fabric must support for 500 VRF/Private network without any additional component or upgrade or design change	
42	Fabric must scale from 100 Tenant to 500 Tenant without any additional component or upgrade or design change	
43	Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCenter, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator	
44	Fabric must be capable of connecting 2500 physical servers and scale to 5000 physical servers.	
45	Fabric must be capable of integrating minimum of 8 nos. of L 4 - L7 services physical or virual appliances (i.e. Firewall, ADC, IPS etc.) and scale upto 16 nos of L4 - L7 Services appliances.	
46	Fabric must support minimum of 220 Leaf switches and scale upto 250 Leaf switches without any design change.	

Sr. No.	Feature Set	Complied (Yes/No)
47	Fabric must support minimum of 2 Spine Switches and scale upto 6 Spine switches without any design change.	
48	Spine Switches must have adequate number of line rate 40/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 40/100 G ports connectivity i.e. Each Spine must have 128 nos. of line rate 40G/100G ports with consideration of leaf to SPINE over subscription ration of 4:1	
49	Fabric must support 20K IPv4 and 10K IPv6 routes scalable to 30K IPv4 and 15K IPv6 routes.	
50	Fabric must support 4K multicast groups scalable to 8K multicast groups.	
51	Fabric must support 256 nos. of MLAG/VPC scalable to 384 nos. Each MLAG/VPC must support maximum 8 member links.	
52	Fabric must support 256 nos. of Port Channel scalable to 384 nos. Each Port Channel must support maximum of 8 member links.	
53	**Fabric management**	
54	Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric.	
55	Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller.	
56	Centralised management appliance or SDN Controller must manages and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager.	
57	Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.	
58	Centralised management appliance or SDN Controller must provide necessary report for compliance and audit.	
59	Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX, OPENFLOW, OVSDB etc. or using Device APIs.	
60	Centralised management appliance or SDN Controller communication with the south bound devices must be encrypted	
61	Centralised management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in-path connectivity and out of band management connectivity	
62	Centralised management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.	
63	Centralised management appliance or SDN Controller must run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario	
64	In Event of all Centralised management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration.	
65	Centralised management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.	
66	Centralised management appliance or SDN Controller must support TACACS+, RADIUS, LDAP or Local Authentication. It must also provide an integration with the Syslog servers.	
Licensing & port requirement for both Leaf & Spine switch		
67	Bidder must quote appropriate license to enable and meet mentioned features in the fabric specification. Port calculation has been taken in consideration based on number of Application server /storage servers& any other components in the design like the firewall / IPS/ Load Balancers etc. and should be scalable to connect other equipment that NIC may desire to hook on to this fabric via leaf. Architecture should be designed with respect to high availability.	

7.4.3. Spine Switch Specification

Sr. No.	Feature Set	Complied (Yes/No)
A	**General Requirement**	
1	The switch OEM should be in the Gartner's Leader or Challenger Quadrant	
2	The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch. All the switches should be from same OEM	
3	The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.	
4	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
5	The switch should not have any single point of failure like CPU, supervisor, switching fabric power supplies and fans etc should have 1:1/N+1 level of redundancy	
6	Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch	
7	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.	
8	Switch with different modules should function line rate and should not have any port with oversubscription ratio applied	
9	Switch should support in service software upgrade of the switch without disturbing the traffic flow. There should not be any impact on the performance in the event of the software upgrade/downgrade. It should support in service patching of selected process/processes only without impacting other running processes	
10	Switch should support non blocking, wire speed performance per line card	
11	**Hardware and Interface Requirement**	
12	Switch should have the following interfaces:	
13	Sufficient nos. of line rate and Non - Blocking 40/100G ports	
14	Switch should have min 80MB buffer and atleast 16GB DRAM from Day 1 which should be field upgradable to atleast 32GB for future support	
15	Switch should have EAL2/NDPP certified	
16	Switch should have console port for local management	
17	Switch should have management interface for Out of Band Management	
18	Switch should be rack mountable and support side rails, if required	
19	Switch should have adequate power supplies for the complete system usage with all slots populated and used, providing N+1 redundancy	
20	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP	
21	Switch should support VLAN tagging (IEEE 802.1q)	
22	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy	
23	Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc and should support in service software upgrade including:	
24	a. Multiple System image	
25	b. Multiple system configuration	
26	c. Option of Configuration roll-back	
27	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/Link Aggregation Group (LAG) etc	
28	**Performance Requirement**	
29	The switch should support 1,20,000 IPv4 and IPv6 routes entries in the routing table with multicast routes	
30	Switch should support Graceful Restart for OSPF, BGP etc.	

Sr. No.	Feature Set	Complied (Yes/No)
31	Switch must support FCOE	
32	Switch should support minimum 1000 VRF instances	
33	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure	
34	The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG	
35	Switch should support total aggregate minimum 28 Tbps minimum of switching capacity including the services:	
36	a. Switching	
37	b. IP Routing (Static/Dynamic)	
38	c. IP Forwarding	
39	d. Policy Based Routing	
40	e. QoS	
41	f. ACL and Other IP Services	
42	g. IP V.6 host and IP V.6 routing	
43	**Virtualization Features**	
44	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890	
45	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	
46	Switch should support Open Flow/Open Day light/Open Stack controller	
47	Switch should support Data Center Bridging	
48	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically	
49	**Layer2 Features**	
50	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S	
51	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN	
52	Switch should support basic Multicast IGMP v1, v2, v3	
53	Switch should support minimum 90,000 no. of MAC addresses	
54	Switch should support 16 Nos. of link or more per Port channel (using LACP) and support 200 port channels or more per switch	
55	Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.	
56	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server. Spine to spine - minimum 16 port Multi Chasis etherchannel/LAG should be provided.	
57	Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports	
58	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
59	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
60	**Layer3 Features**	
61	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface	
62	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing	
63	Switch should support static and dynamic routing using:	
64	a. Static routing	
65	b. OSPF V.2 using MD5 Authentication	
66	c. ISIS using MD5 Authentication	
67	d. BGP V.4 using MD5 Authentication	
68	e. Should support route redistribution between these protocols	

Sr. No.	Feature Set	Complied (Yes/No)
69	f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)	
70	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols	
71	Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality	
72	Switch should be capable to work as DHCP server and relay	
73	Switch should provide multicast traffic reachable using:	
74	a. PIM-SM	
75	b. PIM-SSM	
76	c. Bi-Directional PIM	
77	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)	
78	e. IGMP V.1, V.2 and V.3	
79	Switch should support Multicast routing of minimum 16 way Equal Cost Multi Path load splitting	
80	**Availability**	
81	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
82	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP	
83	Switch should support for BFD For Fast Failure Detection as per RFC 5880 and RFC-7419, 3618, 7296, 7427, 7296.	
84	**Quality of Service**	
85	Switch system should support 802.1P classification and marking of packet using:	
86	a. CoS (Class of Service)	
87	b. DSCP (Differentiated Services Code Point)	
88	c. Source physical interfaces	
89	d. Source/destination IP subnet	
90	e. Protocol types (IP/TCP/UDP)	
91	f. Source/destination TCP/UDP ports	
92	Switch should support methods for identifying different types of traffic for better management and resilience	
93	Switch should support for different type of QoS features for ream time traffic differential treatment using	
94	a. Weighted Random Early Detection	
95	b. Strict Priority Queuing	
96	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
97	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
98	**Security**	
99	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail	
100	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
101	Time based ACL	
102	Switch should support for external database for AAA using:	
103	a. TACACS+	
104	b. RADIUS	
105	Switch should support MAC Address Notification on host join into the network for Audit trails and logging	

Sr. No.	Feature Set	Complied (Yes/No)
106	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
107	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
108	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes	
109	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
110	Switch should support Spanning tree BPDU protection	
111	Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed	
112	**Manageability**	
113	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
114	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
115	Switch should provide remote login for administration using:	
116	a. Telnet	
117	b. SSH V.2	
118	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
119	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
120	a. SNMP V1 and V.2	
121	b. SNMP V.3 with encryption	
122	c. Filtration of SNMP using Access list	
123	d. SNMP MIB support for QoS	
124	Switch should support for basic administrative tools like:	
125	a. Ping	
126	b. Traceroute	
127	Switch should support central time server synchronisation using Network Time Protocol NTP V.4	
128	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces	
129	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management	
130	Switch should provide different privilege for login in to the system for monitoring and management	
131	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding	
132	**IPv6 features**	
133	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as:	
134	a. OSPF V.3	
135	b. BGP with IP V.6	
136	c. IP V.6 Policy based routing	
137	d. IP V.6 Dual Stack etc	
138	e. IP V.6 Static Route	
139	f. IP V.6 Default route	
140	g. Should support route redistribution between these protocols	
141	Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode	

Sr. No.	Feature Set	Complied (Yes/No)
142	Switch should support for QoS in IP V.6 network connectivity	
143	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:	
144	a. SNMPv1, SNMPv2c, SNMPv3	
145	b. SNMP over IP V.6 with encryption support for SNMP Version 3	
146	Switch should support syslog for sending system log messages to centralised log server in IP V.6 environment	
147	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events	
148	Switch should support for IP V.6 different types of tools for administration and management such as:	
149	a. Ping	
150	b. Traceroute	
151	c. VTY	
152	d. SSH	
153	f. DNS lookup	

7.4.4. Leaf (Fibre) Switch Specification

Sr. No.	Feature Set	Complied (Yes/No)
A	**Solution Requirement**	
1	The switch OEM should be in the Gartner's Leader or Challenger Quadrant	
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy	
3	Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system	
4	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.	
5	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied	
6	**Hardware and Interface Requirement**	
7	Switch should have the following interfaces:	
8	a. 48 x 10G/25G Multi Mode Fiber Interface	
9	b. 6 x 40/100GbE QSFP ports	
10	Switch should be EAL2/NDPP Certified	
11	Switch must support FCOE	
12	Switch should support native 25G OR via breakout	
13	Switch should have console port	
14	Switch should have management interface for Out of Band Management	
15	Switch should be rack mountable and support side rails if required	
16	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP	
17	Switch should support VLAN tagging (IEEE 802.1q)	
18	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy	
19	Switch should support Configuration roll-back and check point	
20	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc	
21	**Performance Requirement**	

Sr. No.	Feature Set	Complied (Yes/No)
22	The switch should support 12,000 IPv4 and atleast 6000 IPv6 routes entries in the routing table with 8000 multicast routes	
23	Switch should support Graceful Restart for OSPF, BGP etc.	
24	Switch should support minimum 1000 VRF instances	
25	The switch should have at least 16GB DRAM from Day 1 with optional support upgrade to 24 GB	
26	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure	
27	The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG	
28	Switch should support minimum 1.4 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services:	
29	a. Switching	
30	b. IP Routing (Static/Dynamic)	
31	c. IP Forwarding	
32	d. Policy Based Routing	
33	e. QoS	
34	f. ACL and Other IP Services	
35	g. IP V.6 host and IP V.6 routing	
36	Each leaf should have connectivity to all spine switches and the over subscription should not be less then 4:1	
37	**Advance Features**	
38	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890	
39	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	
40	Switch should support OpenFlow/Open Day light/Open Stack controller	
41	Switch should support Data Center Bridging	
42	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	
43	**Layer2 Features**	
44	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S	
45	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN	
46	Switch should support basic Multicast IGMP v1, v2, v3	
47	Switch should support minimum 90,000 no. of MAC addresses	
48	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch	
54	**Layer3 Features**	
55	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface	
56	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing	
57	Switch should support static and dynamic routing using:	
64	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols	
65	Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality	
66	Switch should be capable to work as DHCP server and relay	
67	Switch should provide multicast traffic reachable using:	
68	a. PIM-SM	
69	b. PIM-SSM	
70	c. Bi-Directional PIM	

Sr. No.	Feature Set	Complied (Yes/No)
71	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)	
72	e. IGMP V.1, V.2 and V.3	
73	Switch should support Multicast routing of minimum 16 way Equal Cost Multi Path load splitting	
74	**Availability**	
75	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
76	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP	
77	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
78	**Quality of Service**	
79	Switch system should support 802.1P classification and marking of packet using:	
	a. CoS (Class of Service)	
	b. DSCP (Differentiated Services Code Point)	
	c. Source physical interfaces	
	d. Source/destination IP subnet	
	e. Protocol types (IP/TCP/UDP)	
	f. Source/destination TCP/UDP ports	
86	Switch should support methods for identifying different types of traffic for better management and resilience	
89	b. Strict Priority Queuing	
90	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
91	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
92	**Security**	
93	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail	
94	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
95	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4	
96	Switch should support for external database for AAA using:	
97	a. TACACS+	
98	b. RADIUS	
99	Switch should support MAC Address Notification on host join into the network for Audit trails and logging	
100	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
101	Switch should support DHCP Snooping	
102	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
103	Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN	
104	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
105	Switch should support to prevent edge devices in the network not	

Sr. No.	Feature Set	Complied (Yes/No)
	administrator's controlled from becoming Spanning Tree Protocol root nodes	
106	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
109	**Manageability**	
110	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
111	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
112	Switch should provide remote login for administration using:	
113	a. Telnet	
114	b. SSH V.2	
115	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
116	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
117	a. SNMP V1 and V.2	
118	b. SNMP V.3 with encryption	
119	c. Filtration of SNMP using Access list	
120	d. SNMP MIB support for QoS	
127	Switch should provide different privilege for login in to the system for monitoring and management	
128	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding	
129	**IPv6 features**	
130	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such	
131	a. OSPF V.3	
132	b. BGP with IP V.6	
133	c. IP V.6 Policy based routing	
134	d. IP V.6 Dual Stack etc	
135	e. IP V.6 Static Route	
136	f. IP V.6 Default route	
137	g. Should support route redistribution between these protocols	
138	Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode	
139	Switch should support for QoS in IP V.6 network connectivity	
140	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:	
141	a. SNMPv1, SNMPv2c, SNMPv3	
142	b. SNMP over IP V.6 with encryption support for SNMP Version 3	
143	Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment	
144	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events	
145	Switch should support for IP V.6 different types of tools for administration and management such as:	
146	a. Ping	
147	b. Traceroute	
148	c. VTY	
149	d. SSH	
150	f. DNS lookup	

7.4.5. Leaf (Fibre) Switch Specification

Sr. No.	Feature Set	Complied (Yes/No)
A	**Solution Requirement**	
1	The switch OEM should be in the Gartner's Leader or Challenger Quadrant	
2	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
3	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy	
4	Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system	
5	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.	
6	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied	
7	Throughput of 2.53 Tbps	
8	24 x 40 GE ports + 4 X 40G/100G ports	
9	Latency 2 microseconds	
10	The switch should support 12,000 IPv4 and IPv6 routes entries in the routing table with 8000 multicast routes	
11	The switch should have at least 24GB DRAM from Day 1	
12	The switch should have support for at least 1000 VRF	
14	The switch OEM should be in the Gartner's Leader or Challenger Quadrant	
15	The switch should have support for FCOE ports	
16	Should support VXLAN EVPN	
17	**Advance Features**	
18	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890	
19	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	
20	Switch should support Open-Flow/Open Day light/Open Stack controller	
21	Switch should support Data Center Bridging	
22	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	
23	**Availability**	
24	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
25	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP	
26	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
27	**Quality of Service**	
28	Switch system should support 802.1P classification and marking of packet using:	
29	a. CoS (Class of Service)	
30	b. DSCP (Differentiated Services Code Point)	
31	c. Source physical interfaces	
32	d. Source/destination IP subnet	
33	e. Protocol types (IP/TCP/UDP)	
34	f. Source/destination TCP/UDP ports	
35	Switch should support methods for identifying different types of traffic for better management and resilience	
36	b. Strict Priority Queuing	

Sr. No.	Feature Set	Complied (Yes/No)
37	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
38	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
39	**Manageability**	
40	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
41	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
42	Switch should provide remote login for administration using:	
43	a. Telnet	
44	b. SSH V.2	
45	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
46	**IPv6 features**	
47	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such	
48	a. OSPF V.3	
49	b. BGP with IP V.6	
50	c. IP V.6 Policy based routing	
51	d. IP V.6 Dual Stack etc	
52	e. IP V.6 Static Route	
53	f. IP V.6 Default route	

7.4.6. Leaf (Copper) Switch Specification

Sr. No.	Feature Set	Complied (Yes/No)
A	**Solution Requirement**	
1	The switch OEM should be in the Gartner's Leader or Challenger Quadrant	
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy	
3	Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system	
4	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.	
5	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied	
1	**Hardware and Interface Requirement**	
2	Switch should have the following interfaces:	
3	a. 48 x 1G/10G Rj45 Interface	
4	b. 6 x 40 QSFP ports	
7	Switch should be EAL2/NDPP Certified	
	Switch must support FCOE	
8	Switch should have console port	
9	Switch should have management interface for Out of Band Management	
10	Switch should be rack mountable and support side rails if required	
11	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP	
12	Switch should support VLAN tagging (IEEE 802.1q)	
13	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy	
14	Switch should support Configuration roll-back and check point	
15	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc	
16	**Performance Requirement**	
17	The switch should support 12,000 IPv4 and atleast 6000 IPv6 routes entries in the routing table with 8000 multicast routes	
18	Switch should support Graceful Restart for OSPF, BGP etc.	
19	Switch should support minimum 1000 VRF instances	
	The switch should have at least 16GB DRAM from Day 1 with optional support upgrade to 24 GB	
20	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure	
21	The switch should support hardware based load-balancing at wire speed using LACP and multi chassis ether-channel/LAG	
22	Switch should support minimum 1.4 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services:	
23	a. Switching	
24	b. IP Routing (Static/Dynamic)	
25	c. IP Forwarding	
26	d. Policy Based Routing	
27	e. QoS	
28	f. ACL and Other IP Services	

Sr. No.	Feature Set	Complied (Yes/No)
29	g. IP V.6 host and IP V.6 routing	
30	Each leaf should have connectivity to all spine switches and the over subscription should not be less then 4:1	
31	**Advance Features**	
32	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890	
33	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	
34	Switch should support OpenFlow/Open Day light/Open Stack controller	
35	Switch should support Data Center Bridging	
36	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	
37	**Layer2 Features**	
38	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S	
39	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN	
40	Switch should support basic Multicast IGMP v1, v2, v3	
41	Switch should support minimum 90,000 no. of MAC addresses	
42	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch	
43	Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.	
44	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server	
45	Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports	
46	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
47	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
48	**Layer3 Features**	
49	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface	
50	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing	
51	Switch should support static and dynamic routing using:	
52	a. Static routing	
53	b. OSPF V.2 using MD5 Authentication	
54	c. ISIS using MD5 Authentication	
55	d. BGP V.4 using MD5 Authentication	
56	e. Should support route redistribution between these protocols	
57	f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)	
58	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols	
59	Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality	
60	Switch should be capable to work as DHCP server and relay	
61	Switch should provide multicast traffic reachable using:	
62	a. PIM-SM	
63	b. PIM-SSM	
64	c. Bi-Directional PIM	
65	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)	
66	e. IGMP V.1, V.2 and V.3	

Sr. No.	Feature Set	Complied (Yes/No)
67	Switch should support Multicast routing of minimum 16 way Equal Cost Multi Path load splitting	
68	**Availability**	
69	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
70	Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP	
71	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
72	**Quality of Service**	
73	Switch system should support 802.1P classification and marking of packet using:	
74	a. CoS (Class of Service)	
75	b. DSCP (Differentiated Services Code Point)	
76	c. Source physical interfaces	
77	d. Source/destination IP subnet	
78	e. Protocol types (IP/TCP/UDP)	
79	f. Source/destination TCP/UDP ports	
80	Switch should support methods for identifying different types of traffic for better management and resilience	
81	Switch should support for different type of QoS features for ream time traffic differential treatment using	
82	a. Weighted Random Early Detection	
83	b. Strict Priority Queuing	
84	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
85	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
86	**Security**	
87	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail	
88	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
89	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4	
90	Switch should support for external database for AAA using:	
91	a. TACACS+	
92	b. RADIUS	
93	Switch should support MAC Address Notification on host join into the network for Audit trails and logging	
94	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
95	Switch should support DHCP Snooping	
96	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
97	Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN	
98	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	

Sr. No.	Feature Set	Complied (Yes/No)
99	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes	
100	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
101	Switch should support Spanning tree BPDU protection	
102	Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed as per banks ISD rules	
103	**Manageability**	
104	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
105	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
106	Switch should provide remote login for administration using:	
107	a. Telnet	
108	b. SSH V.2	
109	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
110	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
111	a. SNMP V1 and V.2	
112	b. SNMP V.3 with encryption	
113	c. Filtration of SNMP using Access list	
114	d. SNMP MIB support for QoS	
115	Switch should support for basic administrative tools like:	
116	a. Ping	
117	b. Traceroute	
118	Switch should support central time server synchronization using Network Time Protocol NTP V.4	
119	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces	
120	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management	
121	Switch should provide different privilege for login in to the system for monitoring and management	
122	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding	
123	**IPv6 features**	
124	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such	
125	a. OSPF V.3	
126	b. BGP with IP V.6	
127	c. IP V.6 Policy based routing	
128	d. IP V.6 Dual Stack etc	
129	e. IP V.6 Static Route	
130	f. IP V.6 Default route	
131	g. Should support route redistribution between these protocols	
132	Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode	
133	Switch should support for QoS in IP V.6 network connectivity	
134	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:	
135	a. SNMPv1, SNMPv2c, SNMPv3	

Sr. No.	Feature Set	Complied (Yes/No)
136	b. SNMP over IP V.6 with encryption support for SNMP Version 3	
137	Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment	
138	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events	
139	Switch should support for IP V.6 different types of tools for administration and management such as:	
140	a. Ping	
141	b. Traceroute	
142	c. VTY	
143	d. SSH	
145	f. DNS lookup	

7.4.7. Application & Gateway Switch:

Sr. No.	Feature Set	Complied (Yes/No)
1	48 Ethernet 1G BASE-T , 2 x10G/25G SFP+ ports, 2 X 40G/100G for future expansion	
2	Redundant Power supply	
3	Aggregate throughput – 300 Gbps	
4	Configurable at least 16000 MAC addresses	
5	Access Control List (ACL) support , ARP support , Auto-negotiation , Auto-uplink (auto MDI/MDI-X), DHCP snooping , Dynamic ARP Inspection (DAI), IGMP snooping , IPv4 support , IPv6 support , Layer 3 load balancing , Link Aggregation Control Protocol (LACP) , MLD snooping , Multiple Spanning Tree Protocol (MSTP) support , Quality of Service (QoS) , RADIUS support , Rapid Spanning Tree Protocol (RSTP) support, Shaped Round Robin (SRR) , STP Root Guard , Syslog support , Trivial File Transfer Protocol (TFTP) support , VLAN support Should have IPv6 Ready Logo	
6	Remote management Support for CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , SSH , TelnetAccess Control List (ACL) support , ARP support , Auto-negotiation , DHCP snooping , Dynamic ARP Inspection (DAI), IGMP snooping , IPv4 support , IPv6 support , Layer 3 load balancing , Link Aggregation Control Protocol (LACP) , MLD snooping , Multiple Spanning Tree Protocol (MSTP) support , Quality of Service (QoS) , RADIUS support , Rapid Spanning Tree Protocol (RSTP), STP Root Guard , Syslog support , Trivial File Transfer Protocol (TFTP) support , VLAN support, Should have be IPv6 Ready Logo	
7	Routing Protocol support BGP-4 , IS-IS , OSPFv3 , PIM-SM , PIM-SSM , RIP-1 , RIP-2 , RIPngRemote management Support for CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , SSH , TelnetAccess Control List (ACL) support , ARP support , Auto-negotiation , Auto-uplink (auto MDI/MDI-X), DHCP snooping , Dynamic ARP Inspection (DAI), IGMP snooping , IPv4 support , IPv6 support , Layer 3 load balancing , Link Aggregation Control Protocol (LACP) , MLD snooping , Multiple Spanning Tree Protocol (MSTP) support , Quality of Service (QoS) , RADIUS support , Rapid Spanning Tree Protocol (RSTP) support, Shaped Round Robin (SRR) , STP Root Guard , Syslog support , Trivial File Transfer Protocol (TFTP) support , VLAN support	
8	Inter-VLAN IP routing should be supported for Layer 3 routing between two or more VLANs.Routing Protocol support BGP-4 , IS-IS , OSPFv3 , PIM-SM , PIM-SSM , RIP-1 , RIP-2 , RIPngRemote management Support for CLI , RMON 1 , RMON 2 , SNMP 1 , SNMP 2c , SNMP 3 , SSH , Telnet	
9	Inter-VLAN IP routing should be supported for Layer 3 routing between two or more VLANs.Routing Protocol support BGP-4 , IS-IS , OSPFv3 , PIM-SM , PIM-SSM , RIP-1 , RIP-2 , RIPng, VXLAN, EVPN	
10	Inter-VLAN IP routing should be supported for Layer 3 routing between two or more VLANs.	
11	The Switch should be NDPP/EAL2 Certified.	

