ODISHA COMPUTER APPLICATION CENTRE

REQUEST FOR PROPOSAL

Enq.No.-OCAC-DC-PMU-0001-2025-25118

Odisha Computer Application Centre (OCAC) invites Request for Proposal (RFP) for Selection of a System Integrator to Establish and Manage the Disaster Recovery Centre-cum-Data Centre Infrastructure at Keonjhar, Odisha. For details please visit websites www.ocac.in & www.odisha.gov.in.

The bid shall be submitted in electronic mode only in the portal **https://enivida.odisha.gov.in** latest by **05.02.2026, 2:00 P.M.** OCAC reserves the right to accept/ reject any/ all bids without assigning any reason thereof.

General Manager(Admin), OCAC, Plot No.-N-1/7-D, Acharya Vihar, P.O.-RRL, Bhubaneswar-751013, Ph.-2567280/ 2567064/ 2567295

Request for Proposal

Request for Proposal for Selection of a System Integrator to Establish and Manage the Disaster Recovery Centre-Cum-Data Centre Infrastructure at Keonjhar, Odisha

RFP No- OCAC-DC-PMU-0001-2025-25118

Odisha **C**omputer **A**pplication **C**entre
(Technical Directorate of E & I.T. Department, Government of Odisha)
N-1/7-D, Acharya Vihar, P.O. - RRL,
Bhubaneswar - 751013
EPBX: 674-2567280 / 2567064 /2567295 / 2567283
Fax: +91-674-2567842
E-mail ID: contact@ocac.in
Website: www.ocac.in

1. Contents

2. Invitation of Bids

2.1. Important Dates

Sl.	Activity	Timeline
1	Availability of Bid Document in the website (www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in/)	30/12/2025
2	Last date for receiving queries through e-mail: **gm_ocac@ocac.in** & **tenders.ocac@odisha.gov.in**	08/01/2026 by 05:00 PM
3	Pre-bid Conference	13/01/2026 at 04:00 PM at OCAC Conference Room
5	Last date and time for Submission of Bid through **https://enivida.odisha.gov.in/**	05/02/2026 by 02:00 PM
6	Opening of Pre-Qualification (PQ) Bids	05/02/2026 by 04:00 PM
7	Opening of Technical Bids (TQ)	To be intimated Later
8	Date of Technical Presentation	To be intimated Later
9	Opening of Commercial Bids	To be intimated Later

2.2. Disclaimer

The information contained in this RFP, or subsequently provided to bidders, whether verbally, in documentary form, or in any other manner by or on behalf of OCAC or any of its employees or advisers, is provided to bidders on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is issued by OCAC. It is not an agreement, nor is it an offer or invitation by OCAC to prospective bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in formulating their bids pursuant to this RFP. This RFP includes statements that reflect various assumptions and assessments arrived at by OCAC. The extension of such assumptions, assessments, and statements does not purport to contain all the information that each applicant may require.

This RFP may not be appropriate for all persons, and it is not possible for OCAC, its employees, or advisers to consider the objectives, technical expertise, and particular needs of each party who reads or uses this RFP.

The assumptions, assessments, statements, and information contained in this RFP, may not be complete or adequate. Each bidder should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments and information contained in this RFP and obtains independent advice from appropriate sources. The information provided in this RFP to the bidders is on a wide range of matters, some of which depends upon interpretation of law.

OCAC makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust, enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender or arising in any way in this Bid Stage.

OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever, caused arising from reliance of any Bidder upon the statements contained in this Tender. may in its absolute discretion, but without being under any obligation to do so, update, supplement the information, assessment or assumptions contained in this Tender. The issue of this Tender does not imply that OCAC is bound to select a Bidder or to appoint the Preferred Bidder for the Project and OCAC reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

OCAC reserves all the rights to cancel, terminate, change, or modify this selection process and/or requirements of bidding stated in the RFP, at any time without assigning any reason or providing any notice and without accepting any liability for the same.

The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. OCAC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on the law expressed herein. OCAC its employees and advisers make no representation or warranty and shall have no liability to any person including any applicant under any law, statute, and rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this selection process.

OCAC also accepts no liability of any nature whether resulting from negligence or otherwise, however, caused arising from reliance of any bidder upon the statements contained in this RFP.

The bidder shall bear all its costs associated with or relating to the preparation and submission of its Proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by OCAC, or any other costs incurred in connection with or relating to its proposal. All such costs and expenses will remain with the bidder and OCAC shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a bidder in preparation or submission of the bid proposal, regardless of the conduct or outcome of the selection process.

3. General Instructions to Bidders

While every effort has been made to provide comprehensive and accurate background information, requirements, and specifications, Bidders are expected to draw their own conclusions regarding the requirements. Bidders and recipients of this RFP are advised to seek independent legal advice in relation to the contents of this document.

All information furnished by the Bidders shall be treated as contractually binding upon them, upon the successful award of the assignment by OCAC based on this RFP. Bidders whose solutions are developed in an entity incorporated in a country sharing a land border with India shall not be eligible to participate in this bid.

In accordance with clause 11. Public Procurement & Procurement of IT Software & Services by Government, para 3, page no 23, of Odisha ICT Policy 2025, Government of Odisha stipulates mandatory participation & collaborative arrangement (min 25% of deployment and maintenance components) for implementation with local enterprises with experience and know-how. The successful bidder should ensure compliance to the above and the “Lead/Prime Bidder” shall remain solely and fully responsible for the overall performance of the Contract, including that of all subcontractors.

This RFP supersedes and replaces any previous public documentation or communication in this regard, and Bidders shall not place reliance on any such prior communications.

3.1. Bid Invitation

Odisha Computer Application Centre invites offer/proposal from interested bidders for “**Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha**” for a period of five (5) years from date of “Final Acceptance Test (FAT) report”. This RFP document is being published on web Portal www.ocac.in, www.odisha.gov.in, and https://enivida.odisha.gov.in. This section provides general information about the issuer, important dates, and addresses for bid submission & correspondence for the bidders. The bidders are advised to study the RFP document carefully. Submission of bids shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

Odisha Computer Application Centre is the nodal agency of Odisha State working towards promotion & implementation of IT, ITeS, and e-Governance. It is the single point of access to any IT business opportunity in the state of Odisha and encourages various players in the field of IT to come forward and invest in the state. OCAC is committed to generating IT business for the public/private sector with a mandate from the Government to develop IT/ITeS in the state. This includes opportunities for software development, supply of hardware & peripherals, networking and connectivity, web applications, e-commerce, ICT training and an entire gamut of direct and indirect IT/ITeS business. The Bid document may be purchased by any interested Bidder on submission of a written application along with the Bid

document fee of Rs. 11,200/- including GST in the form of Demand Draft/ electronic fund transfer from a scheduled bank of India in favor of Odisha Computer Application Centre, payable at Bhubaneswar, during office hours on any working day. The complete bid document has also been published on the website www.ocac.in, www.odisha.gov.in, for downloading. The downloaded bid document shall also be considered valid for participation in the bid process, but such bid documents should be submitted along with the required Bid document fee as mentioned above.

3.2. Fact Sheet

<table>
<tr><td>Proposal inviting agency</td><td>Odisha Computer Application Centre</td></tr>
<tr><td>Start date of Uploading document</td><td>30/01/2025</td></tr>
<tr><td>Non-Refundable RFP Bid Document Fee</td><td>Rs. 11,200 (Including GST)/- in the form of DD/ Bankers Cheque in favour of “OCAC” payable at Bhubaneswar from a nationalized / scheduled commercial bank in India
Bidder has the option to submit the Bid Document Fee through electronic mode to the mentioned Bank account and submit the proof of Bank Transfer screenshot in the PQ Bid Document
<table>
<tr><td>Bank A/c No.</td><td>149311100000195</td></tr>
<tr><td>Payee Name</td><td>OCAC Training</td></tr>
<tr><td>Bank Name & Branch</td><td>Union Bank of India, Acharya Vihar, Bhubaneswar</td></tr>
<tr><td>Account Type:</td><td>Current</td></tr>
<tr><td>IFSC</td><td>UBIN0814938</td></tr>
</table></td></tr>
<tr><td>Contact information</td><td>The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O., – RRL, Bhubaneswar 751013
Ph. - 0674-2582850/ 2588064
Website: www.ocac.in, www.odisha.gov.in, and https://enivida.odisha.gov.in</td></tr>
<tr><td>Last date & time for submission of pre-bid queries</td><td>08/01/2026 by 05:00 PM</td></tr>
<tr><td>Date & time of pre-bid conference</td><td>13/01/2026 at 04:00 PM at OCAC Conference Room</td></tr>
<tr><td>Earnest Money Deposit - (EMD)</td><td>Rs 4,00,00,000.00 (Four Crores) in form of DD / Bank Guarantee in the format prescribed in the annexure.</td></tr>
</table>

<table>
<tr><td></td><td>Bidder has the option to submit the EMD through electronic mode to the mentioned Bank account and submit the proof of Bank Transfer screenshot in the PQ Bid Document
<table>
<tr><td>Bank A/c No.</td><td>149311100000195</td></tr>
<tr><td>Payee Name</td><td>OCAC Training</td></tr>
<tr><td>Bank Name & Branch</td><td>Union Bank of India, Acharya Vihar, Bhubaneswar</td></tr>
<tr><td>Account Type:</td><td>Current</td></tr>
<tr><td>IFSC</td><td>UBIN0814938</td></tr>
</table></td></tr>
<tr><td>Last Date and Time for Submission of Bid Document</td><td>05/02/2026 by 02:00 PM</td></tr>
<tr><td>Opening of Pre-Qualification Bid</td><td>05/02/2026 at 04:00 PM</td></tr>
<tr><td>Opening of Technical Bids & Presentation by the qualified bidder.</td><td>Will be intimated later</td></tr>
<tr><td>Opening of Commercial Bids</td><td>Will be intimated later</td></tr>
<tr><td>Consortium</td><td>Consortium is allowed, with a maximum of two bidders (Lead bidder + Consortium member). However, evaluation shall be based on the credentials of the Prime/Lead bidder. The Lead bidder should take full responsibility for execution of the work and must supply all IT-related equipment.</td></tr>
<tr><td>Bid validity</td><td>Bid must remain valid up to 180 (One Hundred & Eighty) days from the actual date of submission of bid.</td></tr>
<tr><td>Language of the proposal</td><td>This proposal should be filled in English language only. If any supporting documents are to be submitted, in any other language other than English, then translation of the same in English language, attested by the Bidder should be attached.</td></tr>
<tr><td>Proposal currency</td><td>Bidder shall be quoting prices in Indian Rupees (INR) and will receive payment is Indian Rupees only</td></tr>
<tr><td>Address for Correspondence and Clarifications</td><td>The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar 751013
Ph. - 0674-2567280 / 2567064 /2567295 / 2567283
Website: www.ocac.in</td></tr>
</table>

3.3. Acronyms

List of acronyms that have been used in this document has mentioned here along with its full form/meaning.