7.4.8. IP KVM Switches

Sr. No.	Specifications	Complied (Yes/ No)
1	It should have a minimum of 16 ports	
2	It should support 4 remote users and 1 user at the rack with 16 ports	
3	It should take control of servers at BIOS Level	
4	It should facilitate both in-band & out-of band access	
5	It should be able to integrate with intelligent power strips, so as to be able to reset power of remote device at port level.	
6	Remote access of both Servers and serial devices such as routers (through same or different appliances).	
7	It should have facility to integrate with secure management device	
8	Gigabit Ethernet ports.	
9	Virtual Media Support of multiple media including 'ISO image' files	
10	Dual (redundant) Power supply	
11	Dual Ethernet with Failover	
12	PC selection – On screen Display menu hot key	
13	19 inch Rack mountable design	
14	KVM access over IP	
15	Browser based Management available at both remote and local (Supported Browsers = Internet Explorer for MS-Windows, Firefox for MS-Windows and Linux)	
16	Support for resolution of 1600*1200	
17	Single window access to all equipment.	
18	Equipment access logs and event history and send email alerts based on logs details as triggers	
19	Logging should be centralized in one Syslog server.	
20	External telephone or cellular model for emergency access	
21	Perfect mouse synchronization without changing server mouse settings	
22	Connect via LAN, WAN, modem or Internet	
23	Native Windows and Java clients support Windows, Linux, Sun and Mac users	
24	Multi-browser access for Internet Explorer, Chrome, and Firefox access	
25	**Server Connectivity Modules** available for PS/2, USB and USB with virtual media,	
26	**Server Connectivity Modules** supporting analog VGA video, HDMI	
27	Support for Dell, HP, Cisco, and IBM blade servers	
28	Support for up to 1,024 servers **directly or optionally through Any Centralized Management appliance / Software**	
29	256-bit AES encryption	
30	Dual power supplies	
31	All data encrypted, including video transmissions and virtual media	
32	Local or centralized authentication via LDAP, AD, and via RADIUS.	
33	Dual-stack networking: IPv4 and IPv6	
34	Configurable user and group permissions	
35	User-configurable TCP ports	
36	Supports strong password protection	
37	**It should be able to display the desktops of all connected 16 servers in one single screen in a grid manner**	
38	Utilize existing digital security certificates	
39	SNMP v2 and v3 management, Syslog, Email alerts	

7.4.9. Non IP KVM Switches

Sr. No.	Specifications	Complied (Yes/ No)
1	It should be rack-mountable.	
2	It should have a minimum of 16 ports	
3	It should support local user port for rack access	
4	It should support both USB and PS/2 connections.	
5	It should be capable of storing username and profiles.	
6	It should support high resolution 1280 x 1024	
7	It should be capable to auto scan servers	
8	It should work on CAT 6 / CAT 7 cables.	
9	1 U Rack Mount	
10	Display size: Minimum 15 inches diagonal	
11	Display colors: 16 million	
12	Resolution: SXGA 1280 x 1024	
13	Compatible to both PS/2 and USB based inputs	

7.4.10. Link Load Balancer

Sr. No.	Specification	Compliance (Yes/No)
1.00	**Architecture**	
1.01	Should be high performance purpose built next generation multi-tenant hardware with multicore CPU support. Platform should support multiple services including link load balancing with application security and secure remote access VPN functions with dedicated hardware resources for each virtual instance.	
1.02	The appliance should have minimum 4x10G SFP+ dataplane interfaces and 1*10/100/1000 copper management interface from day one	
1.03	Next generation multi-tenant platform must support traffic isolation, fault isolation and network isolation in order to meet the architectural environment. Each virtual instance/tenant must have assigned dedicated hardware resources including I/O interfaces, memory, CPU in order to have predictable performance.	
1.04	Platform should support at least 2 virtual instances and scalable to support 4 virtual instance from day one, in order to cater current and future requirements.	
1.05	All the below mentioned Specifications – per virtual instance- are minimum. The Proposed Solution should have capacity to meet the future requirements.	
2.00	**For link Load balancer instance – at perimeter zone**	
2.01	Link Load balancer instances should have minimum 10 Gbps of system throughput with all link balancing and security functions enabled.	
2.02	Layer 4 connection Per second should not be less than 100K	
2.03	1M concurrent connections	
2.04	Dedicated Management Interface	
2.05	Integrated web application security protection against layer7 attacks	
3.00	**Remote access instance – at DMZ zone**	
3.01	Number of concurrent users – 500 scalable to support 1000 users	
3.02	SSL throughput MIN 500Mbps	
4.00	**Link Load balancing features**	
4.01	Support for multiple internet links in Active-Active load balancing and active-standby failover mode.	
4.02	Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, hash IP , target proximity and dynamic detect?	
4.03	Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links.	
4.04	IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.	
4.05	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation	
4.06	Domain name support for outbound link selection for FQDN based load balancing.	
4.07	Dynamic detect (DD) based health check for intelligent traffic routing and failover	
4.08	In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.	
4.09	Shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.	
4.10	Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.	
4.11	Should support persistency features including RTS (return to sender) and ip flow persistence.	
4.12	Application Performance	
4.13	Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation.	
4.14	Should support TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed.	

Sr. No.	Specification	Compliance (Yes/No)
4.15	TCP optimization option configuration must be defined on per virtual service basis not globally.	
4.16	Software based compression for HTTP based application, support and high speed HTTP processing on same appliance.	
4.17	Should support QOS for traffic prioritization, borrow and unborrow bandwidth from queues.	
4.18	Should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols.	
4.19	Should support rate shaping for setting user defined rate limits on critical application.	
5.00	**Network and application security**	
5.01	Must protect web application against parameter tampering and must have inbuilt controls to block invalid files, filtering of sensitive words in HTTP request and response.	
5.02	Network based security policies for detection and prevention of layer3 attacks	
5.03	Prevention of DOS/DDOS attack with rate limiting security policies	
6.00	**Remote access**	
6.01	SSL VPN solution should be 100% client less for web based applications	
6.02	must support for CIFS file share and provision to browse, create and delete the directories through web browser	
6.03	Should maintain original server access control policies while accessing the file resources through VPN	
6.04	must support Single Sign-On (SSO) for web based applications and web based file server access	
6.05	Should have secure access solutions for mobile PDAs, Android smart phones, I-pad, I-phones.	
6.06	Should Support IPV6	
6.07	SSL VPN solution must provide machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources.	
6.08	Should support following Authentication methods: - LDAP, Active directory, Radius, secure-ID, local database, and certificate based authentication and anonymous access.	
7.00	**Management**	
7.01	Centralized management appliance should have extensive reporting and logging with inbuilt TCP dump like tool and log collecting functionality	
7.02	Solution Should Support Restful API	
7.03	The appliance should have SSH CLI, Direct Console, SNMP and Single Console per Cluster with inbuilt reporting.	
7.04	Should support XML-RPC for integration with 3rd party management and monitoring	
7.05	Should support role based access control with different privilege levels for configuration management and monitoring.	
7.06	The appliance should provide detailed logs and graphs for real time and time based statistics	
8.00	**OEM Criteria**	
9.00	**OEM must have presence in INDIA from last 5 years**	
10.00	**OEM must have local TAC support in INDIA and must have executed at least 5 internet load balancing projects in INDIA**	
11.00	**The proposed load balancing vendor should be present in Gartner's Leader Magic Quadrant / IDC / Frost and Sullivan.**	

7.5. Security Devices for WBSDC:

7.5.1. URL Filter

Sr.No.	URL Filter Specifications	Complied (Yes/No)
1.	Appliance Should have license for Handling 100 concurrent users and in HA (Active-Active or Active-Passive Mode	
2.	URL Filter must be able to configure rules based on the following parameter a) Source/Destination IP/Port b) Time and date access c) User/group role (After Integration with AD) d) Customizable services e) Application (not port) f) QoS g) Geolocation, Country h)Combination of one or multiple of above mentioned parameter	
3.	The URL Filter must be able to filter traffic even if the packets are fragmented.	
4.	It must support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.	
5.	It must be able to control Instant Messaging like Yahoo, MSN, and ICQ, Skype etc. (SSL and HTTP tunneled).	
6.	It must enable blocking of Peer to Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC etc. (over HTTP) and anonymous proxies like Ultra Surf, Tor etc.	
7.	URL Filter must support Access for Granular user, group & policy enforcement.	
8.	Identity Awareness must work in conjunction with Application Control i.e. the solution must able to control user access to various applications based on active directory group membership.	
9.	Should interface with a SIEM to provide the Log data	
10.	URL Filter must support Identity Access for Granular user, group and policy enforcement.	

7.5.2. Next Generation Firewall with Intrusion Prevention System

Sr. No.	Description	Complied (Yes/No)
1	**Note :The Firewall proposed should be from OEMs who are in Leaders and Challengers Quadrant in Gartner's Magic Quadrant on NGFW for at least 2 years in the last three years. (13-14, 14-15, 16-17). Since SDC already has Checkpoint and Fortigate deployed, as a matter of security best practices, their products should NOT be offered**	
2	**Industry Certifications and Evaluations**	
2.1	Firewall solution offered from OEM must satisfy the conditions stipulated above in the Note.	
3	**Hardware Architecture**	
3.1	The appliance based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance	
3.2	The appliance should have at least 8 * (1G / 10G) ports and support 4 * 40 G ports from Day one. The Firewall should be loaded with 10G SR modules as mentioned in BoQ	
3.3	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory	
3.4	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.	
4	**Performance & Scalability**	
4.1	Should support at least 10 Gbps of NGFW performance throughput (includes FW, Application Visibility & IPS)	
4.2	NG Firewall should support at least 4,000,000 concurrent sessions	
4.3	NG Firewall should support at least 60,000 connections per second with Application visibility	
4.4	NG Firewall should support at least 1000 VLANs	
5	**High-Availability Features**	
5.1	Firewall should support Active/Standby failover and minimum 10 virtual Firewalls	
5.2	Firewall should support ether channel functionality for the failover control & date interfaces for provide additional level of redundancy	
5.3	Firewall should support redundant interfaces to provide interface level redundancy before device failover	
5.4	Firewall should support 802.3ad Ether channel functionality to increase the bandwidth for a segment.	
5.5	Firewall should have integrated redundant power supply	
5.6	Firewall should have redundant hot-swappable FANs	
6	**Next Generation Firewall Features**	
6.1	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	
6.2	Firewall should support operating in routed & transparent mode	
6.3	Should support Static, RIP, OSPF, OSPFv3 and BGP	
6.4	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	
6.5	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
6.6	Firewall should support Multicast protocols like IGMP, PIM, etc.	
6.7	Should support security policies based on security group names in source or destination fields or both	
6.8	Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc.	
6.9	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
6.10	Should be capable of automatically providing the appropriate inspections and protections	

Sr. No.	Description	Complied (Yes/No)
	for traffic sent over non-standard communications ports.	
6.11	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
6.12	Should be capable of detecting and blocking IPv6 attacks.	
6.13	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor	
6.14	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.	
6.15	Should must support URL and DNS threat intelligence feeds to protect against threats	
6.16	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	
6.17	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
6.18	Should support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	
6.19	NGFW OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	
6.20	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
6.21	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
6.22	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
6.23	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
7	**Management**	
7.1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software. The Management Platform must be a Hardware Appliance with Support of Managing 10 devices.	
7.2	The management platform must provide a highly customizable dashboard.	
7.3	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
7.4	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
7.5	Should support REST API for monitoring and configure programmability	
7.6	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
7.7	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
7.8	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
7.9	The management platform must risk reports like advanced malware, attacks and network	
7.10	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	

7.5.3. Web Application Firewall& Load Balancer:

Sr. No		NextGeneration web application firewall with load balancer	Complied (Yes/No)
Attribute	-	**Specifications**	-
Requirements of the proposed Cloud platform	1	SI has to design next generation datacenter in order to meet the modern networking requirements including software define networking, network function virtualization, agility, portability & programmability. SI has to ensure multiple network functions to consolidated on purpose built hardware	
	2	Multi-tenancy with Traffic isolation	
	3	Guaranteed performance – dedicated hardware resources including vCPU's, I/O, memory, SSL card , per virtual function , SR-IOV (Single Root –I/O Virtualization) , open vSwitch	
	4	REST-API/Cloud API support for integration with centralized orchestration, cloud platform, and elasticity	
	5	Support for multiple network functions on single platform depending on throughput and capacity requirements per virtual functions	
	6	Support for multiple network functions including application firewall and reverse proxy with application load balancing on same platform.	
	7	The appliance should have minimum 10 x1/10G SFP+ data interfaces from day one	
	8	The appliance should support Minimum 64GB RAM, 2*SSL ASICS/FGPA/cards with SSL I/O virtual function support for guaranteed SSL performance and 2TB HDD	
		Minimum performance specifications	
Performance	9	Should be high performance purpose built next generation multi-tenant hardware with multicore CPU support. Platform should support multiple network functions including application load balancing, application firewall network functions with dedicated hardware resources for each virtual functions.	
	10	Platform should support at least two network functions in order to cater current and future requirements and performance numbers including throughput, connections, SSL throughput and SSL transactions must be per virtual instance.	
	11	For reverse proxy & Load balancer – network function	
		1. Min 18Gbps of system throughput, 10Gbps of SSL throughput	
		2. Minimum of 5M concurrent connection	
		3. Minimum of 10K SSL transaction Per Second per instance	
		4. Dedicated Management Interface	
	12	For Web Application Firewall – network function	
		1. There should be dedicated instance for Web Application Firewall with at least 1.6 Gbps of layer7 throughput.	
		2. Platform should have capacity to accommodate at least one additional instance of same capacity for all network functions mentioned above or 2 x numbers of instances with 50% capacity mentioned above.	
		Functional specifications - Web Application Firewall	
Functional	13	Meet all applicable PCI DSS requirements pertaining to system components and react appropriately (defined by active policy or rules) to threats against relevant vulnerabilities. Platform should be scalable to accommodate more WAF function to meet the performance requirements.	

Sr. No		NextGeneration web application firewall with load balancer	Complied (Yes/No)
Attribute	-	Specifications	-
	14	The Web application firewall should support positive security model with machine learning capabilities to detect and prevent vulnerabilities and anomalies in application traffic and unknown attacks. Machine learning should be based on true ML algorithms, and not just automation of dynamically learnt rules	
	15	New modules of applications should be learnt dynamically, and WAF should also provide the option of deploying the rules learnt dynamically for these new modules without manual intervention.	
	16	WAF positive security model should be intelligent to adapt changes to existing modules of application or dynamically handle new modules without any manual learning and fine-tuning	
	17	The Web application firewall should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), nonstandard encoding and Session Management. Protection from CSRF attacks by Adding a CSRF token to application responses and blocking of POST requests with a missing or incorrect CSRF token	
	18	The Web application firewall should address unknown attacks based on user inputs and application responses using combination of dedicated protectors/signature engines and Machine Learning	
	19	WAF should support built-in correlation engine to detect atomic attacks and complex attack chains. Administrator should have option to define customized correlation rules	
	20	Administrator should have option to define customized correlation rules, edit and create new correlation rules	
	21	WAF correlation should also identify complex attack chains, and not just aggregate events based on attacks or sources.	
	22	Correlation should not be just an aggregation of multiple events, but detail the classification, prioritization and aggregation	
	23	Advanced bot detection mechanism based on smart combination of signature-based and heuristic analysis.	
	24	WAF should be able to provide retrospective analysis of web application attacks either by consuming relevant log files or PCAP files.	
	25	Should be able to take in virtual patching information from Static Analyzers, not Dynamic scanners	
Virtual Patching with static code analysis	26	This module can be proposed as integrated on WAF or dedicated solution to ensure better, improved and accurate working Virtual Patch,	
	27	App firewall should have capability to scan source code using static analyzers (not dynamic scanners) and deploy patches locally	
	28	The solution is required to provide SAST, DAST and IAST approaches to application testing Support PHP, C#, Java and other web based applications	
Reverse proxy and application load balancing	29	Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support. Reverse proxy and WAF should be from different OEM to ensure reduced surface attack area and maximum security	
	30	The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.	
	31	Support for policy nesting at layer7 and layer4, solution should able to combine layer4 and layer7 policies to address the complex application integration.	

Sr. No		NextGeneration web application firewall with load balancer	Complied (Yes/No)
Attribute	-	Specifications	-
	32	Traffic load balancing using e-Policies should support algorithms including round robin, least connections, shortest response, persistence IP, hash IP, hash IP and port, consistent hash IP and snmp	
	33	Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.	
	34	Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.	
	35	should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers	
	36	Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..	
	37	Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.	
	38	Device level HA should support synchronization of network functions configuration from primary/master device to secondary/slave device	
Management	39	The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.	
	40	The appliance should provide detailed logs and graphs for real time and time based statistics	
	41	Should capture, log and display traffic related data to analyze for security incidents.	
	42	Should support XML-RPC, REST-API, Centralized orchestration for integration with 3rd party management and monitoring of the devices.	
	43	The appliance should have extensive report and logging with inbuilt TCP dump like tool and log collecting functionality	
	44	Should be able to send security incidents via syslog	
	45	OEM should have deployed similar solution in INDIA and must have presence in INDIA from last 5 years	
OEM Criteria	46	The proposed OEM should be present in India and should have TAC in India Since last 5 years. Documentary proof of the same needs to be provided	
	47	The OEM (s) should be an established, industry player and should, form a part of the Industry standard, leader's/challenger's quadrant/EAL levels, on the likes of Gartner, Forrester, IDC, ICSA, Common Criteria etc.	

7.5.4. L-7 Anti-DDos Solution

Sr. No	Specification	Complied (Yes/No)
	System Stability and Reliability	
1	The Vendor should guarantee the stability and the reliability of hardware system such as CPU, memory, interface, and software like OS	
2	The proposed Equipment must make sure the DDOS mitigation devices can work independently when there is any problem happened in the DDOS detector.	
3	The proposed Equipment shall be appliance based with fully hardened and secured Operating System (OS).	
	System functions & requirement	
6	The proposed Equipment shall support at minimum of: 8 X 10GE SFP+ port and 1 x Console port	
7	Mitigation capacity of System should be at least 40Gbps & 25,550,000 pps	
8	System should support service availability through functions of service monitoring and protection from DDoS traffic	
9	System should be stable and not be affect service availability even upon any system fault	
10	System should support 'Troubleshooting function' for each system function	
11	System should provide in-line mode and Diversion(off-ramping)/Re-injection(on-ramping) mode for detecting and protecting DDos traffic.	
12	System should detect any DDoS traffic and mitigate any DDoS attack without interrupt legitimate traffic and customer services.	
13	The Proposed system must be able to detect volumetric DDOS traffic and start mitigate volumetric DDOS traffic within 3 min.	
14	System should provide IP reputation list protection to filter blacklisted IP.	
15	Systems should consists of Detector, Mitigator and Management device.	
16	System should provide user defined signatures	
17	System should support detection and protection of DDoS traffic as below: IP Spoofed/Non-spoofed TCP Syn Flooding IP Spoofed/Non-spoofed TCP Syn-ACK Flooding IP Spoofed/Non-spoofed TCP FIN Flooding IP Spoofed/Non-spoofed UDP Flooding IP Spoofed/Non-spoofed ICMP Flooding HTTP GET Flooding HTTP POST Flooding HTTPS Flooding DNS Query Flooding SIP Flooding DNS amplification NTP amplification SSDP amplification Chargen amplification SNMP amplification	
18	System should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and should support a function of exclusion for specific network.	
19	System should support a function 'protection of Payload pattern' after analysis of Payload of Web, DNS, HTTP, etc.	
20	System should support a DDoS protection function for VoIP(SIP) protocol	
21	System should support to protection as a group for several IP addresses	

Sr. No	Specification	Complied (Yes/No)
22	The system should support IPv4 and IPv6 dual-stack without deteriorating performance	
23	In IPv4 and IPv6 dual-stack environment, the application and change operation of individual function should not affect each other	
24	The proposed Equipment shall be able to support VLAN traffic reinjection.	
25	The proposed Equipment shall be able to support MPLS Label traffic reinjection.	
26	The proposed DDoS device shall be able to support high-availability with:	
27	Device (Anti-DDOS) failure detection	
28	Traffic Reinjection Dead Link, gateway and interface detection.	
29	The proposed Equipment shall have built-in high availability (HA) features in the following mode: Active-Passive Active-Active	
30	The proposed Equipment Ethernet interfaces shall support link aggregation (IEEE 802.3ad) standard.	
31	The proposed Equipment shall be able to immediately support both IPv4 and IPv6, and implements dual stack architecture.	
32	The proposed Equipment shall be able to sync with NTP server.	
33	The proposed Equipment shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static , OSPF & BGPv4	
34	The proposed system should be able to be extended it performance using additional modules.	
35	The proposed system should be able to extend the Anti-DDOS performance and capacity automatically without additionally manual traffic distribution when new modules are added. The proposed system should be able to load share the traffic when new modules are added.	
36	The propose Equipment shall support policy based routing (PBR) features.	
37	Time to apply the Anti-DDOS policy should be within 5 minute without any service interruption.	
38	The proposed Equipment must able to support real-time configuration changes without impact to service.	
39	The proposed Equipment must be able to integrate with existing management system via SNMP version 3 and SNMP version 2	
40	The Vendor must provide the latest Management Information Base (MIB) file for SNMP operation.	
41	The proposed Equipment log shall contain the following information: Attack logging User Login logging Operation Activity logging Link Status logging Diversion logging System Performance logging HA logging Traffic Alerts logging DDoS Attack logging Syslog	
42	The Security System provided shall be able to do remote inventory management capability and software download.	
43	The NMS shall provide the flexibility of performing configuration via GUI and command base remotely.	

Sr. No	Specification	Complied (Yes/No)
44	The Vendor must state clearly on the features which are currently supported, to be supported under the road map, and feature that does not support by the equipment.	
45	Security Equipment proposed by Vendor must be fully compatible with the existing Data Center network which mainly Cisco Router/Switches/ Third Party Equipment.	
46	The proposed Equipment shall be able to export syslog to existing syslog server and SIEM system.	
47	The Vendor shall state the maximum number of devices supported	
48	The proposed System shall support secure devices management:	
49	Able to access managed devices through GUI	
50	Able to deploy system OS / firmware patching to managed devices	
51	Able to deploy scripts to automate devices system administration	
52	The proposed System shall support encrypted communication between management system and device.	
53	The Vendor shall state the encryption level & algorithm used.	
54	The proposed System shall be able to execute real-time configuration changes without device service interruption	
55	The proposed System shall be able to push global configuration to all or selected devices.	
56	The proposed System shall support secure web-based access	
57	The proposed System shall be able to limit administrator network access	
58	The proposed system shall support devices security configuration management	
59	Able to deploy single configuration element to all or selected devices	
60	Able to store back-up configuration for selected devices	
61	The proposed System shall support active monitoring: Able to display devices status Able to display system alerts Able to display various traffic data Able to display security component status & alerts	
62	The proposed Equipment shall be able to support authentication schemes but not limited to: Local Password & RADIUS	
63	The proposed system should support the HTTP GET FLOOD detection and mitigation. The mitigation devices should support at least 6 algorithms for http attack protection.	
64	The proposed system should support the extension based on growth of the network and at least support expansion of mitigation devices up to 25 devices.	
65	The proposed system should support the behaviour based and algorithm based DDOS mitigation.	
66	The proposed system must provide multi-level Anti-DDOS mitigation infrastructure. The system must support integration of upstream and downstream Anti-DDoS device to mitigate DDoS Attack effectively.	
67	The proposed system must provide multi-level DDOS + Web application mitigation infrastructure. The upstream Anti-DDoS and downstream WAF can integrate and mitigate layer 1 to layer 7 attack effectively.	
68	The proposed mitigation device should provide auto packet capture function during DDoS mitigation.	
69	The proposed system should provide the traffic AUTO learning function for the DDOS traffic monitoring. The auto learning threshold baseline should captured hourly	
70	The traffic Auto learning threshold can be apply automatically after auto learning completed.	
71	The proposed system should provide the multi-level DDOS mitigation policy and	

Sr. No	Specification	Complied (Yes/No)
	different mitigation action based on DDOS traffic type.	
72	The proposed system should provide the function to monitor the outbound DDOS attack and cooperate with the mitigation platform to block the outbound DDOS attack.	
73	The proposed system must be able to support netflow v5, netflow v9, sflow v4, sflow v5, netstream v5, ipfix.	
74	The proposed system must support double diversion feature that can advertise two BGP diversion prefix under single attack to different devices for mitigation.	
75	The proposed system must support multiple BGP community tagging for different diversion configuration.	
76	The proposed system must support BGP traffic diversion based on attack size in terms of pps/bps.	
77	The proposed system must support auto null route based on attack size in terms of pps/bps.	
78	**Anti-DDOS reporting system**	
79	The proposed System shall support the provisioning of the following reports in detail or in summary:	
80	Attack reports -top sources, targets, attack type etc.	
81	System reports -security events triggered	
82	User reports -user access activity	
83	The proposed system must be able to generate summary attack report of daily/weekly/monthly.	
84	The proposed system must be able to send schedule summary attack report of daily/weekly/monthly.	
85	The Vendor shall provide full details regarding the proposed staff required to fulfill the site design and installation service, including an organization chart, job descriptions and staff competency levels.	
86	The proposed System shall support report format customization	
87	The proposed System shall support remote report view in web HTML	
88	The proposed System shall be able to export reports as documents or images.	
89	The Tendered shall state the export format supported.	
90	The proposed System shall support secure web-based access	
91	The proposed system must be able to limit administrator access by IP address.	

7.5.5. Server Security Solution:

No	Functional Description	Complied (Yes/No)
1	**General**	
1.1	The solution must provide single platform for complete server protection over physical, virtual (server/desktop)& cloud:	
1.1.0	• Complete protection from a single integrated platform: addresses all of the 'Gartner top ten server security priorities'.	
1.1.1	• Provides layered defense against advanced attacks and shields against known vulnerabilities in web and enterprise applications and operating systems.	
1.1.2	• Web reputation prevents access to malicious web sites	
1.1.3	• Protects a wide range of platforms: Windows, Linux, Solaris, HP-UX, AIX, VMware, Citrix, Hyper-Vand Amazon.	
1.2	The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defense at the server: firewall, Anti-Malware ,HIPS , application control etc.	
2	**Management Console**	
2.1	Proposed solution must have a dashboard to display multiple information.	
2.2	The dashboard must be configurable by administrator to display the information which is required only	
2.3	Proposed solution must have a web-based management system for administrators to access using web browsers	
2.4	Providing "Alerts" on the main menu to view administrator notifications concerning system or security events.	
2.5	Providing Firewall Events to view activities on computers with the firewall enabled (typically includes dropped or logged packets).	
2.6	Providing access to DPI Events to view security-related DPI activities. The section should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode).	
3	Providing System Events to view a summary of security-related events, primarily for the Management server and also including Agents' system events. All administrative actions should be audited within the System Events.	
4	**Solution Functions/Modules**	
4.1.	The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites for virtual desktops	
4.2.0	Must be able to provide HIPS/HIDS feature with agent in Physical servers.	
4.2.1	Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.	
4.2.2	Must be ABLE to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.	
4.2.3	Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred	
4.2.4	Must be able to provide protection/shield against known vulnerabilities without installing the OS patch.	
4.2.5	Protection can be pushed out to thousands of virtual/physical servers in minutes without a system reboot	
4.2.6	Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services	
4.2.7	Must include exploit rules to stop known attacks and malware and are similar to	

No	Functional Description	Complied (Yes/No)
	traditional antivirus signatures in that they use signatures to identify and block individual, known exploits	
4.2.8	Must assists compliance (PCI DSS 6.6) to protect web applications and the data they process.	
4.2.9	Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.	
4.3.0	Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.	
4.3.1	Virtual machine isolation.	
4.3.2	Fine-grained filtering (IP and MAC addresses, ports).	
4.3.3	Coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)	
4.3.4	basic prevention of denial of service (DoS) attack	
4.3.5	Design policies per network interface	
4.3.6	Detection of reconnaissance scans	
4.4.0	Must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real-time.	
4.4.1	Provides hypervisor as well as physical server integrity checking, extend security and compliance of virtualized systems to hypervisor. And must support Intel TPM/TXT technology.	
	Provides Agent-less as well as agent based recommendation or baseline scan.	
4.5.0	Provide virtual protection which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.	
4.6.0	The proposed solution must support event tagging so that Administrator can add "tag" to events generated by the solution	
4.6.1	The Tag must be fully customizable; Administrator can add, edit and delete their own Tag with own name	
5	**Support Platform**	
	Support Platform includes:	
	Microsoft Windows	
5.1.0	• Windows 8	
5.1.1	• Windows 7 (32 and 64 bit)	
5.1.2	• Windows 2008 (32 and 64 bit)	
5.1.3	• Windows Vista (32 and 64 bit)	
5.1.4	• Windows 2012	
5.1.5	• Windows XP (32 and 64 bit)	
5.1.6	• XP Embedded	
5.1.7	• Windows 2003 SP2 (32 and 64 bit)	
	Virtual	
5.2.0	• Vmware vSphere 4.1/5.0/5.1	
5.2.1	• Vmware ESXi 5.0/5.1	
5.2.2	• Vmware View 4.5/5.0	
5.2.3	• Citrix XenServer	
5.2.4	• Microsoft HyperV	
	Solaris	
5.3.0	• Solaris OS 8	
5.3.1	• Solaris OS 9	
5.3.2	• Solaris OS 10	

No	Functional Description	Complied (Yes/No)
	Linux.	
5.4.0	• RedHat Enterprise Linux 6.0	
5.4.1	• RedHat Enterprise Linux 5.0 (32-bit/64-bit)	
5.4.2	• SUSE Enterprise Linux 11 (32-bit/64-bit)	
5.4.3	• SUSE Enterprise Linux 10 (32-bit/64-bit)	
	Unix	
5.5.0	• AIX 5.3,6.1 on IBM Power Systems	
5.5.1	• HP-UX 11i v3 (11.31)	
6	**Compliance & Certification**	
	Provides out of the box compliance support for the following	
6.1	• PCI DSS 2.0.	
6.2	• NIST	
6.3	• HIPAA	
6.4	• SOX	
6.5	• Basel 2	
6.6	• ISO 2700x	
6.7	• SAS70	
6.8	• DPA.	
6.9	The solution must be certified to Common Criteria EAL 4+.	
7	**Deployment and Integration**	
7.1	The solution must be integrated to SIEM system including RSA Envision	
7.2	Directory integration so that it integrates with enterprise directories, including Microsoft Active Directory	
7.3	Software distribution, with agent software that can be deployed easily through standard software distribution mechanisms.	
	Management:	
	Features	
1	Solution should have single console to Manage desktop AV , Mail and Web Gateway software solution	
2	Should be a Software Solution Integrated, centrally-managed security framework—for a unified defense	
3	Simplifies administration with automated update deployment and license renewal	
4	Provides single sign-on, eliminating the need to logon to each product	
5	Consolidates data for a master view of Central Manager servers throughout the network	
6	Simplifies administration with a web based console and integrated agent	
7	should have capability for consolidating updates and global alerts	
8	Should have Intelligence with customizable, flexible reports for easy interpretation	
9	Expands visibility into individual clients, reducing desk-side visits	
10	Software should Ensures only authorized personnel make critical changes to the security environment	
11	Assigns specific privileges based on predefined administrative roles	
12	Allows user-defined customizable administrative roles	
13	Supports visibility into clients so central IT can remotely monitor and manage client security	
14	Should have capability to implement Parent-->Child Architecture	
15	Solution should support Role based administration	

No	Functional Description	Complied (Yes/No)
16	Ability to centrally manage Data Loss Prevention features with ability to deploy DLP settings to managed products, collect logs for reports, dashboard widgets etc.	
17	Solution should have the capability to generate Alert in case of following events - Virus outbreak alert - Special virus alert (10) - Virus found - first and second actions unsuccessful - Virus found - first action successful - Virus found - second action successful - Network virus alert - Suspicious vulnerability attack detected	
18	Solution should have the capability to manage following - Outbreak Prevention Mode started - Outbreak Prevention Mode stopped - Outbreak Prevention Policy update unsuccessful - Outbreak Prevention Policy update successful	
19	Solution Should support following Operating Systems indows Server 2008 MS Windows Servers 2012 all versions RHEL SUSE Linux AIX HPUX	
20	Solution should support following Database MSSQL MySQL PostgreSQL Oracle	
21	Solution should support following Reporting capability	
	Shall be able to produce the following reports on a one-time and scheduled basis:	
	Reports shall be available on-line via web interface	
	Shall be able to automatically deliver reports via email to designated users when the report has been generated	
	Reports shall support the following formats: PDF, RTF, ActiveX, Crystal Reports	
	Report templates shall include:	
	Spyware/Gray ware Detection Reports • Spyware/Gray ware Detected • Most Commonly Detected Spyware/Gray ware (10,25, 50, 100)	
	Virus Detection Reports • Viruses Detected • Most Commonly Detected Viruses (10, 25, 50, 100)	
	Antivirus Client Information Reports • Detailed/Basic Summary	
	Antivirus Product Registration Report (Registration Status)	
	Comparative Reports • Spyware/Gray ware, Grouped by (Day, Week, Month) • Viruses, Grouped by (Day, Week, Month)	
	Antivirus Server Deployment Reports • Detailed Summary • Basic Summary • Detailed Failure Rate Summary	

No	Functional Description	Complied (Yes/No)
	Virus Cleanup Services Reports	
	Top 10 Virus Detection Points Report • Includes the top 10 managed products and number of detected viruses.	
	All Entities Virus Infection List • Includes all managed products and number of detected viruses.	
	Top 10 Infected Email Sender Report • Includes the top 10 senders of infected messages and number of infected messages.	
	Top 10 Infected Files Report • Includes the top 10 infected files.	
	Daily Virus Count • Includes the number of viruses detected and counted per day.	
	Top 10 Virus Report • Includes the top 10 viruses detected during the date range specified.	
	Top 10 Security Violation Report • Includes the top 10 content security policies violated and number of infections. Deployment Rate • Includes the deployment status, managed product deployed to, last reported time, and percentage completed.	
	Virus Infection Channel vs. Product • Includes the source of the virus infection and number of infections.	
	Web Security Violations Report • Includes blocking type and rule, as well as the number of web security rule violations.	
	Desktop Antivirus Protection Summary • Includes virus detection of desktop antivirus managed products (for example, Office Scan).	
	Filter Events by Frequency Report • Includes Interscan Messaging Security Suite virus and spam detection.	
	Filter Events by Policy Report • Includes messages filtered according to InterScan Messaging Security Suite policies.	
	Spam Summary for Recipients Report • Includes the top 10 spam recipients and spam information.	
	Spam Summary for Domains • Report Includes the top 10 domains affected by spam.	
	Outdated Antivirus Client • Includes antivirus clients that do not have the current components (virus pattern, scan engine, product program) as the AV server.	
	Consolidated Report A Global Consolidated Report profile generates information provided by all templates, except those provided by the Deployment Rate template.	

7.5.6. Zero Day Protection for Server:

No.	Functional Description for Zeroday protection for Servers	Complied (Yes/No)
1	**General Specs**	
1.1	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.	
1.2	The proposed solution should support the native CEF,LEEF format for SIEM log integration	
1.3	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	
1.4	The proposed solution should support Structured Threat Information eXpression language.	
1.5	Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection	
1.6	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.	
1.7	Proposed Solution can integrate with the existing URLF solution, Server Protection & Endpoint solution for Zero day protection	
1.8	Solution should be deployed on premise along with on premise sandboxing capability	
1.9	The proposed solution should be able to store payload of the detected threats	
1.1	Solution should have ability to interrupt malicious communication	
1.11	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth	
1.12	The Anti-APT solution should have the option to notify the Admin by SMTP over SSL/TLS	
1.13	The solution should check the update from the OEM cloud in every 15 min or best as per proposed OEM	
1.14	Solution deployment should cause limited interruption to the current network environment.	
1.15	The proposed solution should able to work with the existing technologies for advance threat protection through web protocol	
1.16	The solution should support YARA rules	
1.17	The solution should have the Document exploit detection feature	
1.18	The solution should support clustering.	
1.19	The solution should support manual submission of suspected files to the sandbox for further analysis	
1.2	Should support out-of-the-box integration with end point security, Server security products of the same vendor,	
1.21	Open Web Services API allows any product or authorized individual to submit samples and obtain detailed analysis.	
1.22	Should performs page scanning and sandbox analysis of URLs that are manually submitted.	
1.23	Should support at least 30 sandboxes for customization of customer environment or better	
1.24	The solution can detect ransomware, advanced malware, zero- day exploits, command and control (C&C) and multi-stage downloads resulting from malicious payloads or URLs on Windows and Mac OS systems	
2	Decrypt password-protected PDF and Microsoft Office files using a password list	
2.1	**Malware Analysis**	
2.2	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for	

No.	Functional Description for Zeroday protection for Servers	Complied (Yes/No)
	advanced threat detection.	
2.3	The proposed solution should be able to provide minimum 30 customizable sandboxes to fulfill Customer's environments and needs.	
2.4	Sandbox must supports multiple operating systems and for both 32-bits and 64-bits OS or better	
2.5	Solution must have the capability to analyze large files. Must be able to support more than 20MB- 40MB file size or better.	
2.6	The proposed solution should scan minimum 18500 or more samples per day	
2.7	The Proposed solution should support windows XP, Windows 7, Windows 10, Microsoft Windows Server 2012 etc. operating environments for Sandboxing	
2.8	The proposed solution should have gray ware detection capabilities.	
2.9	The proposed solution should have storage inbuilt with RAID feature with redundant power supply	
2.1	The proposed solution should support IPv4 & IPv6 both	
2.11	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp	
2.14	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.	
2.15	The proposed solution must provide the capability to exportable network packet files and encrypted suspicious files for further investigation.	
2.16	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files	
2.18	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing	
2.19	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms	
2.2	The proposed solution must have capabilities to detect Mac and mobile malwares	
2.21	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list	
2.22	The proposed solution must have capabilities to detect Mac, Linux and mobile malwares (optional)	
2.23	The proposed solution should have capability to include User-defined and context-derived passwords for protected archives	
2.24	The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.	
2.25	The Proposed solution should be able to detect known malwares before sending suspicious files to Sandbox for analysis	
2.26	The Proposed solution should be able to correlate local APT attacks with Global historical APT attacks.	
	The Proposed solution should be able to share IOC/threat intelligence to other security solutions.	
3	**Report**	
3.1	The proposed solution should support customizable reporting	
3.2	The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats	
3.4	The proposed solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)	
3.5	The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.	

No.	Functional Description for Zeroday protection for Servers	Complied (Yes/No)
3.6	The proposed solution should have the flexibility to provide customizable dashboard.	
3.7	The proposed solution should have the option to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geo-map, chart, tree-map/pivot table.	
3.8	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.	
3.9	The proposed solution should be able to integrate with the existing endpoint, web and email management solutions at Customer for further detailed reporting.	
4	The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.	
4.1	Authentication Administration and Configuration Requirement	
4.2	The proposed solution shall support Local Password authentication schemes	
4.3	The proposed solution shall support Remote administration using SSH/HTTPS	
4.4	The proposed solution shall support CLI, GUI/Web based Administration Console.	

7.5.7. Antivirus Solution for servers

Sr.No.	Required Minimum Specifications	Complied (Yes/No)
1	Must offer comprehensive client/server security by protecting enterprise networks from which includes virus protection, spyware, rootkits, bots, grayware, adware, malware and other computer Bourne threats or mixed threat attacks or any emergingcyber-attacks or zero day attack protection. The solution should be in the of Gartner's leader's quadrant for Endpoint for last 2 years.	
2	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process.	
3	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
4	Must include capabilities for detecting and removing rootkits	
5	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution	
6	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe	
7	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation	
8	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process	
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to : 9.1 Terminating all known virus processes and threads in memory 9.2 Repairing the registry 9.3 Deleting any drop files created by viruses 9.4 Removing any Microsoft Windows services created by viruses 9.5 Restoring all files damaged by viruses 9.6 Includes Cleanup for Spyware, Adware etc.	
10	Must be capable of cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether	
11	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak	
12	**Behavior Monitoring :**	
	12.1 Must have behavior monitoring to restrict system behavior, keeping security related processesalways up and running	
	12.2 Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent	
13	Must provide Real-time lock down of client configuration allow or prevent users from changing settings or unloading/uninstalling the software	
14	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
15	CPU/memory(physical or virtual) usage performance control during scanning : 15.1 Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer 15.2 Adjusts the scanning speed if: 15.2.1 The CPU usage level is Medium or Low 15.2.2 Actual CPU consumption exceeds a certain threshold	
16	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	
17	Should have Integrated spyware protection and cleanup	

Sr.No.	Required Minimum Specifications	Complied (Yes/No)
18	Should have the capability to assign a client the privilege to act as a update/master relay agent for rest of the agents in the network	
19	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
20	shall be able to scan only those file types which are potential virus carriers (based on true file type)	
21	Should be able to detect files packed using real-time compression algorithms as executable files.	
22	shall be able to scan Object Linking and Embedding (OLE) File	
23	Must provide Web threat protection by the following ways: 23.1 Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings 23.2 Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location 23.3 Must have the capabilities to define Approved URLs to bypass Web Reputation policies 23.4 Must provide real-time protection by referencing online database with millions of rated Web domains 23.5 Configure Web reputation policies and assign them to individual, several, or all end users machine.	
24	Must provide File reputation service 24.1 Must be able to check the reputation of the files hosted in the internet 24.2 Must be able check the reputation of the files in webmail attachments 24.3 Must be able to check the reputation of files residing in the computer	
25	Must protect clients and servers on the network, high performance network virus scanning, and elimination.	
26	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users	
27	Must have smart feedback to enable feedback from the client agents to the threat research centers of the vendor.	
28	Uses any alternate method other than the conventional pattern based scanning with the following features: 28.1 Provides fast, real-time security status lookup capabilities in the cloud 28.2 Reduces the overall time it takes to deliver protection against emerging threats 28.3 Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints 28.4 Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.	
31	Should be able to deploy the Client software using the following mechanisms: 31.1 Client installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged clients, specific installer for servers 31.2 Web install page 31.4 Remote installation 31.5 From a client disk image	
32	Must provide a secure Web-based management console to give administrators transparent access to all clients on the network	
33	The management server should be able to download updates from different source if required.	
35	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.	
36	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console	
37	Should have role based administration with active directory integration 37.1 To create custom role type	

Sr.No.	Required Minimum Specifications	Complied (Yes/No)
	37.2 To add users to a predefined role or to a custom role	
38	Should have integration with the Active directory 2008/2012 or higher	
39	Shall support grouping of clients into domains for easier administration	
40	Establish separate configuration for internally versus externally located machines or equivalent	
42	Must be capable of uninstalling and replacing existing client antivirus software and to ensure unavailability of any residual part of the software.	
43	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network.	
44	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network	
45	The solution should support client installation on all the following: 45.1 Windows XP/Server 2003 32-bit Edition & 64-bit Edition 45.5 Windows 7, Window 8, Windows 10 (32-bit version & 64-bit version) and higher version if any 45.6 Microsoft Cluster Server having all applicable versions 45.7 Microsoft Windows Server 2008/2012 with all its versions 45.8 Client/solution installation on operating systems hosted on virtualization environment. 45.9 Should support Intel x64 , AMD x64 , any other variants of processor 45.10 Should support all handheld mobile devices at no extra cost 45.11 Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, SNMP trap	
46	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from client IPS, client firewall, and/or network virus logs exceed certain thresholds, Signaling a possible attack.	
47	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	
48	Should perform Boot & Rootkit scan and cleaning	
49	Virus definition files should be lighter so that same can be transmitted to remote locations having minimum of 64kbps link or the update pattern size should be less than 200Kb	
50	AV should be seamlessly implemented on all the variants of Windows endpoints including Windows XP.	
51	System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.	
52	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine	
53	The solution should have latest machine learning technology in built from day one.	
54	The End point AV should have the option of integration with on premises sandbox/anti-apt appliance.	
55	The solution should have the option of the endpoint vulnerability shielding in the network.	
56	The solution should have ransomware protection in built.	
57	The solution should have the option of Endpoint DLP plug in from the day one & DLP should not come with in form of separate client. Endpoint DLP should be integrated with the same antivirus client.	
58	The solution should have Machine Learning /Artificial Intelligence or equivalent feature which can identify the malware file before execution.	
59	The endpoint solution can integrate with the Anti-APT solution present in network.	