S. No	Abbreviations	Description / Definitions
1	AMC	Annual Maintenance Contract
2	ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
3	BCP	Business Continuity Plan
4	BOM	Bill of Material
5	BOQ	Bill of Quantity
6	BTA	Business Transaction Activity
7	CAPEX	Capital Expenditure
8	COTS	Commercial off the Shelf
9	Cr.	Crores
10	DC	Data Centre
11	DCMI	Data Centre Infrastructure Management
12	DD	Demand Draft
13	DG	Diesel Generator
14	DOT	Department of Telecom
15	DRC	Disaster Recovery Centre
16	DR cum DC / DR-DC	Proposed Disaster Recovery cum Data Centre
17	DRM	Disaster Recovery Management
18	EMD	Earnest Money Deposit
19	EMP	Exit Management Plan
20	EMS	Enterprise Management System
21	FAT	Final Acceptance Test
22	FRS	Functional Requirement Specification
23	FTP	File Transfer Protocol
24	G2B	Government to Business
25	G2C	Government to Citizens
26	G2G	Government to Government
27	GoO	Government Of Odisha
28	HLD	High Level Design
29	HOTO	Handover Takeover
30	HPC	High Performance Computing
31	IaaS	Infrastructure as a Service
32	ICT	Information and Communication Technology
33	IEEE	Institute of Electrical and Electronics Engineers
34	IOT	Internet over Things
35	IP	Internet Protocol
36	IPS	Intrusion Prevention System
37	IS	The Bureau of Indian Standards
38	ISO	International Organization for Standardization
39	ISP	Internet System Provider
40	IT	Information Technology
41	ITeS	Information Technology Enabled Services
42	ITIL	Information Technology Infrastructure Library
43	ITSM	IT Service Management
44	LAN	Local Area Network
45	LCS	Least Cost Selection
46	LLD	Low Level Design

S. No	Abbreviations	Description / Definitions
47	LUN	Logical Unit Number
48	MAF	Manufacturer Authorization Form
49	MeitY	Ministry of Electronics and Information Technology
50	MPLS	Multiprotocol Label Switching
51	MSA	Master Service Agreement
52	MTTR	Minimum Time to Recover
53	NBC	National Building Code
54	NDA	Non-Disclosure Agreement
55	NGFW	Next Generation Firewall
56	NMS	Network Management Server
57	NOC	Network Operations Centre
58	O&M	Operations and Maintenance
59	OCAC	Odisha Computer Application Centre
60	OEM	Original Equipment Manufacturer
61	OPEX	Operational Expenditure
62	OSDC	Odisha State Data Centre
63	OSDR	Odisha Stare Disaster Recovery Center
64	PaaS	Platform as a Service
65	PAT	Partial Acceptance Test
66	PBG	Performance Bank Guarantee
67	POE	Power over Ethernet
68	POI	Point of Interconnect
69	PSU	Public Sector Undertaking
70	QGR	Quarterly Gross Revenue
71	QOS	Quality of Services
72	RPO	Recovery Point Object
73	RTO	Recovery Time Object
74	SaaS	Software as a Service
75	SAN	Storage Area Network
76	SDC	State Data Centre
77	SDN	Software Define Network
78	SI	System Integrator
79	SIEM	Security Information and Event Management
80	SLA	Service Level Agreement
81	SOW	Scope of Work
82	SRS	System Requirement Specification
83	TCP	Transmission Control Protocol
84	TCV	Total Contract Value
85	TVC	Total Contract Value
86	UAT	User Acceptance Test
87	UPS	Uninterrupted Power Supply
88	WAN	Wide Area Network
89	XDR	Extended Detection and Response

4. Project Objective & Brief Scope of Work

4.1. About OCAC

The Odisha Computer Application Centre, also known as OCAC, serves as the designated technical directorate within the Electronics & Information Technology Department of the Government of Odisha. Over the years, OCAC has transformed into a Centre of excellence dedicated to the promotion and implementation of IT solutions and e-Governance initiatives. It stands as the primary gateway for any IT business opportunity in Odisha, actively encouraging investment from various players in the IT sector.

Engaged in the realms of Electronics, Computer goods, and IT services, OCAC addresses the technological requirements of the government. The directorate plays a pivotal role in the conceptualization and implementation of IT projects for various State Government Departments and agencies.

OCAC is steadfast in its commitment to generating IT business for both the public and private sectors, following a government mandate to foster IT development in the state. This encompasses opportunities spanning software development, hardware and peripherals supply, networking, connectivity, web applications, e-commerce, IT training, and a comprehensive range of direct and indirect IT businesses.

As the Designated Technical Directorate of the Electronics & Information Technology Department, OCAC has significantly contributed to the consistent growth of IT in the state. Its mission is to deliver superior value to beneficiaries through services and solutions, ensuring the reach of IT to the common citizen. By bridging the Digital Divide and promoting widespread IT applications, OCAC establishes a system wherein citizens receive good governance with prompt decision-making from a transparent government, facilitated by an effective e-Governance System.

4.2. Key Objectives of OCAC

1. Provide excellent electronic and IT goods and services to the Government of Odisha.
2. Create a robust IT eco-system to enhance the competitiveness and productivity of key economic sectors, positively impacting most of the state's population.
3. Disseminate IT and ITeS activities across the state, ensuring equitable benefits for the rural population.
4. Offer seamless and reliable citizen-centric services and information, thereby improving the efficiency, transparency, and accountability of the government.
5. Assist customers in adapting to modern management techniques.

4.3. Project Objective

The Disaster Recovery cum Data Centre (DR cum DC) shall be designed to meet specific OCAC’s requirements, influencing the physical design of the data centre. Its structure shall vary based on technologies, operating costs, and business needs. The overall objectives are provided below for reference:

- Provide a geographically diverse disaster recovery site to back up applications hosted at the OCAC DC at Bhubaneshwar.

- Ensure business continuity for e-Governance services in the event of outages, cyberattacks, or natural disasters.
- Build a Tier III compliant, scalable, and secure infrastructure that supports future digital growth and regulatory compliance.
- Disaster Recovery Centre cum Data Centre will be hosting 50% of workload of Data Centre.

4.4. Scope of Work

Bidders are required to conduct a site visit to the Keonjhar Disaster Recovery cum Data Centre (DR-DC) before submission of the bid at their own expense, to assess the requirements of both IT & Non-IT Infrastructure. Accordingly, bidder need to propose the IT and Non-IT architecture for Disaster Recovery cum Datacentre in accordance with industry best practices along with proper Bill of Quantities and overall solution design. Bidder shall submit complete solution, and no financial liability shall be borne by the OCAC for bidder's visit to proposed site nor for bidder's solution incompleteness.