7.6. Enterprise Management Software:

Existing setup of West Bengal Data Center uses Enterprise Management System of CA. Bidders to propose the client licenses so that it there is no integration issues with the existing licenses.

Bidder needs to submit the following compliance sheets for seam EMS Solution:

Sr	Item	Specification	Complied (Yes/No)
1.	**Network and Device Discovery &monitoring Capabilities**	The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.	
		The system should support maps grouped by network topology, geographic locations of the equipment's and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.	
		Help Root Cause analysis and Pinpoint specific causes of outages and performance issues.	
		Controlling, tracking and remediating changes across thousands of network devices.	
		Provide a single platform for monitoring physical, virtualized and cloud environments	
		IT delivers pre-packaged and easily customizable reports, alerts and dashboards.	
		Correlate among multiple events and suppresses symptomatic alarms in order to deliver targeted insights.	
		Monitor parameters like Device Availability, Link Availability, Bandwidth Utilization, Rx, Tx etc. directly as well as through user-created VLANs.	
		Monitor QoS parameters like Jitter, Latency and Packet Loss	
		Monitor availability tracking of Primary & Secondary ISP and critical links like MPLS, P2P, LL etc. via flexible dashboards and reports.	
2	**Device Health Monitoring**	Solution should be a single platform solution for proactive fault isolation, root cause analysis, change management, service aware management, IP services management, policy management, and reporting for network devices across multiple network technologies.	
		Provides highly scalable management platform that can provision for up to many thousands of network device management from a single optimized hardware..	
		The proposed solution must support Network segmentation by supporting IPSEC / GRE Tunnels as well MPLS Layer 3 VPNs (e.g. VRF) & VLANS.	
		Solution must be able to discover, model and create topology map of vPC enabled devices and its vPC channels along with their individual physical port connections	
		Solution must provide intelligent alarms, RCA and Impact Analysis feature for monitoring vPC domains.	
		Proposed fault management must be able to clearly identify	

Sr	Item	Specification	Complied (Yes/No)
		configuration changes as root cause of network problems	
		Proposed solution must have an in-built capability to carry out configuration management without the use of any external software to reduce integration efforts and increase ease of deployment	
		SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.	
		Proposed solution must provide holistic view of availability of host servers on network and their performance data for fault management in a single pane of application	
		Should be able to provide insight on the relationship between physical resources and virtual entities for virtual network environments.	
		Should be able to provide Dashboard view to show the types of inventories in your virtual network, and their growth over time	
		Solution should provide capability to monitor any device based on SNMP v1, v2c & 3	
		Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature, interface bandwidth utilization.	
		Solution should have the ability to receive SNMP traps and syslog	
		Solution should automatically collect and store historical data so users can view and understand network performance trends.	
		Solution should be capable of monitoring packet loss, Packet QOS, Packet Errors on one or more ports	
		SMS and email notification to users against critical alarms, hardware change notification (configurable) etc.	
		Virtualization Monitoring	
		Manage hosts & guests and workloads with automatic discovery of pools, hosts, host CPUs, etc.	
		Monitor key parameters of Host like CPU Cores, Memory, VMs running, etc and VM key parameters like CPU, Memory and Disk Usage, etc. Tracing of VMs across host servers.	
		Supports stand platform VMware ESX/ESXi, Microsoft HyperV, Citrix and Suse/Redhat Linux and other openstack/opensource platforms	
		Application Monitoring Monitor individual applications with respective application specific important parameters.	
		Supports Email applications like Exchange, Notes, Dominos, etc; Web Servers like Apache, Tomcat, IIS, etc; Application Servers like JBOSS, J2EE, Oracle WebLogic, IBM WebSphere etc	
		Support for new devices for traps and automatically generate alarms	
		Server Monitoring should be with and without Agent (Agent-less)loaded on the servers . The Solution should monitor through agent Based (Non-SNMP), agentless (Non- SNMP), agent based (with- SNMP) heterogeneous operating systems for both physical and virtual environments OS including but not limited to Windows 32/64 bit, All Major Flavors of Linux, Solaris, HP-UX etc. Agentless or remote monitoring for critical servers only.	

Sr	Item	Specification	Complied (Yes/No)
		Performance monitoring of servers from all major vendors running on any OS like Windows, Linux, Solaris, AIX etc.	
		Granular level analysis and tracking of individual processes & services running on each servers to track performance issues.	
		Server specific overviews for key parameters like CPU, Memory, Disk & HD Utilization, Server Health, etc.	
3.	**Application Performance Monitoring**	Application Uptime, response time measurement, problem area identification, root cause analysis, code analysis, pin points problems and extract customizable report	
		Dashboard for Users:	
		• The proposed solution should measure the end users' experiences based on transactions without the need to install agents on user desktops in a customizable dashboard. • Solution shall work based on the passive listening of the network traffic to and from the Web servers, and analyzes the transactions without affecting the performance or availability of the IT infrastructure in any way. • The proposed system must be able to detect user impacting defects and anomalies and reports them in real-time: ▪ Slow Response Time ▪ Fast Response time ▪ Low Throughput ▪ Partial Response ▪ Missing component within transaction • The proposed solution should be capable of identifying the problem domain (browser, network or application) thereby it should monitor the browser side metrics and provide reports in real time for: • The proposed system must allow for SLA monitoring • Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc. • The proposed solution should provide Browser Response Time Metrics such as Page Load, AJAX, and JavaScript Function. • As a means of detecting poorly performing SQL, the solution must be able to proactively record all SQL calls, and report on the slow performing ones. The SQL measurements must be made from within the monitored application – not using an external database agent. • The proposed solution must have integrated ability to store historical performance data without requiring external database to be configured for any length of time. • The proposed solution must provide ability to monitor performance of Java/.Net/Php methods based on simple parameters (Strings, Numbers) passed to the methods 24x7 in production environments with negligible impact on monitored application • Customized alerts should be sent to users by SMS and Email.	

Sr	Item	Specification	Complied (Yes/No)
4.	**Database Performance Monitoring**	The solution should monitor multiple database servers and multiple versions of each server including: • Oracle • SQL Server • MySQL • PostgreSQL • DB2 • Informix • Sybase	
		Solution should Provide SQL Response Time for Monitoring Custom Queries	
		Solution should provide response time Monitoring for custom queries through JDBC Mechanism to allow monitoring unsupported databases	
		Database Space Monitoring for both file group and transaction log (Warning threshold, Critical threshold as well as file group/log full)	
		Performance monitoring - capture of DB Engine related performance counters as well as threshold alerting	
		The solution must support SQL Agent monitoring - failed jobs, long running job	
		The solution must support Database Health and Settings - Check database status (offline, suspect), Check database options (auto grow, auto shrink, auto close etc.)	
		The solution must support monitoring of Replication, DB Mirroring and Log shipping if applicable	
		The solution must be able to report & check for last recent Full database backup and last recent Transaction Log backup	
		The solution must be able to run power shell, cmd and VB scripts to perform tests on the database and have the results put into the solution as performance data and or alarms Inclusion of SQL statements within the Solution should be a standard "easy-to-use" function achieved without programmatic intervention	
		The solution should support the creation and management of reusable test templates that contain a specific pre-defined set of database checkpoints/measurements.	
		The solution should support the use of schedules and time filters for database monitoring	
5.	**Service Desk Management**	Solution should provide a web based service support system to automate incident, problem, change, knowledge management, interactive support, self-service and advanced root cause analysis	
		Solution should support request management, problem management, configuration management and change order management.	
		Solution should provide an identity management system that allows user/role management and integration with authentication systems such as LDAP/AD	
		Solution should support multi-tenancy to enable different tenants	
		Solution should provide a distributed and scalable architecture that	

Sr	Item	Specification	Complied (Yes/No)
		caters to growth in number of analysts, end-users and call volumes.	
		Solution should provide Workflow tool or engine to help in modelling and automating ITSM workflows in order to meet complex process or workflow needs. The Workflow tool or engine shall allow building processes/workflows that allow decision-based branching, parallel processing, custom input and approval forms, and integration with home-grown and third-party systems via a variety of integration tools	
		Solution should offer Service Catalog as part of the license for full-fledged request management.	
		Integration of Service Desk with other modules in the EMS	
		An ITIL 2011 certified for at least 10 processes should offer features like worklfows, Knowledge Base, Ticket Notification, Help Desk Reports	
		The proposed solution shall provide a fully functional CMDB (Configuration Management Database) as an integral part of the service desk solution and license. CMDB should be accessible from the same interface	
6.	**Access Management of Server and Network Devices**	Admin Users access to the proposed solution should be via encrypted channel only. Solution should support concurrent 50 admin user access.	
		Solution should provide a system to authenticate user to access system through secure, managed and automated process.	
		The proposed solution should allow to secure, manage, automate and log all activities associated with the privileged accounts for audit trail purpose.	
		The proposed solution should allow specifying automatic password changing for a privileged account each time after it is used.	
		The proposed solution should be policy based and can be configured different policies for different platform privileged accounts.	
		The proposed solution should have alert system for the following: a. SMS b. email	
		The proposed solution should provide secure remote access to sensitive servers such as Windows servers, Unix/Linux, iSeries and network devices without having to expose credentials to end-users e.g. external vendors.	
		The proposed solution should enable extraction and archival of audit logs. The proposed solution should generate compliance audit trail reports for reviewing.	
		The proposed solution should have session timeout capabilities, when session idle and this parameter should be in configurable mode.	
		The proposed solution should control, monitor and record privileged sessions including RDP, SSH, Telnet, HTTP/HTTPS in single module.	
		For WBSDC Department Servers	
		The solution should control even root and Administrator access to files and directories. It should also control whether kernel modules can be loaded or unloaded, even by the root users.	
		The solution should prevent unauthorized termination of processes and services, even for root and Administrator.	

Sr	Item	Specification	Complied (Yes/No)
		The solution shall automatically identify and assign new endpoints to policies. The solution should also support multiple versions of policies to accommodate differences in managed endpoints	
		The solution should enable users to authenticate to windows and Linux using Active Directory domain credentials and ensure that only authorized users or groups can login to the UNIX or Linux endpoints using Active Directory credentials.	
7.	**Asset Management**	The proposed solution should have ability to track Asset status (Asset Lifecycle stages)	
		The proposed solution should have ability to define an Asset Family (i.e. unlimited asset types)	
		The proposed solution should have ability to Classify Assets	
		The proposed solution should have ability to Add and Update Assets and Asset specific information	
		The proposed solution should be able to Define/Assign different individuals to an Asset	
		The proposed solution should be able to associate a Contract documents, terms and conditions to an Asset	
		The proposed solution should have ability to create Asset Groups and Sub-Groups	
		The proposed solution should support AMC/Warranty management Notifications for renewals etc.	
8.	**Business Services Monitoring**	Monitor critical business services & IT services by breaking them into granular components and defining logical groups for the same.	
		Manage Internet, Intranet, Proxy and Email service to ensure improved MTTR and minimize application failures through quick root cause analysis and intelligent event processing	
9.	**Service Level Agreement**	Intelligent SLA monitoring through proactive violation alerting and comprehensive reporting. .	
		Resource level SLA specification and support for multiple SLA templates. Option to choose from the default templates to maintain service policies.	
		Separate specification for Outage, Business Hours and Holidays. Enable SLA Timers to prevent unnecessary escalations	
10.	**Configuration Management**	Manage configurations for routers, switches and other network devices of any vendor.	
		Approval based configuration Management and alerts if configurations are changed without approval	
11.	**Topology Mapping**	Automatic Detection of Network Topology via L2, L3 protocols and projection of the data in Diagrammatic View with easy color-coded status.	
		Representation of the mapped data can be displayed through Flat Network View as well as Geo Maps. Simulate Datacenter architecture on a Live Dashboard using the Network diagram drag-and-drop tool.	
12	**General requirement**	i. Bidders must quote "Commercial of the Shelf" product, with back to back OEM support. ii. Bidder may quote the existing CA solution oralternatively, bidder may quote a completely separate solution, with all licenses as required as per table- **"New Requirement"**. In	

Sr	Item	Specification	Complied (Yes/No)
		case a new solution is proposed, the system must do zero-day integration with the existing EMS system of CA. iii. In case Bidder is proposing existing EMS (OEM-CA), bidder need to quote upgradation of existing licenses (given in below table for **"existing EMS tool Count"**) and cost for additional licenses on top of the existing Licenses as per table for **"New Requirement".** iv. The proposed EMS solution should provide a single console that should be able to recognize devices. v. Proposed system should provide integration with the proposed BMS/ Non IT systems and should provide a single integrated console along with IT systems or separate consoles for the IT and non IT.	

Table: Existing EMS Tool Count

Sr. No.	CA Tools	License based on	Total License procured
1	CA System Edge Agent 4.3(Edge Agent)	Node based	23
2	CA Spectrum 9.4(Spectrum)	Node based	100
3	CA Health 6.3(Health)	Node based	120
4	CA Service Desk 12.9(Service Desk)	Analyst Access Concurrent login	5
5	CA Wily APM 9.5(Willy)	Core Based License- Factor 0.5	60
6	CA Control Minder R12.8 Agent (AC)	Node Based	23
7	CA DPM R11.5(DPM/UIM)	Core Based License- Factor 0.5	4
8	CA Patch Management r12.5(Pat)	Node Based	100
9	CA ITCM r12.5(ITCM)	Node Based	100

Table: New Requirement:

Sr. No.	New License Requirement	New License Count
1	Server, Device& infrastructure health checkup, Device discovery, Monitoring &Management (with or without agent)	150 Devices
2	Application performance Monitoring (includes Java, .Net and PHP packs)	80 Applications
3	Access Management of Server and Network Devices	200 Devices
4	Database Performance Monitoring	80 databases
5	Service Desk Management	10Users
6	Patch Management for windows & Linux	150 Devices
7	Asset Management for IT & Non-IT	150 Devices

8. Technical Specification Compliance details – Non IT Components

1.1.Cold Aisle Containment

Sr.No.	Description	Complied(Yes/No)
1.	Supply, Assembly and installation of Cold Aisle Containment	
2.	The Containment uses a series of panels, door frames and doors, and air blocks to enclose a cold aisle zone which contains cooling unit supply air	
3.	Cold Aisle Containment: The cold aisle zone is the space between two rows of IT equipment racks with cold air being supplied between the two rows of racks (or one row of racks and an architectural wall) and the IT equipment exhausts hot air away from the aisle. In this enclosed space cooling unit supply air is collected inside of the Containment. The cool air is supplied to the IT equipment while the IT equipment exhaust air is pushed outside the Containment and returned to the cooling unit. By preventing mixing of cool supply air and hot exhaust air, this self-contained configuration is capable of supporting a complete range of low, medium and high power/heat density loads, and can be deployed in multiple environments without affecting the surrounding area.	
4.	All system components shall be certified as suitable for this data center environment by documentation supporting UL Listings: UL484, and UL723S.	
5.	Ceiling panels shall be minimum 6.0 mm or thicker Lexan clear-ribbed panels or 2.36 mm thick V0 clear panels with aluminum framing.	
6.	Ceiling panels shall be designed to be supported by the frames of the IT Equipment racks. Ceiling Panel frames sizes shall be suitable to match up with various rack widths, row width, and aisle widths.	
7.	The ceiling system shall be designed to permit removal of the ceiling panel from within the contained zone without the use of tools for service access to the space above the Aisle.	
8.	Metal door frames and doors shall be provided to establish air containment at the end of two rows of racks. The door frame system shall match the height of the rack based equipment, and match the design width of the contained aisle.	
9.	Doors shall be Sliding, to permit access into the contained aisle for maintenance or servicing.	
10.	Doors shall be provided with a window, handles and latches.	
11.	Door locks and three matching keys per door	
12.	Automatic door closure system for sliding door	
13.	Sliding Doors shall be provided with swing-open functionality in case of emergency inside the aisle.	
14.	Foam Rubber gaskets or metal/composite, brush, or plastic air blocks shall be installed at Aisle joints to minimize open gaps between containment system components, such as door frames, ceiling and duct panels, and IT Equipment racks and rack based equipment. Gasketing and/or air blocks may include, but not be limited to, the following. 1. Joints between adjacent ceiling/duct panels 2. Joints between ceiling/duct panels and top of racks, if not metal to metal. 3. Joints between door frames and ceiling/duct panels, if not metal to metal. 4. Joints between door frames and racks at the end of the row(s). 5. Joints between rack bottom rear frame and floor. 6. Joints between duct panel and ceiling/roof of room.	

Sr.No.	Description	Complied(Yes/No)
15.	Can be used to provide an aesthetic alternative for varying dimension enclosures.	
16.	Blanking Panels shall be placed where gaps between racks exist to seal contained aisle. The panel shall match the height of the enclosures and match the width of the gap. It shall not be mounted to any adjacent blanking panels nor shall it support any adjustable height supports.	
17.	Depth Extenders shall mount to front or back of enclosures to align aisle. The extender shall match the depth of the adjacent racks and match the width and height of the enclosure (including any height adapters) of which it is being mounted	
18.	Height Adapters shall mount to the top of enclosures to align the enclosure height. The height adapter match the height of the adjacent racks and shall match the width and depth of the rack (including any depth adapters) of which it is being mounted.	

1.2. Electrical:

1.2.1. Wiring/ Cable Works:

Sr No.	Specifications	Complied (Yes/No)
1	Cable trays should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the trays. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a crisis crossing is avoided and final take off to switch gear is easily facilitated.	
2	All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminum strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.	
3	Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.	
4	Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.	
5	Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.	
6	Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.	
7	The space between data and power cabling should be as per standards and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.	
8	PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 1100 volts grade. Color code for wiring shall be followed.	
9	Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations. No wire smaller than 3.029 sq.mm shall be used.	
10	Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.	
11	Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.	

Sr No.	Specifications	Complied (Yes/No)
12	Circuits fed from distinct sources of supply or from different distribution boards or MCCB's and M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases.	
13	All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.	
14	Metal clad sockets shall be of diameter cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.	
15	All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.	
16	Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts The earth continuity insulated copper wire in Green color shall be run inside the conduit to earth the third pin or socket outlets, earth terminal of light fixtures, fan etc. as required. Lights points shall be either of single control, twin control or multiple points controlled by a single switch / MCB as per scheduled of work. Bare copper wire shall be provided with each circuit from DB as specified in the item of work and terminated in earth bar of DBs and switch boxes with proper lugs as required maximum number of PVC insulated 1100 grade copper conductor cable which can be drawn in a conduit.	

1.2.2. Specification for Moulded Case Circuit Breakers and Switchboards

Sr. No.	Specifications	Complied (Yes/No)
	Moulded Case Circuit Breakers	
1	General •The circuit breakers shall comply with the requirement of IEC 60947 / IS 13947: 1993. MCCBs shall be suitable for nominal voltage of 3 phase 660 volts electronic release microprocessor control. •The circuit breaker shall comply with the isolation function requirement of IEC 60 947-2 section 7.1.2 to marked as suitable for isolation / disconnection to facilitate safety of operating personnel while the breaker is in use. •The circuit breaker shall provide class II insulation between the front cover and internal power circuits to avoid any accidental contact with the live moan current carrying path with the front cover open. •All MCCB / ACB's required as per BOQ shall have Ics = 100% Ics	
	Switchboards	
2	•Switchboards shall be suitable for operation at three phase 4 wire, 415 volt, 50 Hz, neutral grounded at transformer system with a short circuit level withstand as per schedule of quantities and drawings. •The enclosures shall be designed to take care of normal stress as well as abnormal electro-mechanical stress due to short circuit conditions. All covers and doors provided shall offer adequate safety to operating persons and provide ingress protection of IP 54 unless otherwise stated. Ventilating openings and vent outlets, if provided, shall be arranged such that same ingress protection of IP 54 is retained. Suitable pressure relief devices shall be provided to minimize danger to operator during internal fault conditions.	

1.2.3. Earthing

Sr. No.	Specifications	Complied (Yes/No)
1	Earthing should be done inside the Data Center for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, and AC units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.	
2	All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.	
3	The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.	
4	Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.	
5	The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room.	
6	There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.	
7	The earth connections shall be properly made .A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.	
8	The DCO would be responsible for providing separate Earthing pits for Servers, UPS & Generators as per the standards.	