The proposed DR cum DC is planned at 1st floor of Dharanidhar University, South Campus, Science Block, Keonjhar, Odisha. Site visit will be facilitated upon mail request to the Contact Officer, as mentioned in the Invitation of Bid section.

4.4.1. Disaster Recovery Centre

The primary goal of the DR-DC is to safeguard essential digital services and ensure their availability even in the face of disruptions. This entails the construction of a robust infrastructure capable of withstanding various threats, from power failures to cyberattacks. Furthermore, the centre must be equipped with state-of-the-art technology to facilitate swift data recovery and maintain continuity of operations.

The bidder shall undertake detailed assessment of the requirement of DR cum DC and NOC, IT and non-IT infrastructure including civil and electrical works as required.

OCAC shall carry out a detailed assessment of the proposed solution design and review the same for DR cum DC and NOC centre including all its components such as server room, operators seating arrangement, helpdesk facility, conference rooms, common areas, video-wall set-up, etc on the parameters of overall design, safety & security, aesthetics. OCAC reserves it's right to accept, reject or suggest for modifications on the proposed solution. The bidder shall also deploy services of a professional architect to prepare the interior design of the DR cum DC premises and carry out the required minimum civil, electrical, and furniture works.

The site preparation activity to be carried out by the successful bidder would include but not limited to necessary civil works for NOC centre interiors, realignment of available space based on requirement and architectural plan, necessary masonry, electrical, carpentry and other works, partitioning, flooring, false ceiling & false flooring as appropriately required, painting work, fire proofing of surfaces, cabling, ducting, etc. The bidder shall also undertake necessary civil, electrical, carpentry, partitioning work as

required for creation of cabins for supervisors, officials, conference rooms, cafeteria, reception area/visitors waiting area etc.

The bidder shall be responsible for the overall architectural design, aesthetic considerations, and optimal utilization of allotted space to ensure that the NOC Centre and DR cum DC locations are state-of-the-art facilities in line with the importance of the project. If any of the requirements are not mentioned in the RFP, bidder shall include the same as part of additional work to ensure that the requirements and expectations of the project are met.

The upkeep, maintenance, repairs, etc. of the non-IT infrastructure and items commissioned by the successful bidder as part of site preparation shall be the responsibility of the bidder for the entire duration of contract. At no point during the contract period, the facilities and infrastructure should be rendered unrepaired or damaged.

The bidders are advised to visit the site of DR cum DC and ascertain the scope of work and activities to be carried out at these locations for site preparation. All necessary costs involved in site preparation to be included in the financial proposal.

The overall Scope of Work (SoW) for the bidder is summarized below:

1. Design, supply, installation and setting up of the necessary Infrastructure at NOC Centre and DR cum DC in terms of minimum civil, interior, electrical and Air-Conditioning System for Disaster Recovery Centre, Fire Prevention, Detection and Suppression System, Lighting system, physical security infrastructure like access-control system, CCTV/ surveillance systems, etc.
2. The bidder shall take consultation and approval of OCAC for the interior layout. The bidder shall follow the specification of material to be used for these establishments.
3. The bidder shall complete site preparation, installation and commissioning of NOC Centre and DR cum DC as per the requirement in consultation with the OCAC.
4. The scope for minimum civil work is to furnish the NOC Centre, in all aspects. The furnishing includes but not limited to furniture & fixtures (tables, chairs, sofa, desk, etc.), cutting and chipping of existing floors, trench works, masonry works, hardware and metals, glazing, paint work, false flooring & ceiling (if required), storage space, portioning & partitioning, doors and locks wherever required, painting, fire proofing all surfaces, cement concrete works, insulation works etc., All material to be used shall be of fine quality as mentioned in the technical specification.
5. The bidder shall install the top false ceiling if required with 18” (typically) of space from the actual room ceiling. This false ceiling shall house A/C ducts (if required) and cables of electrical lighting, firefighting, and CCTV. Appropriate pest control measures shall be taken to keep pests at bay.
6. The bidder shall be responsible for raised flooring if required and provide for suitable pedestal and under structure designed to withstand various static and rolling loads subjected to it in server racks. The entire raised floor shall have suitable laminated floor covering and beadings on all sides of the panel.

7. The bidder must provide the Penta scanning report for Ethernet and OTDR for Fibre.
8. Design, supply, installation and setting up of all the IT components are mentioned in the RFP at NOC Centre and DR cum DC.

4.4.2. Replication

The bidder shall adequately do the sizing of DR and DC replication links and maintain them with (1+1) redundancy, to meet the RTO and the RPO requirements. (OCAC will provide the required link as per the sizing recommendation of the bidder). The bidder shall be responsible for timely DR-drills as per this tender document and as per OCAC requirements during the project contract period.

The bidder shall be responsible for providing/ facilitating replication tools/ software/processes for VMs, Servers, etc., for seamless replication from DC to DR and vice versa to meet RPO and RTO requirements. The bidder shall mention details of this tools/ software in their solution document. The bidder shall provide detailed operating manuals/ procedure documents for entire DR replication.

The bidder shall provide details of replication mechanism for (but not limited to) the following:

- Servers
- VMs
- LDAP/DNS/NTP etc.
- DC-DR Failover & Restoration - DR Drills/ Actual Disaster
- The responsibility of bidder includes but not limited to: -
    - Planning and Preparation
    - Scenario(use case) Development
    - Communication and Coordination
    - Simulation and Execution
    - Evaluation and Analysis
    - Remediation and Plan Updates

The bidder shall clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for complete switchover to DR in the BCP/ Procedure document. The bidder shall also define the access mechanism of all users to DR site during disaster/ drills in the solution document and BCP.