1.3. UPS: Critical Load

Sr.No.	Description	Complied(Yes/No)
	Make : APC/EMERSON/EATON	
1	The scope shall include supply, transportation, storage, unpacking, erection, testing, successful commissioning and satisfactory completion of trial operations of the same on the rated load . The UPS system should have (i) field replaceable UPS modules (ii)requisite redundancy built up so that under all circumstances the system should be able to supply 200KVA power to the load (iii)the battery backup has to be for 30 mins for the 200KVA Load.	
2	The SI can offer modular UPS systems , each module rated between 25KVA and 50KVA , with either of the below specifications • A single frame of modular UPS of 200KVA capacity with N+1 redundancy with 30 minutes of battery backup at 200KVA Load. Scalability in Capacity to 400KVA should be achievable through addition of similar modules in the same or an additional frame. The Modules should be replaceable without any interruption to the connected load and without putting the Load on Bypass • A Dual frame modular UPS, each individually of Capacity 200KVA operating parallelly, leading to N+N redundancy with 30 minutes of battery backup on individual frame. In case of failure of any module inside one frame, the frame can be taken offline and module changed, while the other frame continues to supply the rated load at 200KVA. This system should also be scalable by adding additional frames.	
3	The UPS battery shall be standard SMF made up by owner replaceable batteries of similar specifications .Notification should be displayed in the UPS display in the case of fault, removal and insertion of any one of the battery banks. Each power module shall contain a fully rated, power factor corrected input rectifier/boost converter hereafter referred to as the PFC input stage, a fully rated output inverter, battery charging circuit, Control & Logic Circuit and field replaceable fans.	
4	The UPS shall automatically maintain AC power within specified tolerances to the critical load, without interruption (for specified duration as per battery run time), during failure or deterioration of the mains power supply.	
5	The UPS system shall be expandable by inserting additional modules of the same rating, to provide for module redundancy or load growth requirements. Each power Module rating shall be maximum 50 KVA and minimum 25 KVA	
6	The manufacturer shall design and furnish all materials and equipment to be fully compatible with electrical, environmental, and space conditions at the site.	
7	It shall include all equipment to properly interface the AC power source to the intended load and be designed for unattended operation.	
8	Standards: The UPS shall be designed in accordance with the applicable sections of the current revision of the following documents. Where a conflict arises between these documents and statements made herein, the statements in this specification shall govern the following: • Low Voltage Directive: CE	

Sr.No.	Description		Complied(Yes/No)
	• General and safety requirements for UPS used in operator access area: IEC/EN 62040-1-1 • Electromagnetic compatibility (EMC) requirements for UPS: IEC/EN 62040-2		
9	Design Requirements - UPS Module	Voltage. Input/output voltage specifications of the UPS shall be: Rectifier Input: [380] 400 [415] volts, three-phase, 4-wire-plus-ground Bypass Input: [380] 400 [415] volts, three-phase, 4-wire-plus-ground	
		Output: [380] 400 [415] volts, three-phase, 4-wire-plus-ground	
10	Design Requirements - UPS Module	Output Load Capacity. Specified output load capacity of the UPS shall be 200KVA at 0.9 power factor. No derating of power capacity from 0 degree to 40 degree ambient.	
11	Design Requirements - UPS Module	Current Sharing: When multiple UPS modules are connected in parallel and powering a common load, each UPS module output current will not differ by more than 5% of the rated full load current of one UPS module.	
12	Design Requirements – Battery	The UPS battery shall support battery plant Sealed Maintenance Free type Batteries. The battery bank monitored for voltage and temperature for use by battery diagnostic. Battery charging current shall be temperature compensated.	
13	Design Requirements – Battery	The UPS shall incorporate a battery management system to continuously monitor the status of battery Bank.	
14	Design Requirements – Battery	The batteries shall be long life batteries (minimum 3 years) and the battery casing shall be flame retardant type. The battery bank should have series parallel combination of batteries, so that in case one module fails, the corresponding UPS should not shut down.	
15	MODES OF OPERATION		
A	Normal:	The PFC input stage and output inverter shall operate in an on-line manner to continuously regulate power to the critical load. The input and output converters shall be capable of full battery recharge while simultaneously providing regulated power to the load for all line and load conditions within the range of the UPS specifications	

Sr.No.	Description		Complied(Yes/No)
B	Battery	Upon failure of the AC input source, the critical load shall continue being supplied by the output inverter, which shall derive its power from the battery system. There shall be no interruption in power to the critical load during both transfers to battery operation and retransfers from battery to normal operation. Upon restoration of utility power to the UPS input, the UPS shall recharge the battery.	
C	Static Bypass:	The static bypass shall be used to provide controller transfer of critical load from the inverter output to the bypass source. This transfer, along with its retransfer, shall take place with no power interruption to the critical load. In the event of a UPS output fault or significant output overload emergency, this transfer shall be an automatic function. Manual transfer to static bypass (called "requested bypass") shall be available in order to facilitate a controlled transfer to maintenance bypass.	
16	PFC INPUT STAGE		
A	General:	The PFC input stage converters of the system shall be housed within the removable power modules, and shall constantly control the power imported from the mains input of the system, to provide the necessary UPS power for precise regulation of the DC bus voltage, battery charging, and main inverter regulated output power. These power modules shall be connected in parallel within the UPS frame.	
B	Input Current	Total Harmonic Distortion: The input current THDI shall be held to <= 5% at rated load while providing conditioned power to the critical load bus, and charging the batteries under steady-state operating conditions. This shall be true while supporting both a linear or non-linear load. This shall be accomplished without the requirement for additional or optional filters, magnetic devices, or other components	
C	Soft-Start Operation:	As a standard feature, the UPS shall contain soft-start functionality, capable of limiting the input current from 0 percent to 100 percent of the nominal input over a default 10 second period, when returning to the AC utility source from battery operation. The change in current over the change in time shall take place in a linear manner throughout the entire operation.	
D	Magnetization Inrush Current:	The UPS shall exhibit zero in-rush current.	
E	Input Current Limit:		

Sr.No.	Description		Complied(Yes/No)
	i. The PFC input stage shall control and limit the input current draw from utility to 124 percent of the UPS output. During conditions where input current limit is active, the UPS shall be able to support 100 percent load, charge batteries at 10 percent of the UPS output rating, and provide voltage regulation with mains deviation -15 percent.		
	ii. In cases where the source voltage to the UPS is nominal and the applied UPS load is equal to or less than 100 percent of UPS capacity, input current shall not exceed 116 percent of UPS output current, while providing full battery recharge power and importing necessary power to account for system losses.		
F	Redundancy:	The UPS shall be capable of being configured with redundant PFC input stages, each with semiconductor fusing, and logic-controlled contactors to isolate a failed module from the input bus.	
G	Charging:		
i.	The battery charging shall keep the DC bus float voltage of ±1 percent.		
ii.	The battery charging circuit shall contain a temperature compensation circuit, which shall regulate the battery charging to optimize battery life.		
iii.	The battery charging circuit shall remain active when in static bypass and in normal operation.		
iv.	The UPS shall be capable of reducing the battery charging current under low input voltage conditions.		
v.	Battery charge shall be limited to 10 percent of the battery Ah capacity by default.		
vi.	An input connection will be provided that will allow the user to inhibit boost charging.		
vii.	The UPS shall be capable of reducing the battery charging current down to zero based on user defined input.		
viii.	Back-Feed Protection: The above mentioned logic-controlled contactor shall also provide the back-feed protection required.		
17	OUTPUT INVERTER		
A	General:	The UPS output inverter shall constantly develop the UPS output voltage waveform by converting the DC bus voltage to AC voltage through a set high frequency power converters. In both normal operation and battery operation, the output inverters shall create an output voltage independent of the mains input voltage. Input voltage anomalies such as brown-outs, spikes, surges, sags, and outages shall not affect the amplitude or sinusoidal nature of the output voltage sine wave of the inverters.	
B	Overload Capability:	The output power converters shall be capable of 230 percent for short circuit clearing. Steady-state overload conditions, of up to 150 percent of system capacity shall be sustained by the inverter for minimum 30 seconds, 125% for 10minutes/ 125% for 1 min or above in normal operation. Overloads persisting past the outlined time limitation the	

Sr.No.	Description		Complied(Yes/No)
		critical load shall be switched to the automatic static bypass output of the UPS.	
C	Battery Protection:	The inverter shall be provided with monitoring and control circuits to limit the level of discharge on the battery system.	
D	Redundancy:	The UPS shall be capable of being configured with redundant output inverters.	
18	STATIC BYPASS		
A	General: As part of the UPS, a system static bypass shall be provided which rated for full capacity of UPS Frame. The system static bypass shall be hot swappable and provide no break transfer of the critical load from the inverter output to the static bypass input source during times where maintenance is required, or the inverter cannot support the critical bus. Such times may be due to prolonged or severe overloads, or UPS failure. The UPS and static bypass switch shall constantly monitor the auxiliary contacts of their respective circuit breakers, as well as the bypass source voltage, and inhibit potentially unsuccessful transfers to static bypass from taking place.		
B	Design: The design of the static switch power path shall consist of silicon-controlled rectifiers (SCR)		
C	Automatic Transfers: An automatic transfer of load to static bypass shall take place whenever the load on the critical bus exceeds the overload rating of the UPS. Automatic transfers of the critical load from static bypass back to normal operation shall take place when the overload condition is removed from the critical output bus of the system. Automatic transfers of load to static bypass shall also take place if for any reason the UPS cannot support the critical bus.		
D	Manual Transfers: Manually initiated transfers to and from static bypass shall be initiated through the UPS graphical user interface.		
E	Overloads: The static bypass shall be rated and capable of handling overloads equal to or less than 125 percent of the rated system output continuously.		
F	Modular: The static bypass switch shall be of a modular design		
G	System Protection: Back-feed protection in the static bypass circuit shall also be incorporated in the system design. To achieve back-feed protection, a mechanical contactor in series with the bypass SCR(s) shall be controlled by the UPS/static switch, to open immediately upon sensing a condition where back-feeding of the static switch by any source connected to the critical output bus of the system is occurring. One such condition could be a result of a shorted SCR.		
19	DISPLAY AND CONTROLS		
A	Control Logic: The UPS shall be controlled by independent fully redundant modules within each power module.		
B	Graphical User Interface: A microprocessor-controlled, user interface/display unit shall be located on the front of the system.		
C	Metered Data: The	a) Input\output voltages, currents, frequencies.	

Sr.No.	Description		Complied(Yes/No)
	following data shall be available on the graphical user interface/display:	b) Breaker and switch status.	
		c) Battery status.	
		d) Event log	
D	Event Log:	The display unit shall allow the Owner to display a time and date stamped log. The event log shall be capable of holding more than 300 events.	
E	Alarms: The display unit shall allow the Owner to display a log of active alarms. The following minimum set of alarm conditions shall be available:	1 Input frequency outside configured range.	
		2 AC adequate for UPS but not for bypass.	
		3 Low/no AC input, startup on battery.	
		3. Intelligence module inserted.	
		4. Intelligence module removed.	
		7. UPS fault.	
		8. On battery.	
		10. Bad power module.	
		11. UPS in bypass due to overload.	
		12. System in forced bypass	
F	Controls: The following controls or programming functions shall be accomplished by the use of the user interface/display unit. The touch screen display shall facilitate these operations:	1) Silence audible alarm.	
		2) Display or set the date and time.	
		3) Enable or disable the automatic restart feature.	
		4) Transfer critical load to and from static bypass.	
		5) Test battery condition on demand.	
		6) Set intervals for automatic battery tests.	
		8) Adjustable ramp-in times from 1 to 40 seconds.	
G	Free Contacts: The following potential free contacts shall be available on an optional relay interface board:	1) Normal operation.	
		2) Battery operation.	
		3) Bypass operation.	
		4) Common fault.	
		5) Low battery.	
		6) UPS off.	
H	Communication Interface Board: A communication interface board shall provide the following communication ports which shall be able to be used simultaneously:	Ethernet interface port for a remote display.	
I	Emergency power off (EPO)	(Note: The EPO pushbutton shall include a protective cover to prevent unintentional operation).	
20	BATTERY		
A	The UPS battery shall support battery plant of SMF batteries		

Sr.No.	Description		Complied(Yes/No)
B	The battery jars housed within each battery shall be of the SMF valve regulated lead acid (VRLA) type of OEM approved make of batteries provided		
C	The UPS shall incorporate a battery management system to continuously monitor the status of battery bank		
D	The batteries shall be long life batteries (minimum 3years or more) and the battery casing shall be flame retardant type.		
E	The UPS shall incorporate a battery capacity test that will be capable of determining available runtimes.		
21	Software and Connectivity		
A	Network Adaptor:	The Ethernet SNMP adaptor shall allow one or more network management systems (NMS) to monitor and manage the UPS in TCP/IP network environments.	
B	Unattended Shutdown:	The UPS, in conjunction with a network interface card, shall be capable of gracefully shutting down one or more operating systems during when the UPS is operation from the battery.	
C	Remote UPS Monitoring: The following methods of remote UPS monitoring shall be available:		
	Simple Network Management Protocol (SNMP):	Remote UPS monitoring shall be possible through a standard compliant platform.	
22	Installation manual, which includes instructions for storage, handling, examination, preparation, installation, and start-up of UPS & User manual, which includes operating instructions must be provided along with.		
23	ISOLATION TRANSFORMER	UPS shall be provided with Input isolation Transformer of 300 KVA capacity	

1.4. UPS: Non-Critical Load

Sr.No.	Description	Complied(Yes/No)
1.	Design : Transformer less based on IGBT rectifier and IGBT inverter	
2.	Technology: Online double-conversion mode	
3.	Waveform Type: Sine Wave	
4.	Configuration: 2 units of 20KVA UPS running in N+1 mode	
5.	Nominal Input Voltage: 400V 3PH	
6.	Input voltage range for main operations: -15%, +20% at 100% load, -50%, +20% at 50% load	
7.	Dual mains Input: Should be available	
8.	Input frequency: 45-55 Hz (auto sensing)	
9.	Input Power Factor at Full Load: At least 0.98	
10.	Output power capacity: 20.0 kVA	

Sr.No.	Description	Complied(Yes/No)
11.	Output Power Factor: 0.8 or more	
12.	Nominal Output Voltage: 400V 3PH	
13.	Other Output Voltages: Configurable for 380 or 415 V 3 Phase nominal output voltage	
14.	Efficiency: 94% at full load	
15.	Output Voltage Distortion: Less than 5% at full load	
16.	Output Frequency: 47-53 Hz for 50 Hz nominal	
17.	Bypass: Maintenance Bypass & Static Bypass both Built-In	
18.	Parallel Capacity: At least 4 units can be connected in parallel	
19.	Operating Ambient Temperature: 0 - 40 °C	
20.	Operating Relative Humidity: 0 - 95 %	
21.	Audible noise at 1 meter from surface of unit: Less than 56dBA	
22.	Protection Class : IP 20	
23.	Battery type: Sealed Maintenance Free type Lead Acid battery with suspended electrolyte : leak-proof	
24.	Charging type: Temperature compensated charging must be available	
25.	Backup Time: 30 minutes on each UPS	
26.	Battery VAH: More than 24000VAH on each UPS	
27.	Approved Battery make: Rocket/Exide/Quanta	
28.	Front Control panel & Alarm: Multifunction LCD status and control console along with audible & visible alarms which is prioritized by severity	
29.	SNMP card: Must be inbuilt	
30.	Emergency Power Off (EPO): Must be available	
31.	Warranty on UPS: Standard 1 year	
32.	**Note:** The UPS system should assure the Data center equipment with continuous power at a solution uptime of 99.749% and with redundancy available up to the load end.	

1.5. Precision AC

Sr.No.	Description	Complied (Yes/No)
a)	Make: APC Schneider/Emerson/Stulz	
b)	Model	
c)	System capacity- 25 Tr = 5 Nos.	
d)	Type of redundancy.N+1 (5+1)	
e)	General Specifications.	
f)	The Precision Air conditioner shall be High sensible cooling capacity and high SHR (i.e. the sensible to total cooling capacity ratio). Low running costs, achieved by using digital/tandem/inverter scroll compressors, combined with an accurate selection of the components. The units to be provided with compatibility of green refrigerant R410a	
g)	The unit construction shall be enables to access all the main components of the	

Sr.No.	Description	Complied (Yes/No)
	machine from the front for installation purposes and routine servicing. Outside panels shall be coated with polyester paint, which guarantees the long-term durability of their original features. The front panels are attached to the framework by means of rapid-coupling "fasteners". The cabinet shall be provided with double skin side panels with inner panel of minimum thickness of 0.8mm and outer panel of thickness of 1.0mm. Insulation in the side panels should be 19 mm thick glass wool and front & back panels should be insulated with 25 mm thick special acoustic mineral wool	
10)	The PAC unit shall be with multiple digital/tandem/inverter scroll compressors arrangement which will enable the system to work at part load & will have better efficiency. Electronic expansion valve which is a class of art device which precisely modulates the flow of refrigerant & maintains a constant superheat, high COP by maintaining a lower condensing temperatures & dehumidification by constant airflow should be a standard part of the system.	
11)	FANS	
a)	**Unit must be provided with** direct drive backward curved fans each running with DC drive electronically communicated motors**, the fans should be aligned and balance statically and dynamically.**	
12)	**EVAPORATOR COIL**	
a)	The exchanger is composed of copper tubes mechanically expanded on aluminum fins, complete with a hydrophilic treatment to reduce the surface tension between the water and the metal surface, thus favoring film-wise condensation.	
b)	The exchanger is situated upstream from the fans to ensure unhindered air distribution and is complete with a stainless steel condensate tray with a flexible conduit for its drainage and an incorporated trap. Coils should be flat/slant in construction which is fully accessible from front.	
13)	**REMOTE AIR COOLED CONDENSER**	
a)	These condensers are characterized by a single circuit exchanger with aluminum finned copper tubes, complete with low-speed axial-flow fans to reduce the sound pressure level. The frame is made of CRCA sheet with excellent weather-resistant characteristics. The remote condenser is complete with an electric power and control board, fully wired and tested at the factory. Condensers shall be suitable for 24 hours operation and be capable of providing vertical or horizontal discharge	
b)	Condenser fan shall be provided with Fan speed controller working based on condensing pressure and should control speed according varying ambient conditions.	
c)	Server room average temperature 20 to 22 Centigrade and Relative umidity:45% to 55% Auxiliary Area : Temperature: 22 to 26 Centigrade Relative Humidity: 50% to 65%	
14)	**ELECTRIC HEATING**	
a)	Electric heating with aluminium-stripped heating elements complete with safety thermostat. It shall have arrangement for manual resetting to cut off the power supply and trigger the alarm in the event of overheating.	
15)	**FILTERATION**	
a)	Air filters of EU5 efficiency made of self-extinguishing, artificial-fiber cellular material. The frame containing the filter material is made of metal. Low airflow and clogged filter alarm sensors consisting of two pressure switches for controlling the operating conditions of the fans and the build-up of dirt on the air filters inside the unit.	
16)	**Humidifier**	
a)	Immersed-electrode/ Infrared humidifier for modulating sterile steam production should be provided with the automatic regulation of the concentration of salts in the	

Sr.No.	Description	Complied (Yes/No)
	boiler to allow for the use of untreated water. Proportional control of the humidifier's operation (achieved by controlling the electric current allowed to pass through the cylinder's electrodes) and the periodic flushing cycle (controlled by continuously monitoring the water's conductivity) guarantee a perfect efficiency of the system, a low energy consumption and a greater durability of the components.	
17)	**MICROPROCESSOR BASED CONTROL**	
a)	The microprocessor controller manages the unit operations autonomously. In direct expansion unit the algorithms permits integral management of the Electronic expansion valve (EEV) with consequent optimization of energy saving, constant air flow during dehumidification and absolute operating stability. Units have been designed and developed to interact with all the most widely used Building Management Systems, exchanging data via the most common communication protocols through serial connections.	
c)	The units should have sequencing as an inbuilt feature. The units shall be designed to work for equal no of run hours also in case of fault the stand by unit should Start.	
d)	The microprocessor control system shall be capable of connecting following optional cards:	
e)	RS485 serial adapter for data transfer to a central supervisor system with STD protocol or MODBUS protocol or SNMP card for tcp / ip	

1.6. New LT DB

Sr.No.	Description	Complied(Yes/No)
1.	**New LT DB Comprising the following**	
1.1	800 Amps 4P 50 kA Incomer MCCB with Microprocessor Based Trip Unit Under voltage Release for Interlock	
1.2	400 Amps 4P 50 kA Outgoing MCCB with Microprocessor Based Trip Unit	
1.3	100 Amps 4P 50 kA Outgoing MCCB with Microprocessor Based Trip Unit	
1.5	PLC for Changeover and Interlock Logic with Battery Backed SMPS	
1.6	Wired Floor Standing IP54 Cabinet with Copper Busbar/Cable/Wires Type 1 Surge Arresters for Incomer Digital Voltmeter & Ammeter for Incomers RYB Indication	
2	**Distribution Cabinet for New UPS 1 no comprising**	
2.1	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	
2.2	160 Amps 4P 25 kA Outgoing MCCB with Microprocessor Based Trip Unit	
2.3	32 Amps 4P 10 kA MCB	
2.8a)	Wired Floor Standing IP54 Cabinet with Copper Busbar/Cable/Wires RYB Indication	
3	**Distribution Cabinet for existing UPS-1 comprising the following**	
3.1	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	
3.2	160 Amps 4P 25 kA Outgoing MCCB with Microprocessor Based Trip Unit	
3.4	Wired Floor Standing IP 54 Cabinet with Copper Busbar/Cable/Wires RYB Indication	
4	**Distribution Cabinet for Raw Power 1 No comprising the following**	
4.1	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	
4.2	100 Amps 4P 25 kA Outgoing MCCB with Microprocessor Based Trip Unit	
	Wired Floor Standing IP54 Cabinet with Copper Busbar/Cable/Wires RYB Indication	
5	**Distribution Cabinet for Auxiliary UPS 1 Comprising the following**	
5.1	100 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	
5.2	32 Amps 4P 10 kA MCB	

Sr.No.	Description	Complied(Yes/No)
5.7	Wired Floor Standing IP54 Cabinet with Copper Busbar/Cable/Wires RYB Indication Industrial Grade Ethernet Switch	
6	**Server DB**	
6.1	160 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	
6.2	63A 10 kA 3P MCB	
6.3	32A 10 kA 1P MCB	
6.6	Wired Wall Mounted IP54 Cabinet with Copper Busbar/Cable/Wires RYB Indication Industrial Grade Ethernet Switch	
7	**Modification in the existing UPS OP Cabinet**	
7.1	400 Amps 4P 25 kA Incomer MCCB with Microprocessor Based Trip Unit	
7.3	Additional Cabinet Section with Copper Busbar/Cable/Wires Industrial Grade Ethernet Switch	

1.7. LAN Passive Components:

1.7.1. Cabling

Sr.No.	Description	Complied(Yes/No)
1	**LC-MPO 24 Core Optical Fiber Cassettes - MPO OM4 FOR NETWORK & SERVER RACK**	
a)	Type: MPO cassettes shall house OM4 Multi Mode, 2 Nos 12-Fiber Cassette.	
b)	Standard: MPO cassettes shall meet the most recent revision of TIA/EIA-568-C.3 standard.	
c)	Connectors: Cassettes shall have 12 LC Duplex connectors on the front and two (12-fiber) MPO connections on the back.	
2	**24 Core LC-MPO Fan-out Cable, OM4 Multi Mode 5 mtr Fiber patch cord**	
a)	Pre-Terminated 24 Core LC-MPO Fan out OM4 LSZH Cable Length 5 meter.	
b)	Patch cord should be LSZH, LC-MPO type	
3	**1G/10G, LC-LC, OM4 Multi Mode 3 mtr fiber patch cord (TYPE - II)**	
a)	Optical Fiber duplex patch cords shall comprise of OM4 Fiber.	
b)	Patch cord should be LSZH, LC-LC type	
c)	The Fiber Patch Cord shall be duplex type and factory terminated with Connectors terminated at each end for connecting SFP modules of supplied Switches with LIU.	
d)	Shall support 1 Giga/10 Giga fiber connectivity	
4	**Optical Fiber Trunk Cable**	
a)	Type: The optical fiber cable used in construction of the optical fiber trunk cables shall contain 12 (OM4) fibers	
b)	Standard: Trunk Assemblies shall be tested to comply with the most recent revision of TIA/EIA-568-C.3 and ISO/IEC 11801 standards.	
c)	Termination: The trunk cables shall be factory terminated in the appropriate number of 12-fiber, [MPO-style] connectors both end. Each [MPO-style] connector shall terminate 12 fibers.	
d)	Polarity: Trunk cable polarity shall be pair-flipped AB/BA. Each trunk cable shall have protective devices to prevent damage to the connectorized ends during installation	
5	**Unloaded Fiber Enclosure for MPO Cassettes**	
a)	Type: 1U, 19 Inch rack mountable metallic distribution enclosure Unloaded with 6 slots for MPO cassettes. Should be capable of / MPO Cassettes with 12 couplers for 24 fiber of OM4.It should have capacity to cater 72/96 Core in 1U Rack Size or 288 Core in 2U Rack size as per requirement. LIU should include sufficient blank plate as required to cover empty cassette space.	
6	**Horizontal cable Manager – Single Sided**	
a)	Assembly – Metallic with cable manager covers	
b)	Cable management accessories for EIA standard 1U height	
7	**Unshielded Twisted Pair, Category 6A, TIA / EIA 568-C-2**	
a)	23 AWG Annealed bare solid copper, CAT-6A U/UTP Cable, Channel optimized to 700 Mhz or more.	
b)	Meets EIA/TIA 568-C.2 Category 6A specifications, UL Listed. Cat 6A U/UTP Solution Zero bit error rate ETL report need to submit. Cat 6A 4 Connector Channel Performance ETL Report need to be submit to validate the cable channel performance..	
c)	Worst Case Cable Skew : 45 nsec/100 meters	
d)	Characteristic Impendence : 100±6 Ù@ 1-500 Mhz	
e)	Insulation HDPE	

Sr.No.	Description	Complied(Yes/No)
f)	Solid Cable should be compliance to RoHS.	
g)	Sheath Fire retardant PVC Compound (FRPVC)	
h)	Standard length: 305 Mtrs (1000 ft.)	
8	**UTP Jacks Type - Unshielded Twisted Pair, Category 6A, TIA / EIA 568-C.2**	
a)	Made from high-impact, flame-retardant, UL- RATED 94v 0 thermoplastic – ABS	
b)	DC Resistance: 69 milli ohms.	
c)	DC Resistance imbalance : 20 milli ohms.	
d)	Insulating resistance 500 Mega ohms minimum.	
e)	Current Rating : 1.5 A (max)	
f)	Spring Contact : 50u" gold over 100u" nickel	
g)	The performance exceeds EIA/TIA 568-C.2 Category 6A component specifications	
h)	The outlet is of IDC (insulation Displacement Contact) 180 deg punch type	
i)	UL Listed specifications	
j)	ROHS compliant	
9	**UTP Jack Panels** **Type - 24-port Unloaded, Unshielded Twisted Pair, Category 6A, TIA / EIA 568-C.2**	
a)	Unloaded, 24-Port & should be capable for Un-shielded	
b)	The keystone modules are fire-retardant, moulded plastic modules UL94 VO rated, consisting of horizontal index strips for ease of re-termination.	
c)	110 IDC Termination 180 degree Punch, allowing wires between 22 – 26 AWG sizes.	
d)	Meets or Exceeds EIA/TIA – 568 – C-2 Category 6A connecting hardware specification.	
e)	RJ45 (8P8C) T568A/T568B colour coding termination.	
f)	Cable Guide way to guide the cable on the rear side	
g)	1U size for 6/12/24/48 Ports.	
h)	UL Listed specifications	
i)	Jack Panel should be RoHS Complaint.	
10	**Faceplates** Type - 1-port, White surface box	
a)	MaterialABS / UL 94 V-0	
b)	No. of portsOne / two	
c)	High Impact Plastic Body ABS FR Grade 86 x 86 mm	
d)	Flush mountable or surface mountable with a back mount frame	
11	**Workstation/Equipment cords** Type - Unshielded Twisted Pair, Category 6A, TIA / EIA 568-C.2	
a)	Patch cords shall be of multi strand copper cable with UL Listed.	
b)	With Matching colored snag-less, elastomer polyolefin boot	
c)	Terminals with gold contacts, 50 micron" gold over nickel	
d)	Patch cord has a characteristic impedance of 100 +/- 3 Ohms	
e)	Patch cord has extra-long boot to maintain the bend radius.	
f)	Assembled with short body RJ45 50u gold plate to minimize untwist pair length.	
g)	Designed for high speed transmission	
h)	Back-ward-compatibility with all current Cat.5 products and applications.	
i)	Material : ROHS compliant	

1.7.2. Technical Specification For Cable Ducts:

Sr No.	Specifications	Complied (Yes/No)
1	**General Requirements :-** Cable ducts are intended for the support and accommodation of cables and possibly other devices in Electrical/Control/ Instrumentation/Communication systems	
2	**Design and Fabrication of Cable Trays / Ladders:-**	
3	The Cable duct shall be fabricated according to the design specified by IEC 61537 and certified for 90 minutes of Fire Protection (E90) as per DIN 4102-12. It should be tested for Safe Working Load (SWL). The relevant details of SWL and the load chart with respect to SWL, supporting distance and the deflection is explained below.	
4	The minimum support distance should be 2 meters, and no supports permitted for installation in less than 2meters	
5	The Cable duct shall be made of Steel, Pre-galvanized sheet (275 gsm) and then Epoxy powder coated with 60-80 microns with bright colors, preferable RAL1023. No Thermoplastic/ Polyester material permitted for straight lengths/ covers in the entire installation	
6	The Cable duct should have all the accessories which can be mounted readily, preferably modular features which is plug and play with no special tools / fasteners for drop-offs, mounting of connectors readily installable on the straight lengths, and easy to manage the changing needs in future	
7	The Cable duct must be strong enough to withstand the installed loads by itself without the need of covers. Covers should be an optional accessory to be used wherever it is required only	
8	The straight lengths of ducts and covers should be available in multiples of 2m or 3m only, and for widths in multiples of 100 mm, Eg. 200mm and 300 mm (4", 8" and 12"). The sides/ height of the Ducts should be 50mm±10mm (2") or 100±10mm (4")	
9	A provision to readily remove and add the cables for expansion / maintenance should be provided without disturbing the support system. The same straight lengths should be supported from one – side (cantilever type) or simply supported from both sides, depending on the installation needs	
	The Safe working load (SWL) for upto 200 mm wide cable ducts should be 60 kg/m when supported at 2m span, and above 200mm wide cable ducts is 35 kg/m when supported at 2m span	
	The CE-marking of products is placed on the product or on the packaging according to Low Voltage Directive 2014/35/EU.	
	EMC directive 2004/108/EC The Cable Support System is neutral according to the EMC directive 2004/108/EC	

1.7.3. PVC Conduit

Sr No.	Specifications	Complied (Yes/No)
1	The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for non-metallic conduit 1.6 mm thick as per IS 9537/1983.	
2	All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.	
3	No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.	
4	All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.	
5	Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw and junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.	
6	Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.	
7	The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.	

1.8. Data Center Infrastructure Management

Sr No.	Description	Complied (Yes / No)
1.	Proposed DCIM should be created in separate installations to maintain sanctity of data as follows: a. Gateway/Convertor Devices: Required for connecting to third party BMS/ third party BMS controller's /field devices etc. b. Monitoring layer: Responsible for polling all Monitoring Points as mentioned in Section D below. c. Converged Infra Management Layer: Responsible for Analytics and Insightful data analysis of DCIM data points. d. Specialized IT server level Integration for CPU and Power profiling which may be an inherent part of Monitoring Layer as well for some DCIM OEM. e. Cluster or Backup Server for Management Layer f. The bidder should quote for 500 nodes. Actual number will be confirmed during design in implementation phase	
2.	The Gateway/Convertor so proposed to integrate third party BMS/BMS controllers and Field devices over Modbus /Modbus TCP, Bacnet /bacnet-ip, Lon should be able to communicate natively via BACnet, LonWorks, and Modbus and should support simultaneous exchanges on its various protocols, essentially meaning you can use all protocols at once hence giving us a single device to aggregate all type of protocol devices.	
3.	The Gateway/Convertor should employ a modular I/O design to allow expansion of the unit to incorporate more Field devices if so required in future for AI/AO/DI/DO. This Input and output capacity is to be provided through plug-in modules of various types.	
4.	The Gateway/Convertor should have its own web interface to display various register information polled across various Field devices or through third party BMS systems over BACNET/Modbus. Through this Web Interface it should provide global supervisory control functions so that user can log on to engineer, Features commission, supervise, and monitor its attached I/O modules and field bus devices.	
5.	Converged Management Layer concept arise from the fact that irrespective of various underlying components like Power, Cooling, Network, U space all of them have to converge to a single unified system. This System should facilitate the complete Lifecycle approach for Datacenter involving: a. Analysis b. Design c. Implement d. Operate e. Evaluate	
6.	a. Empty Racks	
	b. Filled Racks: stating the Racks are being used by a Process/Client	
	c. Reserved: Racks reserved for a specific Process/Client	
	d. Internal Use: Racks reserved for some Internal requirements	
7.	Predictive Analysis/What If Analysis & Hypothetical Provisioning/Modelling to ease decision making (such as: where is the best place to put new server, do my dc have sufficient power, cooling & space to occupy new equipment, etc.)	
8.	Power Path: Ability to model power connections between the equipment supplying and delivering power and the equipment requiring power. This includes power path from switchgear, UPS, main PDU with modular circuit breaker mapping, rack	

Sr No.	Description	Complied (Yes / No)
	RPDU and to individual servers.	
9.	Impact simulation: Generates a list of equipment that would be impacted if the selected piece of equipment, e.g. a UPS or cooling unit, about to fail or put in maintenance mode.	
10.	Power Capacity: Ability to assign planned capacity for each rack and illustrate rack capacity consumption compared to the planned/ recommended values for that rack. Provide information such as remaining power, the amount exceeding the recommended capacity etc.	
11.	The DCIM tool will have a dedicated Equipment browser view where device Fields can be customized and sorted as per user need. It should allow for export of these data fields in the same format in a CSV file which can be opened in Excel as set by the user in the Equipment browser and also to save these formats for later use inside the DCIM.	
12.	The graphical floor plan of the configured data center layout should include overlays showcasing capture index (CI), plenum pressure, plenum velocities, and 3D rendering of the temperature map, including airflow and temperature thresholds. As the design takes place, client will get a qualified estimation of the effect of changes in supply temperature, airflow, and number of cooling units and room-based cooling parameters. The data is expected to be simulated on the basis of plate rating of various cooling devices, racks, perforated tiles, grilles etc.	
13.	In the 3D view, client should be able to see the room's simulated airflow above the raised floor. Velocity vector and temperature results should look like those from traditional CFD applications and provide the same ability to quickly locate problem spots and understand the underlying causes.	
14.	DCIM thermal model should incorporate Thermal calculations utilizing both mechanisms: Simulated and Real Time T/H sensor polling. User should have the ability to simulate his datacenter on any of them at any time and see Thermal Maps in X, Y and Z Planes.	
15.	DCIM should facilitate the 3D model to depict equipment's placed on Rack Mounted Trays like Modems stacked on a Tray.	
16.	DCIM thermal model should allow Third Party Building Management Rack T/H sensors also to be utilized for calculating Thermal Maps apart from the DCIM OEM's own T/H sensors.	
17.	Commissioning: The solution should provide provisions to recommend the best location for a server in the rack layout, utilizing available space, cooling, and power capacity	
18.	The application should provide real time Power Usage Effectiveness (PUE), DCIE values and able to deliver Weekly, Monthly, Quarterly & Yearly PUE report.	
19.	DCIM should be able to deliver the cost and CO_2 emission per subsystem where subsystem data can either be measured (live) or computed (without power meters).It should showcase graphs for IT load, current PUE/DCiE, historical PUE/DCiE, costs and CO_2 emission per subsystem.	
20.	Real time server power consumption and Real time cpu utilization. This detection of server level details should happen without installing any special agents on the servers for discovery using standard protocols like SNMP, WMI, SSH, Telnet or through VMWARE/service processor integration. WMI, SSH, VMWARE access would be through root level administrator logins per server or vCenter basis which will be given to DCIM vendor by the client.	

Sr No.	Description	Complied (Yes / No)
21.	This Module will be able to control and put the CRAC units in Software driven and Manual Mode as required in certain instances.	
22.	The Module will be responsible to create Cooling Influence Maps for the data center, clearly showcasing the Influence of specific CRAC units on certain regions across the datacenter. This would help the client in identifying which CRAC to run at any point of time.	
23.	Should Monitor all the MCCBs at all and Rack PDU units and create a summary report. Any problem should generate alert SMS and trigger a mail to designated personnel.	
24.	Proposed platform should offer Dashboard & Reporting on data center key performance indicators, displaying customizable information for a high-level overview of data center operations.	
25.	We understand that certain DCIM systems may have restrictions to the number of points being Trended so to keep it logical the OEM will have to provision for trending and reporting parameters on site as per their mutual discussion during Pre Installation Survey. Any transducers or sensors necessary should be provisioned by SI . At minimum DCIM should provide Trending and Reporting for the following(include necessary sensors/meters)	
a)	PUE- Daily, Weekly, Monthly	
b)	Total Facility Load	
c)	Total IT Load	
d)	Total Cooling Load	
e)	Row Wise IT Load	
f)	Rack Wise IT Load	
g)	PDU Wise IT Load	
h)	MCCB wise Current (Phase wise)	
i)	Avg Temperature and Humidity at Cold Aisle	
j)	Avg Temperature and Humidity at Hot Aisle	
k)	Avg temp of 8 designated High Density Racks	
l)	CFM of ECM Fans from PAC	
m)	CFM of Active tiles	
n)	Energy Meter: Per phase input voltage and Current	
o)	Energy Meter: Per phase Output voltage and Current	
p)	Power Factor per phase	
q)	Frequency	
r)	Active Energy in KWH/MWH	
s)	Transformer Temperatures	
t)	Transformer Oil Level	
u)	UPS Per Phase Load percentage	
v)	UPS Input Power	

Sr No.	Description	Complied (Yes / No)
w)	UPS Output Power	
x)	UPS Time Running on Battery	
y)	CRAC/Inrow : Supply Air Temperature	
z)	CRAC/Inrow : Return Air Temperature	
aa)	CRAC/Inrow : Supply Air Temperature Set point	
bb)	CRAC/Inrow : Supply Air Humidity Set point	
cc)	Diesel Generator: Per Phase Voltage	
dd)	Diesel Generator: Mains Frequency	
ee)	Diesel Generator: Genset Frequency	
ff)	Diesel Generator: Engine Speed (rpm)	
gg)	Diesel Generator: Oil Pressure	
hh)	Diesel Generator: Oil Temperature	
ii)	Diesel Generator: Fuel Level	
jj)	Diesel Generator: Running Time	
kk)	Existing BMS system has to be integrated to DCIM	

1.9. Video Wall Specifications

Sr No.	Specification		Complied (Yes/No)
1	Monitor Type	LED	
2	Panel Technology	IPS	
3	Screen Size	46/47" (diagonal)or Higher	
4	Aspect Ratio	(16:9)	
5	Native Resolution	1,920 x 1,080 (Full HD) or higher	
6	Brightness	450nit or higher	
7	Contrast Ratio	1,200 : 1 or more	
8	Dynamic CR	400,000 : 1 or higher	
9	Viewing Angle (H x V)	178 x 178 degree	
10	Response Time	Up to 12ms (GTG σ)	
11	Orientation	Portrait & Landscape both	
12	Inputs		
13	Digital	HDMI(1),DVI-D(1) **, 1 no RJ45**	
14	Analog	RGB(1), Component (RGB Shared), AV	
15	Audio	PC Audio In-1, AV/Component Audio In (RCA-1]	
16	External Control	RS232C(1), RJ45(1), IR(1)	
17	USB	1 or more	
18	Outputs		
19	Digital	DVI-D(1) or Display Port (1) as required	
20	Analog	RGB(1)	
21	Audio	External Speaker-1	
22	External Control	RS232C(1)	
23	Bezel to Bezel Gap	4.9 mm or less	

1.10. Modular Architecture based Video Wall Controller for 3*2 Video Wall

(Approved makes: AMX / ATEN / EXTRON / CRESTRON/DELTA/BARCO)

Sr No.	Specifications	Complied (Yes/No)
1	Supports up to 8 or higher Digital Input sources (Either DVI / VGA / HDMI or Combination of DVI & HDMI)	
2	Support from OEM for a period of 5 years after FAT .	
3	Supports up to 8 or higher Digital Outputs e.g Displays (Either DVI or HDMI or Combination of DVI & HDMI)	
4	Seamless Switch feature provides continuous video streams, real-time switching and stable signal transmission	
5	It should be able to implement matrix system architecture to easily switch between multiple sources and multiple displays	
6	Looping less Videowall . No Loop In Loop Out is Allowed	
7	It should have a provision to put a Redundant Power Supply	
8	Built-in wizard – provides an easy way to customized settings	
9	Control & Configuration through Ethernet, RS232 & front panel buttons	
10	It should be Hot Swappable i.e cards can be removed and inserted without shutting down the system	
11	Equipped with front paneled LCD for operation display	
12	Support high data transfer rate at 1080p / 1920 x 1200 @ 60Hz	
13	Superior video quality – HDTV resolution of 480p, 720p, 1080i, and 1080p (1920 x 1080), VGA, SVGA, SXGA, UXGA (1920 x 1080)	
14	It should have a built in Scalar so that it can scale the input resolution of the displays upto 1080p.	
15	Every Input & Output Board has Analog balanced/unbalanced stereo audio inputs/outputs for separate audio routing	
16	It should support Bezel Adjustment Setting .	
17	Videowall profile creation depending upon the number of displays connected. Profile Scheduling, Digital Signage Profile, Videowall Profile.	
18	GUI Features: Customize Profile, Scheduling, Scaling resolution,	
	The Panel should be lockable for security purposes	

1.11. 46/47 Inch or Higher LED Monitor

Sr. No.	Description	Complied (Yes/No)
1.	Panel Diagonal Size 46"/47"	
2.	Resolution 1920x1080 (16:9)	
3.	Pixel Pitch(mm) 0.53025(H) x 0.53025(V)	
4.	Brightness min 700 nits/700cd per m2	
5.	Dynamic Contrast Ratio 10000:1	
6.	Viewing Angle(Horizontal/Vertical) 178/178	
7.	Response Time (G-to-G) 8ms	
8.	Display Color 8 bit - 16.7M	
9.	Static Contrast Ratio 4,000:1	
10.	Connectivity Input –RGB , HDMI , DVI-D	
11.	HDMI, DVI	

1.12. IBMS Components

VESDA, CCTV camera, VIDEO STREAMER and Integration of Gas Based Fire Suppression System

1.12.1. Supply, Installation, Testing & Commission of Split AC Units

Sr.No.	Specifications	Complied (Yes/No)
1	(I) 2TR Split, Wall Mount AC Unit with wired remote & anti corrosion finish stand for outdoor unit. . The AC units will be 3 Star rated for energy efficiency. (Electrical, UPS etc. Room) (II) Copper refrigerant piping of required size with insulation making opening / cutouts in partitions, brick walls as required complete. (III) Electrical Cabling for 2TR split unit indoor to outdoor making opening / cutouts in brick walls, partitions as required complete. (IV) Sequential Time controller for 2TR AC unit (V) Copper refrigerant piping with insulation making opening / cutouts in brick masonry walls, partitions for 2 TR Split units (VI) Electrical Cabling for 2 TR split unit indoor to outdoor making opening / cutouts in brick masonry walls, partitions (VII) Drain piping for all AC units making opening / cutouts in brick masonry walls, partitions	

1.12.2. Water Leak Detection system

Sr	Specifications	Complied (Yes/No)
1	Supply, Installation, Testing & Commission of Water Leak Detection System.	
2	Water Leak detection panel	
3	Water Leak detection module	
4	Water leak detection cable sensor (30 Mtrs) including end connectors, mounting accessories.	
5	Electronic Hooter	
6	Supply and laying of 3 core 4 sqmm FRLS armoured cable complete with tags, ferruling ...etc.	
7	WLD Interface card to be monitored through Modbus, backnet or SNMP	

1.12.3. Biometric Door Access System

Sr. No.	Specifications	Complied (Yes/No)
1	Optical Fingerprint scanner with 500 dpi resolution	
2	Registration Time <1 Sec , 1:1 Match < 1 sec, 1:N match <1 sec for 1000 templates	
3	Equal Error Rate < 0.1%	
4	User Database capacity of 30,000	
5	Transaction storage capacity of last 60,000 events	
6	Capacity to store 1900 fingerprint templates expandable up to 9000	
7	Built in most accurate RTC (Real Time Clock) with Lithium cell backup	
8	Built in Card reader for different authentication modes like only Finger , only Card, Card + Finger	
9	Card reader options – HID iClass, Mifare	
10	RJ45 High speed Ethernet connectivity	
11	Interface for exit reader	
12	Interface for door lock, exit switch & door sensor	
13	Support of template on card mode with contactless smart card	
14	Support of command cards for easy user management	
15	Multicolor LED indication for successful match	
16	Programmable Buzzer & LED control from controller	
17	Sleek plastic molded enclosure	
18	Operating voltage 12VDC	

1.12.4. Access Control System

Sr. No.	Specifications	Complied (Yes\No)
1	The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on proximity as well as biometric technology for the critical areas and Proximity technology for non-critical areas.	
2	An access control system consisting of a central PC, intelligent controllers, proximity readers, power supplies, proximity cards and all associated accessories is required to make a fully operational on line access control system.	
3	Access control shall be provided for doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure.	
4	The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors.	
5	Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts.	
6	Controlled Entries to defined access points	

Sr. No.	Specifications	Complied (Yes\No)
7	Controlled exits from defined access points	
8	Controlled entries and exits for visitors	
9	Configurable system for user defined access policy for each access point	
10	Record, report and archive each and every activity (permission granted and / or rejected) for each access point.	
11	User defined reporting and log formats	
12	Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.	
13	Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.	
14	One user can have different policy / access rights for different access points.	
15	Should be able to check the reports, logs, define access policies/configuration.	