The failover from primary DC to DR cum DC should be done through a proper DR announcement process which should be documented as part of BCP planning. In the event of a disaster, setup at proposed DR cum DC site will become the primary DC.

Application data and application states must be replicated between DC & DR cum DC, so that when an outage occurs, failover to the surviving Data Recovery Centre can be accomplished within the specified RTO.

The bidder shall also provide a tool/mechanism for OCAC to trigger DR switch over and perform all necessary development and configuration of any additional scripts for successful working of DR cum DC. Bidder shall provide detailed DR activity plans which will contain steps/procedures to switch over services to DR site and vice-versa (DR to DC) in the event of disaster at DC site.

The bidder shall partner/coordinate with respective applications/product support vendors onsite to bring the applications up and running at DR site, support DR in event of disaster/drills or for performing periodic maintenance & upgrade activities.

The bidder shall conduct quarterly DR drills or as required, wherein the Primary DC must be deactivated, and complete operations shall be carried out from the DR Site. The pre-requisites of DR drill must be carried out by the bidder. The bidder must formulate and design the exact process of the DR drill, in consultation with OCAC and its application support team, in such a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process must be documented by the bidder as part of the disaster recovery plan (DRP). The bidder shall plan the activities to be carried out during the mock drill and issue a notice and a POA (Plan of Action) to the OCAC at least 15 working days before such drill. The bidder shall provide a detailed DR drill report, with RPO/ RTO achieved during the drill, after each planned drill activity.

4.4.3. Business Continuity Plan (BCP)

The bidder shall ensure following features with respect to DR site:

- The successful bidder shall define and submit (as part of the solution), a detailed approach for “Business Continuity Planning”. This should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which “disaster” would be declared.
- The bidder should have a practicing framework for business continuity planning and plan development which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.
- The bidder should practice Business continuity and security incident testing at planned intervals as defined by OCAC (Quarterly or as and when required) or upon significant organizational or environmental changes.

The brief of minimum list of activities to be carried out by the SI is provided below for reference:

A. Non-IT Infrastructure

i. NOC Operation area

NOC Centre will have 06 operators console with control desk, and officer’s cabin.

ii. Server room

This part of the DR-DC will host all active and passive component required in the solution like servers, server racks, storage racks, networking component (routers, switches, etc.) and Telecom terminals. The

approximate size of the server room shall be based on the space availability of the facility provided at Keonjhar. Access to this area where the surveillance project IT infrastructure is hosted should be demarcated, and physical access to the place would be restricted for unauthorized access. Only designated officials of Keonjhar and bidder's representative will have the access based on their role. Indoor Surveillance Cameras and Access Control System shall be installed to monitor and restrict the physical access of this area.

iii. Electrical and utilities room

This area shall accommodate all the Un-Interrupted Power Supply units, Grid Power Distribution Units (PDUs) to feed the components such as UPS, lighting, fixtures, Power Switch Gears, etc. This shall also accommodate all the batteries accompanying the UPS component. SI needs to carry out a detail assessment of the proposed solution design and review design documents for the DR-DC and NOC Centre on the parameters of overall design, Safety & Security.

iv. Disaster Recovery Centre Site preparation

The bidder shall complete site preparation, installation, and commissioning for the DR-DC site as per the requirement but not limited to the following.

v. **Civil and Architectural work.**

The scope for civil work in this RFP is to furnish the DR-DC in all aspects. The furnishing includes but is not limited to the following:

- Cutting and chipping of existing Floors
- Trench works
- Masonry works.
- Hardware and metals
- Glazing
- Paint Work
- Storage
- Raised Flooring
- False Ceiling
- Fireproof doors
- Fireproof Partitions
- Insulation
- Earthing
- Partition
- Other Cement Concrete Works

Note: All material to be used shall be of fine quality ISI marked unless otherwise specified

vi. Electrical Distribution System

The bidder shall be responsible for proper and uninterrupted working of DR-DC and shall ensure this by having the DR-DC power distribution system with redundancy with following:

- Arrangement of change over system two incoming HT grid feeder supply from different sub-stations. Even if one feeder is down, the other one keeps power available.

- Emergency Diesel Generator backup on failure of both main feeders, UPS system with battery bank for critical loads.
- Connection between UPS system and the network switch racks shall be redundant. No single point of failure shall exist in the power connectivity between network racks and UPS system.

vii. Electrical work for Disaster Recovery Centre

The electrical cabling work shall include the following:

- Main electrical panel in Disaster Recovery Centre
- Power cabling
- UPS distribution board
- UPS point wiring
- UPS system shall provide a redundant power supply to the following needs:
- Servers and important network and storage equipment
- Access control, Fire Detection & suppression system, and surveillance system
- Power cabling for utility component and utility points etc.
- Online UPS
- The bidder should use fire retardant cables of rated capacity exceeding the power requirements of existing and proposed components to be used at maximum capacity.
- All materials to conform to IS standards as per industry practice.
- The system shall be automatic switchover between primary power source (Grid power) and DG set as secondary source for the Disaster Recovery Centre.
- The bidder shall carryout all the Electrical work required for setting up all the DR-DC component of the system including:
- The bidder will be responsible for carrying out all the electrical work required for powering all the DR-DC components.
- Electrical installation and wiring shall conform to the electrical codes of India.
- The bidder shall arrange for alternate or redundant power supply in form of UPS, etc. in case the primary source of power fails for the DR-DC equipment.

viii. Earthing and Lightning Protection

- The bidder shall comply with the technical specifications, considering lightning proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power, and signal cable laying. bidder shall describe the planned lightning-proof and anti-interference measures in the bidding documents.
- Corresponding lightning arrester shall be erected at DR-DC site.
- All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to Low Voltage devices due to the surge suppression.
- Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the industry standards.

- Separate Earth pits for the components and for sensitive component or lightning protection, earth resistance < 1 ohm is preferred.
- The earthing cable shall be installed in a secure manner to prevent damage, and it shall be rust proof. The earthing down lead and the earthing electrode shall be galvanized, and the earthing value shall meet the requirements. Earthing test report shall be produced by the bidder.
- Two separate earth pits should be constructed and interconnected between them with a cupper strip and extended to the server components for Strong and redundant earthing. Earthing should be regular testing and maintenance. Separated earth pit is required for server / network rack, chassis, and UPS.

ix. Diesel Generator set.

The diesel generator set should be in N+1 redundancy mode. The bidder shall be responsible for regular operations and maintenance of the DG set.

The bidder shall be responsible for but not limited to:

- Fuel
- Preventive maintenance
- Corrective maintenance
- AMC
- Replacement of parts

x. Air Conditioning and Natural Convection

Since server room is a critical area, precision air conditioning system shall be exclusively installed to maintain the required temperature. The AC should be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow.

The task of the bidder shall include (but not limited to):

- Connecting the indoor unit with the mains electrical point Connecting indoor and outdoor units mechanically (with appropriate size of hard gauge copper piping)
- Connecting indoor and outdoor unit electrically
- The air conditioner should be linked to secondary power supply as well to prevent them from shutting down in case of power outage.

xi. Fire Detection and Suppression System

The DR-DC shall be equipped with adequate and advanced Fire Detection and Suppression system. The system should raise an alarm in the event of smoke detection. The system should have proper signage, response indicators and hooters in case of an emergency. The system should be based as per NFPA standards.

The DR-DC is to be equipped with gas based (Suitable for data Centre environments) fire suppression system appropriately sized for the given size of the DR-DC. Very Early Smoke Detection Apparatus (VESDA) system shall be installed in DR-DC to provide an early notification of fire incidents. The system shall include but not be limited to, a Control Panel with Display, Detector Assembly, and properly designed sampling pipe network.

xii. Access control system

The Biometric / Proximity card-based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble connected with BMS system. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.

xiii. Indoor surveillance system

Indoor surveillance system shall be installed within the DR-DC and NOC Centre on 24X7 bases. All important areas of the DR-DC, NOC Centre along with the non-critical areas like site for DG sets, entry and exit of NOC Centre, Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations.

xiv. Water leak detection system

The Water Leak Detection System shall be installed to detect any seepage of water into the critical area and alert the security control room for such leakage. It shall consist of water leak detection cable and alarm module. The cable shall be installed in the ceiling and floor areas around the periphery of the DR-DC.

xv. Building Management system

The Building Management System (BMS) shall be implemented for effective management, monitoring, and integration of various components like Access Control System, VESDA, fire detection system etc.
The BMS shall perform the following general functions including but not limited to:

- Building Management and control
- Data collection and archival
- Alarm event and management.
- Trending
- Reports and MIS generation
- Maintenance and complaint management

The scope shall include designing, supplying and installation of Building Management System.

xvi. Rodent Repellent

The entry of rodents and other unwanted pests shall be controlled using non-chemical, nontoxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However, the bidder shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

xvii. UPS installation

- The UPS shall serve as a backup for commercially available utility power at the intersections and shall ensure no-break functioning of all DR-DC components at each intersection in event of failure of utility power supply.
- The bidder shall install UPS at the defined intersections in secure, tamper-proof housing in corrosion resistant cabinets.

- The bidder shall ensure that the UPS is suitably protected against storms, power surges and lightning.
- The bidder shall supply and install the UPS for efficient heat dissipation without air conditioning. It should be able to withstand temperatures prevalent in outdoor condition throughout the year.

xviii. Temperature and Humidity Control:

All enclosure compartments shall be equipped with a natural convection air circulation system featuring maintenance-free air circulation filters that allow for the free movement of air within the enclosures. This system is essential for preventing overheating and mitigating the effects of humidity and heat, while simultaneously restricting the entry of elements that could compromise system operation. The bidder shall ensure that all hardware placed inside the outdoor enclosures can withstand the year-round outdoor temperatures. Add up the calculation of BTU/hr for all active components based on the initializing load and 10–20% extra capacity for future expansion and redundancy.

i. Maintain server room temperature between 18°C to 22°C.
ii. Standard humidity level should be maintained between 50- 60% for a server room.
iii. Use humidifiers/dehumidifiers integrated with HVAC systems and monitoring continuously.

B. IT Infrastructure

i. **Compute Infrastructure:**

- Supply, installation, configuration, testing, and commissioning of compute infrastructure, including hardware and software components such as Servers, Operating Systems, and cloud orchestration and virtualization management.

ii. Network Infrastructure:

- Supply, installation, configuration, testing, and commissioning of Network infrastructure, comprising Spine switch, Leaf switch and management switch.
- Deployment of Server Load Balancer, Link Load balancer and other components are per the RFP requirement.

iii. Storage Area Network (SAN):

- Supply, installation, configuration, testing, and commissioning of Storage Area Network with Storage system, SAN switches, etc.

iv. Security Infrastructure:

- Supply, installation, configuration, testing, and commissioning of Security infrastructure, including D-DOS protection, Next Generation Firewalls, SLB, WAF Solution.
- Create different Pods, as required by OSDR Team.

v. Centralized Cloud Environment:

- Establishment of a centralized cloud environment capable of hosting multiple applications
- Simplification of operations and enhancement of application responsiveness to support the next generation of distributed applications.
- Unified management of performance, capacity, and compliance of cloud infrastructure.
- On-premises service implementation for the Orchestration layer.

4.4.4. Onsite Support for DR-DC Operations:

Onsite support for Data Centre Operations on a 24x7x365 basis by qualified and trained engineers/professionals for a five-year period to ensure more than 99.982% service availability.

4.4.5. Maintenance and Provisioning of Services:

- Five years on-site comprehensive maintenance and provisioning of services for all ICT infrastructure components.
- Provision of onsite spares on a 24x7x365 basis after successful execution and acceptance by OCAC.