Additional Points:

Sr. No.	Specifications	Complied (Yes/No)
1	Access controller 2 door tcp/IP based capable of handling entry and exit of doors with Built in power supply unit and with all accessories. UL listed	
2	PROXIMITY Card Reader with 2" - 4 " read range fastened with security screws.	
3	Electro Magnetic Lock with magnetic contact.	
4	Exit Push Button	
5	Emergency Release Switch	
6	Smart card - Blank Face	
7	Access Management Client Software UL listed.	
8	Panic bar for emergency exit. (If applicable)	
9	Supply and laying of 2/4 core 1.5/1 sq. mm shielded FRLS armored cable complete with tags, ferruling.	
10	Supply and laying of 6 core 1 sq. mm shielded FRLS armored cable complete with tags, ferruling.	

1.12.5. Fire Detection and Control Mechanism

Fire Alarm System:

Sr. No.	Specifications	Complied (Yes/No)
1.	Rugged CRCA sheet with powder coated finish.	
2.	Operates on 220V, A.C supply	
3.	Battery backup with built in charging	
4.	16 X 2 LCD Dot Matrix Display.	
5.	Evacuate and Key pad Enable, Disable Facility.	
6.	Low battery visual warning with audible tone.	
7.	Relay output for actuators.	
8.	Remote fire indication with Audible Tone.	
9.	Compatible to all types of conventional detectors.	
10.	Zone Disable (Isolation) facility with loop voltage cut off.	
11.	Intelligent Addressable standalone fire alarm control panel 1 Loop with battery backup of 24 hrs in normal condition and 30 min in alarm condition with battery charger, power supply and all necessary accessories. UL listed	
12.	Intelligent Addressable Smoke multi criteria detectors with base.	
13.	Response Indicator	
14.	Intelligent Addressable Manual Pull Station	
15.	Short circuit Isolator module	
16.	Addressable sounder	
17.	Intelligent Addressable control module for Access Control, PAC, Gas discharge.	
18.	Intelligent Addressable Monitor module.	
19.	Supply and laying of 2 core x 1.5 sq.mm shielded FRLS Armoured cable red in colour with saddles, spacers, Junction box, lugs, glands, ferruling.	
20.	Hand held fire extinguisher CO2 4.5 KG ISI Marked	
21.	Repeater panel	
22.	Two mode operation facility (Auto / Manual).	
23.	Programmable FAP input selection Facility.	
24.	Programmable Solenoid Output with On and OFF Timer.	
25.	Main / Standby Cylinder output Facility (Optional).	
26.	Gas Inhibition and Instant release facility.	
27.	Manual Gas Release with or without timer.	
28.	Actuator pressure low sensing facility.	
29.	Pressures switch facility.	
30.	The Fire alarm system shall be an automatic 1 to n (e.g. 24) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.	
31.	Detection shall be by means of automatic heat and smoke detectors located throughout the Data Center (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.	

32.	The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.	
33.	All controls of the system shall be via the control panel only.	
34.	All site-specific data shall be field programmable and stored in an integral EEPROM. The use of EPROM's requiring factory 'burning' and re-programming is not acceptable.	
35.	All internal components of the control panel shall be fully monitored.	
36.	The control panel shall be capable of supporting a multi device, multi zone 2-wire detection loop. Removal of 1 or more detection devices on the loop shall not render the remaining devices on the loop inoperable.	
37.	The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.	
38.	All user primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2. Essential controls, such as Start / Stop sounders and Cancel fault buzzer, etc. will be clearly marked.	
39.	Cancel fault and display test functions shall be configurable to be accessed from level 1 or level 2.	
40.	All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.	
41.	The control panel shall log a minimum of 700 events comprising of 100 event fire log and 200 event fault, disablement and historic logs, giving time, date, device reference and status of indication.	
42.	Fire, fault and disablement events shall be logged as they occur. Visual and audible conformation shall be given on an array of LEDs, the Liquid Crystal Display and the internal supervisory buzzer.	
43.	The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full alarm load conditions. The system shall be capable of full re-charge within 24 hours following full system discharge. The performance of the power supply and batteries shall be monitored and alarm rose, should a fault be detected. The system shall protect the batteries from deep discharge.	
44.	All terminations within the control panel with the exception of the 230V mains connection will be via removable terminal screw fixing points.	
45.	The control panel will have a programmable maintenance reminder to inform the user that maintenance of the system is required. This function shall provide the user with the option of a monthly, quarterly, annually or bi-annually reminder prompts. The maintenance reminder will be indicated on the control panel. This message shall be resettable by the user and will not require the intervention of specialist support. The control panel will provide programmable free text field as part of the maintenance reminder facility.	
46.	The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.	
47.	Start sounders	
48.	Silence sounders	
49.	Reset system	

50.	Cancel fault buzzer	
51.	Display test	
52.	Delay sounder operation	
53.	Verify fire condition	
54.	Enter or modify device text label	
55.	Setup maintenance reminder	
56.	Assign or modify zones	
57.	Disable zones, device, sounders, FRE contact, auxiliary contacts	
58.	Action weekly test	
59.	Disable loop	
60.	The control panel will include the necessary top entry and rear entry cable entry points via 20mm knockouts.	
61.	MCP's shall be addressable and of the steady pressure break glass type manufactured to the requirements of BS 5839: Part 2. A test key shall be provided to allow the routine testing of the unit to meet the requirements of BS 5839 Part 1 1988, without the need for special tools or the need to unfasten the cover plate.	
62.	The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. The device shall incorporate a short circuit isolation device and a red LED indicator.	
63.	The MCP shall be suitable for surface or flush mounting. When flush mounted the device shall be capable of fixing to an industry standard single gang box.	
64.	Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.	
65.	Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.	
66.	Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.	
67.	The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.	
68.	All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.	
69.	The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.	
70.	Detector bases shall fit onto an industry standard conduit box.	
71.	The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.	
72.	The labelling of Device and Zone labels should be part of the system.	
73.	Necessary Software to the control panel	

1.12.6. Fire Suppression System

Sr.No.	Specifications	Complied (Yes/No)
1	Supply and installation of fire suppression system with necessary gas cylinders, valves, piping, nozzles, mounting arrangement and all other accessories required for safe operation. Bidder shall submit execution drawings prior to execution for approval	
2	Fast and effective against a wide range of Class A, B and electrical fires.	
3	Safe for occupied areas	
4	Non-corrosive and electrically nonconductive	
5	No post-discharge residue and clean-up	
6	Environmentally acceptable	
7	25 / 42 bar system	
8	Range of system release options	
9	Low installation and maintenance costs	
10	Computer design maximizes effectiveness of system	
11	Also shall have:	
	i. 80 Ltr. Seamless Cylinder with valve with discharge hose, nozzle, Cylinder low pressure switch and necessary accessories. As per the fire standards.	
	(i) NOVEC 1230 Extinguishing gas	
	(ii) Solenoid Actuator Assy 24V DC	
	(iii) Manual Actuator	
	(iv) Pneumatic actuator	
	(v) Flexible discharge hose	
	(vi) Actuation hose	
	(vii) Manifold check valve (UL)	
	(viii) Abort Switch	
	(ix) Manual release switch	
	(x) Nozzle (UL)	
	(xi) Rack-Wall mount kit	
	(xii) M.S. Seamless pipes as per ASTM A 106 Gr. B, schedule 40 with necessary fittings.	
	(xiii) Signage and hooter outside the room	
	(xiv) 2 Zone Gas Release Panel with Battery Backup	
	(xv)Smoke Detector	
	(xvi) Hooter	
	(xvii) 2 core x 1.5 sq.mm cu. Armoured cable	

Sr.No.	NOVEC Cylinder Specifications	Complied (Yes/No)

Sr.No.	NOVEC Cylinder Specifications	Complied (Yes/No)
1.	Fire suppression system shall deploy NOVEC 1230 based gas suppression systems with cross-zoned detector systems for all locations. These detectors should be arranged in a manner that they activate the suppression system zone wise to cater to only the affected area.	
2.	Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm	
3.	The OEM (/ Bidder) shall give a Certificate stating that their NOVEC system is approved by UL / FM / VDS / LPC/CNPP for use with Seamless Steel Cylinders (Component as well as System Approval).	
4.	The OEM (/ Bidder) shall also provide a Letter that the OEM has NOVEC Flow Calculation software suitable for Seamless Steel cylinder bided for as per the Bill of materials and that such Software shall be type approved by FM / UL / VdS / LPC.	
5.	The Storage Container offered shall be of Seamless type, meant for exclusive use in NOVEC systems, with VdS/FM/UL/LPC/CNPP component approval. Welded cylinders are not permitted.	
6.	The Seamless storage cylinder shall be approved by Chief Controller of Explosives, Nagpur and shall have NOC from CCOE, Nagpur for import of the same. Documentary evidence to be provided for earlier imports done by the bidder.	
7.	The NOVEC valve should be Differential Pressure Design and shall not require an Explosive / Detonation type Consumable Device to operate it.	
8.	The NOVEC Valve operating actuators shall be of Electric (Solenoid) type, and it should be capable of resetting manually. The Valve should be capable of being functionally tested for periodic servicing requirements and without any need to replace consumable parts.	
9.	The individual NOVEC Bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure.	
10.	The system flow calculation is carried out on certified software, suitable for the Seamless Steel Cylinder being offered for this project. Such system flow calculations shall be also approved by VDS / LPC/ UL / FM.	
11.	The system shall utilize 25 Bar / High pressure (362 psi) technology that allows for a higher capacity to overcome frictional losses and allow for higher distances of the agent flow; and also allow for better agent penetration in enclosed electronic equipment's such as Server Racks/ Electrical Panels etc.	
12.	The designer shall consider and address possible Fire hazards within the protected volume at the design stage. The delivery of the NOVEC system shall provide for the highest degree of protection and minimum extinguishing time. The design shall be strictly as per NFPA standard NFPA 2001.	
13.	The suppression system shall provide for high-speed release of NOVEC based on the concept of total Flooding protection for enclosed areas. A Uniform extinguishing concentration shall be 4.7% (v/v) of NOVEC for 21 degree Celsius or higher as recommended by the manufacturer.	
14.	The system discharge time shall be 10 seconds or less, in accordance with NFPA latest standard.	
15.	Sub floor and the ceiling void to be included in the protected volume.	
16.	The NOVEC systems to be supplied by the bidder must satisfy the various and all requirements of the Authority having Jurisdiction over the location of the protected area and must be in accordance with the OEM's product design criteria.	

Sr.No.	NOVEC Cylinder Specifications	Complied (Yes/No)
17.	The detection and control system that shall be used to trigger the NOVEC suppression shall employ cross zoning of photoelectric and ionization smoke detectors. A single detector in one zone activated, shall cause in alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.	
18.	The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's certified software, which shall also be approved by third party inspection and certified such as UL / FM / VDS / LPC.	
19.	The Cylinder shall be equipped with differential pressure valves and no replacement parts shall be necessary to recharge the NOVEC containers.	
20.	NOVEC shall be discharged through the operation of an Electric (solenoid) operated device or pneumatically operated device, which releases the agent through a differential pressure valve.	
21.	The bidder shall provide all documentation such as Cylinder Manufacturing Certificates. Test and Inspection Certificates and Fill Density Certificates.	
22.	The NOVEC discharge shall be activated by an output directly from the `NOVEC' Gas Release control panel, which will activate the solenoid valve. NOVEC agent is stored in the container as a liquid. To aid release and more effective distribution, the container shall be super pressurized to 360 psi (g) at 21°C with dry Nitrogen.	
23.	The releasing device shall be easily removable from the cylinder without emptying the cylinder. While removing from cylinder, the releasing device shall be capable of being operated, with no replacement of parts required after this operation.	
24.	Upon discharge of the system, no parts shall require replacement other than gasket, lubricants, and the NOVEC agent. Systems requiring replacement of disks, squibs, or any other parts that add to the recharge cost will not be acceptable.	
25.	The manual release device fitted on the NOVEC Cylinder(s) shall be of a manual lever type and a faceplate with clear instruction of how to mechanically activate the system. In all cases, NOVEC cylinders shall be fitted with a manual mechanical operating facility that requires two-action actuation to prevent accidental actuation.	
26.	NOVEC storage cylinder valve shall be provided with a safety rupture disc. An increase in internal pressure due to high temperature shall rupture the safety disc and allow the content to vent before the rupture pressure of the container is reached. The # contents shall not be vented through the discharge piping and nozzles.	
27.	NOVEC 1230 containers shall be equipped with a pressure gauge to display internal pressure.	
28.	Brass Discharge nozzles shall be used to disperse the `FM-200'. The nozzles shall be brass with female threads and available in sizes as advised by the OEM system manufacturer. Each size shall come in two styles: 180° and 360° dispersion patterns.	
29.	All the Major components of the NOVEC system such as the Cylinder, Valves and releasing devices, nozzles and all accessories shall be supplied by one single manufacturer under the same brand name.	
30.	Manual Gas Discharge stations and Manual Abort Stations, in conformance to the requirements put forth in NFPA 2001 shall be provided.	
31.	Release of NOVEC agent shall be accomplished by an electrical output from the NOVEC 1230 Gas Release Panel to the solenoid valve and shall be in accordance with the requirements set forth in the current edition of the National Fire Protection Association Standard 2001.	

1.12.7. CCTV

Sr. No.	Specifications	Complied (Yes/No)
1	The Critical area of the Data Center along with the Non Critical area needs to be under constant video surveillance. The primary objective of implementing a CCTV system is to ensure effective surveillance of the area and also create a record for post event analysis. Monitoring cameras should be installed in proper areas to cover all the critical areas of the data center. The scope of work involves supply, installation, commissioning, testing and maintenance of the Closed Circuit Television system for State Data Center.	
2	The CCTV system shall provide an on-line display of video images on monitor. The entire setup shall be monitored from the control room on 24/7 basis. Cameras with suitable lenses shall be used to view all the critical areas of the Data Center, Reception and Corridor.	
3	The CCTV system shall be based on the use of fixed dome cameras	
4	The CCTV System shall be colour, fixed and designed for continuous duty. The system and each of its devices shall be designed to meet the site ambient temperature and the site environmental conditions and shall operate satisfactorily under the specified permitted voltage and frequency variation band of the power supply source system.	
8	A complete CCTV control facility that performs all the functions with provision to increase the total number of inputs for each monitor site.	
9	CCTV Cabinets as required complete with all cable termination facilities, cable distribution system for video and power system along with any additional video amplifiers and other video equipment as may be required.	
11	Test equipment covering all tools, tackles and testing equipment / kits as required for preventive and first line maintenance including test monitors, camera adjustment and testing facilities.	
12	Complete range of accessories as required.	
13	All necessary relay boxes connectors, extension cables and adapter boxes as required at each of the ends of the CCTV System as required.	
14	All systems and components shall have been thoroughly tested and proven in actual use.	
15	All systems and components shall be provided with a one-day turnaround repair express and 24-hour parts replacement. The manufacturer and SI will provide warranty for 5 years after FAT	
16	Specifications included in this section are indicative and considered as a minimum; component and software that shall be acquired at the time of implementing the project shall be the latest versions available in the market.	
17	The system also should provide clear & accurate indication of an intruder or abnormal movement within and around the Facility.	
18	The system shall provide visual images from the cameras located throughout the facility. The cameras located shall be fed into the NVR located in the BMS room.	
19	The NVR shall consist of 16 channels Digital Multiplexer with built-in recording system into Hard Disk.	
20	The Main Security Control Room which shall house the Monitors and the NVR	
21	The CCTV should be equipped with Digital recording facility for later scrutiny, with at least 90 days of recording facility.	
22	The cameras will be of 1/3" format CCD pickup device for fixed lens camera. The cameras	

Sr. No.	Specifications	Complied (Yes/No)
	are being used for special observation purposes.	
23	The cameras being used at these locations shall have the following basic minimum requirements:	
24	The cameras shall be fixed dome camera cameras shall be complete with the latest state of the art optical systems, filters, light sensitive pickup systems suitable for capturing images with very low light levels, and necessary interlaced scanners, encoders, decoders, associated amplifiers, synchronization facilities and any interfacing adapters as required, with all systems of that type suitable for a compact, durable, distortion free and clear image processing type camera.	
33	The cameras shall have standby circuitry for when the camera is not selected on any of the monitors. The beam current of the camera pickup device shall be switched off automatically.	
34	The cameras shall have automatic circuitry which relates the black level in the signal to the darkest spot of the picture (black level control), limits the video signal in case of scene high-lights in order to prevent overloading of the monitor (White limiter), and prevents the automatic sensitivity control from reacting to strong highlights (Peak white eliminator).	
47	The monitor shall be suitable for use as desktop units.	
48	The monitors shall be high-resolution video monitors. The monitor shall have a bandwidth of at least 10 MHz (-3dB) and a horizontal resolution in the center of the picture minimum 420 lines in the case of colour monitor.	
49	The monitors shall have the facilities to loop the video signal through the other monitor.	
50	Each monitor shall have local control knobs and remote control equipment and panel for monitor controls associated with power on/off switch standby on/off switch and for adjustment brightness, contrast, horizontal hold, vertical hold etc.	
51	Dome Cameras should be with the following specs • Image sensor 1/2.8 MOS • Supported Video Codec H.265 / H.264 / JPEG • Resolution Full HD (1,080p) • Max. FPS H.265/H.264 50 / 60 • Super Dynamic / WDR / BLC Wide Dynamic • Day/Night Day / Night (ICR) • Day/Night Day / Night (ICR) • Lens f=3.6mm, F2.0 • Angular field of view H: 87 deg. V: 48 deg. • SD memory Card Slot 1 • Power POE, 12 VDC • Temp 5 deg to 55 degree Centigrade	

Sr. No.	Specifications	Complied (Yes/No)
52	**The NVR should carry the following specifications** User-friendly GUI for easy operation supported Connection to IP camera, IP dome and video server Connection to Hikvision, Panasonic, Sony, AXIS, Bosch, SANYO IP cameras, etc. Support decoding at H.264, MPEG4 compression standard, etc. Stream storage at PS standard capsulation format ols Up to 1280×1024 VGA output resolution Up to 1920×1080 HDMI output resolution Support high-definition video preview, storage and playback. Digital zoom in preview and playback Up to 16-ch synchronous playback Different recording storage period configurable for each channel Redundant recording HDD management in groups NTP,SMTP and NFS support Up to two 10/100/1000Mbps self-adaptive UTP Ethernet interfaces. Support TCP/IP, UDP, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, and NFS (access to NAS) protocol. Unicast and multicast transmission; TCP, UDP, and RTP protocols supported in unicast. Remote search, playback and download, lock/unlock of video files; support breakpoint resume. Remote access and configuration of parameters; remote import/export of device configuration parameters. Remote access of device running status, system log and alarm status. Remote button operation. Remote lock/unlock of front panel buttons and mouse. Remote formatting of hard disk, upgrade, reboot/shutdown and other system maintenance operations. RS -232/RS-485 transparent channel transmission. Event alarm and exceptions upload to remote management center. Remote manual recording. Remote video image capture in JPEG format. Local output via HDMI/VGA, Main or Spot video/audio output port. HDMI display, with up to 1920×1080 resolution. VGA display, with up to 1280×1024 resolution. 1/4/6/8/9/16-division video live view, with adjustable cameras order for display. Group switch, manual switch and automatic cycle modes selectable for video live view, with the auto cycle period configurable. Digital zooming in live view mode. Motion detection, video loss detection and video tampering detection configurable. Privacy masking capability. Configuration and call up of presets, patrols and patter Supports up to eight SATA HDD, eight network HDD(eight NAS disks or seven NAS disks+one iSCSI disk), each disk can support over 2TB Scheduled and event video recording parameters configurable separately. Multiple recording types, including manual, continuous, alarm, motion, motion | alarm and motion & alarm recording, etc. Min 8 recording time periods configurable with separate recording types.	

Sr. No.	Specifications	Complied (Yes/No)
	Search of record files by event type. Lock and unlock of video files over client software. Local redundant recording. Up to 16-channel synchronous Record files backed up via USB device or SATA CD-RW. Support backup he files via e-SATA(optional) Bunch backup by file or by time. Backup video clips in playback. Management and maintenance for backup devices.	