5. Submission of Proposal

5.1. Submission of the Proposal Instruction to Bidders for Online Bid Submission

eNivida is a Comprehensive end-to-end Unified eProcurement & eAuction system for procuring and selling of goods/services. The instructions given below are meant to assist the bidders in registering on e-Nivida Portal and submitting their bid online on the portal. More information useful for submitting online bids on the e-Nivida Portal may be obtained at: https://enivida.odisha.gov.in.

5.2. Guidelines for Registration

Bidders are required to enrol themselves on the eNivida Portal **https://enivida.odisha.gov.in** or click on the link **"Bidder Enrolment"** available on the home page by paying Registration Fees of Rs 2500/- with applicable GST. As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

a. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication with the bidders.
b. Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify/ TCS / nCode/ eMudhra etc.), with their profile.
c. Only valid DSC should be registered by a bidder. Please note that the bidders are responsible for ensuring that they do not lend their DSCs to others, which may lead to misuse.
d. Bidder then logs in to the site through the secured log-in by entering their user ID /password and the password of the DSC / e-Token.
e. The scanned copies of all original documents should be uploaded in pdf format on e-Tender portal.
f. After completion of registration payment, bidders need to send their acknowledgement copy on our help desk mail id odishaenivida@gmail.com for activation of the account.

5.2.1. Searching for Tender Documents

There is various search options built in the e-Tender Portal, to facilitate bidders to search for active Tenders by several parameters.

Once the bidders have selected the Tenders they are interested in, then they can pay the Tender fee and processing fee (NOT REFUNDABLE) by net-banking / Debit / Credit card then you may download the required documents / Tender schedules, Bid documents etc. Once you pay both fees, Tenders will

be moved to the respective 'requested' Tab. This would enable the e- Tender Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the Tender document.

5.2.2. Preparation of Bids

Bidder should consider any corrigendum published on the Tender document before submitting their bids. Please go through the Tender advertisement and the Tender document carefully to understand the documents required to be submitted as part of the bid.

Bidder, in advance, should get ready the bid documents to be submitted as indicated in the Tender document / schedule and generally, they can be in PDF formats. Bid Original documents may be scanned with 100 dpi with Colour option which helps in reducing size of the scanned document.

To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, GST, Annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Documents" available to them to upload such documents.

These documents may be directly submitted from the "My Documents" area while submitting a bid and need not be uploaded again and again. This will lead to a reduction in the time required for bid.

5.2.3. Submission of Bids

a. Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.

b. The bidder must digitally sign and upload the required bid documents one by one as indicated in the Tender document as a token of acceptance of the terms and conditions laid down by the Department.

c. The bidder must select the payment option as per the Tender document to pay the Tender fee / Tender Processing fee & EMD as applicable and enter details of the instrument.

d. In the case of BG bidders should prepare the BG as per the instructions specified in the Tender document. The BG in original should be posted/couriered/given in person to the concerned official before the Online Opening of Financial Bid. In case of non-receipt of BG amount in original by the said time, the uploaded bid will be summarily rejected.

e. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOM format with the Tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOM file, open it and complete the yellow Coloured (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOM file is found to be modified by the bidder, the bid will be rejected.

f. The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this during bid submission.

g. The uploaded bid documents become readable only after the Tender opening by the authorized bid openers.

h. Upon the successful and timely submission of bid click “Complete” (i.e. after Clicking “Submit” in the portal), the portal will give a successful Tender submission acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.

i. The Tender summary must be printed and kept as an acknowledgement of the submission of the Tender. This acknowledgement may be used as an entry pass for any bid opening meetings.

5.2.4. Clarifications on using e-Nivida Portal

a. Any queries relating to the Tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a Tender or the relevant contact person indicated in the Tender.

b. Any queries relating to the process of online bid submission or queries relating to e-Tender Portal in general may be directed to Helpdesk Support. Please feel free to contact Helpdesk (as given below) for any query related to e-Tendering. Phone No.: 011-49606060, Mail id: odishaenivida@gmail.com

5.3. Late Proposals

Any proposal received by OCAC after the deadline for submission, as specified by OCAC, shall be rejected.

5.4. Proposal Prices

a The prices outlined in the price schedule should be listed as follows:

   i. The total quoted price must encompass the cost of IT and Non-IT components supply, installation, commissioning, and provision of hardware, licenses, software, testing, and commissioning of the Solution, as well as support. It should also include all applicable taxes, duties, levies, charges, and additional costs for incidental services such as transportation, insurance, training, factory acceptance tests, acceptance tests at the site, certification, periodic health checks, operation, and maintenance, etc.

   ii. The cost of operation and maintenance of IT systems for a period of FIVE (5) years after the date of Go Live.

   iii. Manpower support cost for period of FIVE (5) Years after the date of Go-Live

b The Bidder is not permitted to quote for the project in parts.

c Before bidding, the Bidder must conduct a site visit of the proposed sites/locations, at Keonjhar, to assess the actual physical and technical requirements. Site visit will be facilitated upon mail request to the Contact Officer, as mentioned in the Invitation of Bid section.

d The bidder must submit a detailed Bill of Material, including Make & Model, and Bill of Quantity for each component.

e OCAC reserves the discretion to increase or decrease the quantity and items if the need arises.