1.12.8. Rodent Repellent and Pest Control System

Sr.No.	Specifications	Complied (Yes/No)
1.	Ultrasonic Rodent System consists of one main console, 12 transducers & a cable bundle of 0.25 Sq.mm 2 core cable.	
2.	The main console is a microcontroller based system with embedded power electronic circuits to generate a pattern of ultrasound waves at 800mW power output per transducer. The Master Console is installed in the control room and the satellites in the problem area. The successful bidder shall make detailed working drawings and coordinate them with other agencies at site.	
3.	All parameters such us start frequency, end frequency, sweep time, wave pattern etc. can be keyed in using smart keypad & alpha numeric LCD.	
4.	Principle of Operation The powerful high frequency sound waves (well above the 20 K Hz frequency which is the upper limit of the hearing range of human ear) generated by the satellites are within the hearing range of the many pests and cause them pain and discomfort and thereby, forcing them to abandon the protected area.	
5.	To be monitored through communication protocol like Modbus. Backnet or SNMP protocols	
6.	Features	
7.	**Master Console**	
	The Master Console would need a power connection and should be equipped with a 3-pin power supply cord of 2.5 meters.	
	Satellites	
	Each Satellite should cover an open area of 300sq. ft. when the average height of the ceiling is 10 ft. When installed in false ceiling / false flooring it should cover an approximate area of 150 sq. ft.	
	• Each satellite should occupy a maximum of space of 24 cu.in. And could be mounted in any angle.	
	• They should be mono-polar and there should be no risk of sparking	
	• They should be able to withstand high temperatures in the false ceilings.	
	• They would not need a power connection.	
8.	Technical Information	
9.	**Satellites**	
	• Crystal DM 44T 24V MAS Germany. Visible Hexagonal, Triangle excitor center damp horizontal line excitors.	
	• Frequency :Peak frequency responses of the satellites should be,	
	o 21.6 KHz +/- 3 KHz	
	o 31.6 KHz +/- 3 KHz	
	o 50.4 KHz +/- 3 KHz	
	o 60 KHz +/- 3 KHz	
	• Nature of Sound Waves. The sound waves propagated by the satellites should be linear sine waves with constantly varying frequencies.	
	• Operating Environment. The satellites should operate in a temperature range of – 4 Deg. C to 60 Deg. C, and can propagate sound waves in 100% humid conditions, and even when they are submerged under water.	
10.	• Pressure should vary from 50 dB to 110 dB (with built – in control for steady output).	
11.	Power Supply. Provision for 230 VAC and 24 VDC	
12.	The entry of Rodents and other unwanted pests shall be controlled using both chemical&	

Sr.No.	Specifications	Complied (Yes/No)
	non-chemical, non-toxic devices.	
13.	Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. To be extended to the electrical room also.	
14.	Master Console with necessary transducer	
15.	Above 20 KHz(Variable)	
16.	50dB to 110dB (at 1 meter)	
17.	800mW per transducer	
18.	15W approximately	
19.	230V AC 50 Hz	
20.	Wall/Table mounting	
21.	There will no false ceiling in Server room as cabling will be through ladder based over the top. The repellant system may be designed for false ceiling only for the non-critical area.	

1.13. Infrastructure Set Up and required civil and interior works

1.13.1. Raised Flooring

Sr.No.	Specification	Complied (Yes/No)
1	False flooring - 600mm ht	
2	Providing and fixing Access floor systems as per following specifications confirming to EN 12825 or equivalent standards.	
3	Access floor system to be installed should provide a maximum finished floor height of 600 mm from the existing floor level. The entire Access floor system will provide for adequate fire resistance, acoustic barrier and air leakage resistance.	
4	PANEL: Panels will be made up of inert material Calcium Sulphate. The bottom of the panel shall be of 0.05 mm Aluminum foil to create a fire and humidity barrier and this should provide floor's electrical continuity. Panels will remain flat through and stable unaffected by humidity or fluctuation in temperature throughout its normal working life. The Panels will be UL listed/ FM/DM approved.	
5	Panels will provide for impact resistance top surfaces minimal deflection, corrosion resistance properties and shall not be combustible or aid surface spread of flame. Panels will be insulated against heat and noise transfer. Panels will be 600 x 600mm x 30 mm height fully interchangeable with each other within the range of a specified layout. Panels shall rest on the grid formed by the stringers which are bolted on to the pedestals. Panels shall be finished with anti-static 0.9 mm Laminate and 0.45 mm thick plastic edge material that is self-extinguishing and will be PVC free	
6	Panel Loading: The system will provide for suitable pedestal and under-structure designed to withstand Concentrated point load: 450 Kg as per European standard EN 12825*. Uniformly Distributed Load (UDL) : 2000 Kgs/M^2	
7	Fire Rating: The Panels will confirm to class O and Class 1 Fire Ratings tested as per BS 476 Part 6 & 7 (30 min). The factory test certificate for fire rating of 30 min to be furnished.	
8	Pedestals: Pedestal installed to support the panel will be suitable to achieve a finished floor height of 600mm. Pedestal design will confirm speedy assembly and removal for relocation and maintenance. Pedestal base to be permanently secured to position on the sub-floor. Pedestal assembly will provide for easy adjustment of leveling and accurately align panels to ensure lateral restrain. Pedestals will support an axial load of 1500 Kgs, without permanent deflection and an ultimate load of 3000 Kgs. Pedestal head will be designed to avoid any rattle or squeaks	
9	Pedestal Assembly : The structure is made entirely of galvanized steel consisting of min 80 mm diameter, 1.5 mm thick base plate, with 6 shaped stiffening ribs with niches that improve adhesion and with minimum 4 holes mechanical fastening to the ground. The assembly will provide a range of height adjustment up to 25mm, with the help of check nuts.	
10	Understructure: Understructure system consists of stringers of size minimum 500 x 30x 25 x 0.7 mm thick to form a grid of 600 x 600mm. These stringers are locked into the pedestal head and run both ways. The system will provide adequate solid, rigid and quiet support for access floor panels.	
11	Stringers: Stringer system is composed of a special frame, made of pressed galvanized steel plate and with a section 25mm wide, 30 mm high and 0.8 mm thick. The longitudinal ribs and flaps in the lower part should be designed to increase flexion resistance. The grid formed by the pedestal and stringer assembly will receive the floor	

Sr.No.	Specification	Complied (Yes/No)
	panel.	

1.13.2. Partitions

Sr.No.	Specification	Complied (Yes/No)
1	Providing and fixing in position full height partition wall of 125 mm thick fire line gyp-board partition using 12.5 mm thick double fire line gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition	
2	Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cutouts for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating.	
3	With glazing including the framework of 4" x 2" powder coated aluminum section complete (in areas like partition between server room & other auxiliary areas).	
4	Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).	
5	All doors should be minimum 1200 mm (4 ft) wide.	
6	Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for the partition wall between the Server Farm of approx. 1500 sq.ft. complete with all the required accessories.	

1.13.3. Painting

Sr.No.	Specification	Complied (Yes/No)
1	Providing and applying Fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.	
2	For all vertical Plain surface.	
3	For fire line gyp-board ceiling.	
4	Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.	
5	Applying approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.	

1.13.3.1. Civil Work

Sr.No.	Specification	Complied (Yes/No)
1	Providing and laying 115 mm thick brick work in cement mortar of 1:4 (1 cement: 4 sand) with bricks of approved quality chamber bricks of class designation 50.	
2	Providing & making SS signage with text in etched & black painted to be located as directed (wall mounted) for space nomenclature/ directions.	
3	Plastering with cement mortar 1:5 (1 cement : 5 sand) of 12 mm thick in interior face of the walls and concrete columns including hacking the concrete surface brushing, scaffolding, curing and surface shall be smooth trowel finish as per standard specification.	
4	Anti-termite treatment of the entire critical area.	
5	The Outer Wall will be of 10 inch including Plaster.	
6	The Interior walls will be 5 Inch including plaster. It should be made of fire retardant bricks and be reinforced by Concrete pillars as deemed necessary.	
7	The Reception lounge, Managers Room, Passage has to be build up as shown. The Partitions will be of fire rated material. The NOC, MUX or Network Room or BMS Room should have fire rated Gypsum partition with front of NOC made of Fire rated glass.	

2. General Guidelines

i. SI shall envisage implementing the IPv6 enablement. The existing SI/DCO will support in implementing IPV6 implementation during the migration process.
ii. Approach to implementing Green Data Center shall be adhered
iii. SI to adopt industry leading practices for effective power utilization and shall time to time review the niche techniques which may be followed by O&M team post implementation.
iv. All the hardware specifications mentioned in the RFP are the required minimum, higher or better specifications would be acceptable.
v. Component furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such component's and/or needed for erection, completion and safe operation of the component's as required by applicable codes though they may not have been specifically detailed in the technical specification, unless included in the list of exclusions. All similar standard components/parts of similar standard components provided shall be inter-changeable with one another.
vi. The methodology of cabling and installation work to be adopted for the State Data Center has to ensure minimum damage to the existing structure of the building. Any damage to the existing flooring/ walls/paint etc. shall be made good by the selected bidder. It is advised that bidder should visit site before submitting the tender to get apprised about the site conditions.
vii. The selected bidder shall be responsible for providing all materials, components, and services, specified or otherwise, which are required to fulfill the intent of ensuring operability, maintainability, and reliability of the complete component covered under this specification within his quoted price. This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.
viii. The selected bidder shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools for completing the scope of work as per the specification is also the responsibility of the selected bidder.
ix. The selected bidder shall perform the services and carry out its obligations with all due diligence, efficiency and economy in accordance with generally accepted professional techniques and practices and shall observe sound management practices and employ appropriate advance technology and safe methods. The selected bidder shall always act in respect of any matter relating to this contract or to the services as faithful advisers to the SIA.
x. The selected bidder shall furnish complete, well-fabricated and reliably operating and secure systems to SIA. Design and selection of component and software shall be consistent with the requirements of long term trouble free operation with highest degree of reliability and maintainability. All components shall be constructed to operate safely without undue heating, vibration, wear, corrosion, electromagnetic interference or similar problems and all software shall be proven, tested and reliable.
xi. All interconnecting cables required to connect the communication component shall be furnished. All cables shall be fully assembled connector pre-terminated and factory tested as part of overall system checkout. Cables shall be neatly & properly tied up and dressed using appropriate cable hangers and Velcro bands. All the cables, connectors, sockets, panel's etc. shall be labeled for identification purpose. All the cabling should adhere to the TIA-942 Data Center Standard.
xii. All component, accessories and cables supplied under this contract shall be in accordance with the latest applicable recommendations, regulations and standards of:
    - CCITT / ITU
    - ANSI
    - IEC 60364
    - IEEE Standard 1100
    - IETF
    - TIA 942
    - IS 3843
    - EIA / TIA 568 Standards

- NFPA 72 and NFPA 318
- International Electro-technical Commission (IEC)
- Cable (Cat 6a) and cable accessories (Cat6a) UL Listed and verified

xiii. For parameters not covered under the above codes, internationally acceptable standards shall be accepted. The selected bidder shall furnish a complete list of all standards and codes under which his component is designed, manufactured and assembled along with the bids.

xiv. Functionality/accessibility of each component of the system and the system as a whole should be demonstrated to the satisfaction of SIA.

xv. Reliable over voltage and over current protection circuits shall be provided in the component power supply units. The component power supply units shall be self-protecting and also protect connected component's against interference, noise, voltage dips and surges & impulses that may be present in the mains power supply sources

xvi. Component shall be guaranteed for operation over the following AC power range to be made available by SIA: 240 V AC +/-10%, 50 Hz +/- 5%

xvii. The SIA shall provide suitable AC power at a single power point at one locations and distribution of this power to the various component's shall be responsibility of the selected bidder for which necessary distribution board, cable etc. shall be provided by the selected bidder.

xviii. Bidder who provides Environmental Friendly Solution (Power Savings etc.) would be preferred.

xix. The bidders must provide data sheets, white papers, OEM certificates and any other third party research papers in support of the quoted items against the minimum specifications provided in this RFP.
MCCBOEM's for all products as applicable should be from Gartner's leader quadrant of last 2 years (except Firewall for which OEM must be rated as 'leaders' or 'Challengers' in the last 2 years Magic Quadrant)

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____

SECTION – J

TECHNICAL CAPABILITY OF BIDDER

(Tender No.WTL/PAR/SDC/17-18/029)

Sl. No.	Project Name	Start Date	End Date / Status	Brief description of project & scope of work (implementation, operation & maintenance)	Type of project	Approx value of the project	Contact details of the Customer

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____

Note:

A. Type of Project shall indicate the implementation of services (Supply& Installation of VC / Networking).
B. Scope of work shall indicate whether it is implementation, Operation or maintenance.
C. Submit Customer Order Copy details of the order indicating the project value, customer contact details.

SECTION – K

FINANCIAL CAPABILITY OF BIDDER

(Tender No.WTL/PAR/SDC/17-18/030)

FINANCIAL INFORMATION

Sl. No.	Name of the Bidder	Turnover (Rs. / Crores)		
		2013-14	2014-15	2015-16
1				

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____

Note:
Submit the audited financial statement/ audited annual report of the last three financial years.

SECTION – L

BIDDERS'S DETAILS

(Tender No.WTL/PAR/SDC/17-18/030)

1	Name of the Firm	
2	Registered Office Address	
	Contact Number	
	Fax Number	
	E-mail	
3	Correspondence / Contact address	
	Name & Designation of Contact person	
	Address	
	Contact Number	
	Fax Number	
	E-mail	
4	Is the firm a registered company? If yes, submit documentary proof	
	Year and Place of the establishment of the company	
6	Former name of the company, if any	
7	Is the firm ▪ a Government/ Public Sector Undertaking ▪ a propriety firm ▪ a partnership firm (if yes, give partnership deed) ▪ a limited company or limited corporation ▪ a member of a group of companies, (if yes, give ▪ name and address and description of other companies) ▪ a subsidiary of a large corporation (if yes give the name and address of the parent organization). If the company is subsidiary, state what involvement if any, will the parent company have in the project.	
8	Is the firm registered with Sales Tax department? If yes, submit valid VAT Registration certificate.	
9	Is the firm registered for Service Tax with Central Excise Department (Service Tax Cell)? If yes, submit valid Service Tax registration certificate.	
10	Total number of employees. Attach the organizational chart showing the structure of the organization.	
11	Are you registered with any Government/ Department/ Public Sector Undertaking (if yes, give details)	
12	How many years has your organization been in business under your present name? What were your fields when you established your organization	
13	What type best describes your firm? (Purchaser reserves the right to verify the claims if necessary) ▪ Manufacturer ▪ Supplier ▪ System Integrator ▪ Consultant ▪ Service Provider (Pl. specify details) ▪ Software Development ▪ Total Solution provider (Design, Supply , Integration, O&M)	

	▪ IT Company	
14	Number of Offices in district headquarters in West Bengal	
15	Is your organization has ISO 9001:2008 certificates?	
16	List the major clients with whom your organization has been / is currently associated.	
17	Have you in any capacity not completed any work awarded to you? (If so, give the name of project and reason for not completing the work)	
18	Have you ever been denied tendering facilities by any Government / Department / Public sector Undertaking? (Give details)	

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Company Rubber Stamp: _____

SECTION – M

MANUFACTURER'S AUTHORIZATION FORM

Date:

To
Webel Technology limited
Plot-5, Block-BP, Sector-V
Salt Lake
Kolkata-700 091

Ref: Tender No.: WTL/PAR/SDC/17-18/030 dated 27.11.2017

WHEREAS _____ who are official producers of _____ and having production facilities at _____ do hereby authorize _____ located at _____ (hereinafter, the "Bidder") to submit a bid of the following Products produced by us, for the Supply Requirements associated with the above Invitation for Bids.

When resold by _____, these products are subject to our applicable standard end user warranty terms.

We assure you that in the event of _____, not being able to fulfill its obligation as our Service Provider in respect of our standard Warranty Terms we would continue to meet our Warranty Terms through alternate arrangements.

We also confirm that _____is our authorized service provider/system integrator and can hence provide maintenance and upgrade support for our products.

We also confirm that the products quoted are on our current product list and are not likely to be discontinued within 5 years from the day of this letter. We assure availability of spares for the products for the next five years after three years warranty.

We also confirm that the material will be delivered within 45 days from the date of placement of confirmed order.

Name In the capacity of

Signed

Duly authorized to sign the authorization for and on behalf of _____

Dated on _____ day of_____2017

Note: This letter of authority must be on the letterhead of the Manufacturer and duly signed by an authorized signatory.

SECTION – N

FORMAT FOR PRE-BID MEETING QUERY

(Tender No.WTL/PAR/SDC/17-18/030)

Name of the Bidder:

Queries

Sl. No.	Section No.	Clause No.	Page No.	Queries

Note: The filled form to be submitted in XLS & PDF Format. There is a cutoff date for receiving of queries before Pre Bid Meeting. Queries received after the cutoff period will not be accepted. The Purchaser reserves the right to respond all queries over e-mail.

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Company Rubber Stamp: _____

SECTION - O

SUPPORT SERVICE CENTER & MANPOWER DETAILS OF BIDDER

(Tender No.WTL/PAR/SDC/17-18/030)

Sl. No.	Name of Place	Address	Name of Support Personnel	Contact Number

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Company Rubber Stamp: _____

SECTION – P

LIST OF CLIENTS OF SIMILAR ORDERS

(Tender No.WTL/PAR/SDC/17-18/030)

Sl. No.	Name of the Client	Address	Contact Person	Designation	Contact Numbers

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Company Rubber Stamp: _____

SECTION – Q

PROFORMA FOR PERFORMANCE BANK GUARANTEE

(On non-judicial stamp paper of appropriate value to be purchased in the name of executing Bank)

PROFORMA OF BANK GUARANTEE FOR SECURITY DEPOSIT –CUM-PRFORMANCE GUARANTEE

Ref ..... Bank Guarantee no.....

Date.....
PROFORMA OF BG FOR SECURITY DEPOSIT

KNOW ALL MEN BY THESE PRESENTS that in consideration of WEBEL TECHNOLOGY LIMTED, a Government of West Bengal Undertaking incorporated under the Companies Act, 1956 having its Registered office at Webel Bhavan, Block EP&GP, Sector V, Kolkata-700 091 (hereinafter called "The Purchaser") having agreed to accept from _____(hereinafter called "The Contractor") Having its Head Office at _____, a Bank guarantee for Rs. _____ in lieu of Cash Security Deposit for the due fulfillment by the Contractor of the terms & conditions of the Work Order No. _____dated_____ issued by the Purchaser for _____(hereinafter called "the said work order _____ _____dated_____)". We _____ (Name & detailed address of the branch) (hereinafter called "the Guarantor") do hereby undertake to indemnify and keep indemnified the Purchaser to the extent of Rs._____ (Rupees _____ _____) only against any loss or damage caused to or suffered by the Purchaser by reason of any breach by the Contractor of any of the terms and conditions contained in the said Work Order No. _____ dated_____ of which breach the opinion of the Purchaser shall be final and conclusive.

(2) AND WE, _____DO HEREBY Guarantee and undertake to pay forthwith on demand to the Purchaser such sum not exceeding the said sum of _____Rupees_____) only as may be specified in such demand, in the event of the Contractor failing or neglecting to execute fully efficiently and satisfactorily the order for _____ _____ Work Order no. , _____dated _____

(3) WE _____ further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said order as laid down in the said Work Order No. _____ dated _____ including the warranty obligations and that it shall continue to be enforceable till all the dues of the Purchaser under or by virtue of the said Work Order No. _____ dated _____ have been fully paid and its claims satisfied or is charged or till the Purchaser or its authorized representative certified that the terms and conditions of the said Work Order No. _____ dated _____ have been fully and properly carried out by the said contractor and accordingly discharged the guarantee.
(4) We _____ the Guarantor undertake to extend the validity of Bank Guarantee at the request of the contractor for further period of periods from time to time beyond its present validity period failing which we shall pay the Purchaser the amount of Guarantee.

(5) The liability under the Guarantee is restricted to Rs. _____ (Rupees _____ _____) only and will expire on _____ and unless a claim in writing is presented to us or an action or suit to enforce the claim is filled against us within 6 months from _____ all your rights will be forfeited and we shall be relieved of and discharged from all our liabilities (thereinafter)

(6) The Guarantee herein contained shall not be determined or affected by liquidation or winding up or insolvency or closer of the Contractor.

(7) The executants has the power to issue this guarantee on behalf of Guarantor and holds full and valid power of Attorney granted in his favour by the Guarantor authorizing him to execute the Guarantee.

(8) Notwithstanding anything contained herein above, our liability under this guarantee is restricted to Rs. _____ (Rupees _____) only and our guarantee shall remain in force up to _____ and unless a demand or claim under the guarantee is made on us in writing on or before _____ all your rights under the guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there under.

WE, _____ lastly undertake not to revoke this guarantee during the currency except with the previous consent of the Purchaser in writing. In witness whereof we _____have set and subscribed our hand on this _____ day of _____.

SIGNED, SEALED AND DELIVERED

_____
(Stamp of the executants)

WITNESS

1) _____

2) _____
(Name & address in full with Rubber Stamp)

INSTRUCTIONS FOR FURNISHING BANK GUARANTEE

1. Bank Guarantee (B.G.) for Advance payment, Mobilization Advance, B.G. for security Deposit-cum-Performance Guarantee, Earnest Money should be executed on the Non- Judicial Stamp paper of the applicable value and to be purchased in the name of the Bank.
2. The Executor (Bank authorities) may mention the Power of Attorney No. and date of execution in his/her favour with authorization to sign the documents. The Power of Attorney is to be witnessed by two persons mentioning their full name and address.
3. The B.G. should be executed by a Nationalised Bank/ Scheduled Commercial Bank preferably on a branch located in Kolkata. B.G. from Co-operative Bank / Rural Banks is not acceptable.
4. A Confirmation Letter of the concerned Bank must be furnished as a proof of genuineness of the Guarantee issued by them.
5. Any B.G. if executed on Non-Judicial Stamp paper after 6 (six) months of the purchase of such stamp shall be treated as Non-valid.
6. Each page of the B.G. must bear signature and seal of the Bank and B.G. Number.
7. The content of the B.G. shall be strictly as Proforma prescribed by WTL in line with Purchase Order /LOI/ Work Order etc. and must contain all factual details.
8. Any correction, deletion etc. in the B.G. should be authenticated by the Bank Officials signing the B.G.
9. In case of extension of a Contract the validity of the B.G. must be extended accordingly.
10. B.G. must be furnished within the stipulated period as mentioned in Purchase Order / LOI / Work Order etc.
11. Issuing Bank / The Bidder are requested to mention the Purchase Order / Contract / Work Order reference along with the B.G. No. For making any future queries to WTL.

SECTION –R

NIT DECLARATION

(Bidders are requested to furnish the Format given in this section, filling the entire Blank and to be submitted on Bidder's Letter head)

To
WebelTechnologyLimited
Plot–5,Block–BP,SectorV,SaltLakeCity,
Kolkata–700091.

Sub:.

Dear Sir,

We the undersigned bidder/(s) declare that we have read and examined in details the specifications and other documents of the subject tender no. WTL/PAR/SDC/17-18/030 dated 27.11.2017 for "Revamping & Physical Expansion of West Bengal State Data Center" published by Webel Technology Limited in e-Tender website.

We further declare that we have agreed and accepted all the clauses / sub-clauses / formats / terms & conditions other requirements related to the said tender and we will abide by the same as mentioned in the tender document while participating and executing the said tender.

Thanking you,

Yours faithfully

.....
Signature

.....
Name in full

.....
Designation

.....
Company Stamp

Dated, this.....dayof.....2017