5.5. Earnest Money Deposit

Bidders are required to submit an Earnest Money Deposit (EMD) of Rs. 4,00,00,000.00 (Rupees Four Crore), in the form of a bank guarantee issued by any nationalized/scheduled commercial bank in favour of OCAC. The EMD format is provided in Annexure 4 (EMD forwarding letter format) and Annexure 5.

a The bank guarantee should be payable at Bhubaneswar and valid for a minimum period of 180 days from the last date of the submission of the Bid.

b OCAC will refund the EMD of all unsuccessful bidders within 60 days after the selection of the successful Bidder. The EMD of the successful Bidder will be returned upon the submission of the Performance Bid Security.

c The EMD amount is interest-free and will be refunded to the unsuccessful bidders without any accrued interest. The proposal submitted without tender fee and EMD in the prescribed format mentioned above, shall be summarily rejected.

d The EMD may be forfeited:

i. If a Bidder withdraws its proposal within the validity period.

ii. In case of a successful Bidder, if the Bidder fails to sign the contract in accordance with this RFP as per the mutually agreed terms.

iii. Fails to deliver as per the Terms & conditions of RFP & deliverables.

iv. Any material breach of contract.

e The fee can also be paid through electronic mode to the following bank account

Bank A/c No.	149311100000195
Payee Name	OCAC Training
Bank Name & Branch	Union Bank of India, Acharya Vihar, Bhubaneswar
Account Type:	Current
IFSC	UBIN0814938

5.6. Performance Bank Guarantee

a An unconditional and irrevocable Bank Guarantee equivalent to 10% of the total cost of project (without GST) from any nationalized / scheduled commercial bank in the prescribed format (in annexure 17) in Favor of the Odisha Computer Application Centre shall be submitted by the successful bidder within 15 days of issue of Purchase Order.

b Failure of submission of PBG within the specified time may lead to cancelling the Purchase Order.

c The Bank guarantee shall be valid till 5 years and 9 Months (69 Months) beyond completion of all installation of the necessary Hardware/components/Licenses at OCAC.

d In the event of the bidder being unable to provide services and other terms and conditions of the PO/RFP for whatever reason, OCAC would revoke the PBG. OCAC shall notify the Bidder in writing of the exercise of its right to receive such compensation within 15 days, indicating the contractual obligation(s) for which the Bidder is in default.

5.7. Bid Validity Period

a The Earnest Money Deposit (EMD) submitted with the bid will remain valid for the entire duration specified in the fact sheet.

b In exceptional circumstances, OCAC may, prior to the expiration of the bid validity period, request bidders to extend the validity for a specified additional period at the bidder's cost. Both the request and the responses to it shall be communicated in writing. While a bidder has the option to refuse the request without risking forfeiture of the EMD, doing so will disqualify the bidder from further consideration for the award. Bidders agreeing to the extension request will not be permitted to modify their bids but are required to ensure that the bid remains secured for the extended period.

c Upon the completion of the validity period, unless the bidder formally withdraws the bid in writing, the bid will be considered valid until such time that the bidder officially communicates (in writing) the withdrawal of the bid.

5.8. Compliance and Completeness of Response

a Bidders are strongly advised to meticulously review and assess all instructions, forms, appendices, terms, conditions, and deliverables outlined in the RFP document. Failure to provide all the required information as stipulated in the RFP documents or submitting an offer that is not substantially responsive in every aspect to the RFP documents will be at the bidder's own risk and may lead to the rejection of their RFP offer.

b The RFP offer may be outrightly rejected without prior notice to the bidder if the complete information, as specified in the RFP document, is not provided, or if the particulars requested in the forms/Proforma in the RFP are not fully furnished.

c Bidders are required to:

i. Include all documentation specified in this RFP in their bid.
ii. Adhere to the format of this RFP while developing the bid and respond to each element in the order as set out in this RFP.
iii. Comply with all the requirements outlined within this RFP.

5.9. Clarification on RFP and response to pre-bid queries

Bidders may raise clarifications on this RFP, and all such queries/clarifications should reach OCAC through the following email **tenders.ocac@odisha.gov.in**, with a copy to **gm_ocac@ocac.in** on or before the date mentioned in the fact sheet. OCAC may or may not incorporate any changes in the RFP based on acceptable suggestions received. The decision of OCAC regarding acceptability of any suggestion/request shall be final in this regard and shall not be called upon to question under any circumstances. The prospective bidders shall submit their queries through mail only in prescribed format (Ms-Excel) below not later than date and time indicated above.

Name of the Sl -						
Name of the Contact Person with Designation, email ID & Mobile Number -						
Sl. No	**Page No**	**Clause No**	**Clause header**	**Clause details as in RFP**	**Query/ Clarification Required**	**Justification / Reason for changes required (If any)**
1.						
2.						

At any time prior to the last date of submission of proposal, OCAC may for any reason be able to modify the RFP.

Any modifications in RFP or reply to queries shall be hosted – **www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in/**

a. Queries received, after due date, will not be entertained.
b. Queries should be given in MS-Excel only. Queries received beyond the given format will not be accepted.
c. At any time prior to the last date for receipt of bids, OCAC may, for any reason, modify the RFP Document by a corrigendum.
d. The Corrigendum (if any) & clarifications to the queries from all bidders will be posted on the websites www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in /
e. Any such corrigendum shall be deemed to be incorporated into this RFP
f. OCAC at its discretion may extend the last date for the receipt of proposals.
g. Once the queries are answered, any further similar queries will not be entertained further.
h. It is expected that the bidder shall do their own due diligence on the queries / question they may ask. Any changes sought must be with proper justification. Any statement such as ‘specification/requirement is not vendor neutral’ OR ‘it implies to single OEM’ or any such statement like this, must be asked with adequate and credible proof and justification, else such queries will not be accepted.

5.10. Amendment of Proposals

RFP Proposals, once submitted, are non-amendable. However, in the event of administrative exigencies, OCAC may choose to solicit fresh proposals from all bidders before the opening of the Technical Proposal.

OCAC, at its discretion, reserves the right to request clarifications in the form of letters, declarations, datasheets, brochures, etc., during the technical evaluation. It is mandatory for bidders to promptly submit the requested documents as part of the evaluation process.

5.11. Opening of Proposals by OCAC

The date and time for the opening of proposals and the technical presentation will be determined and communicated by OCAC through the official website www.ocac.in /official mail IDs of the bidders. The evaluation committee, duly authorized by OCAC, will conduct the proposal opening in the presence of bidders or their representatives who may choose to attend. The bidder's representatives (limited to a maximum of two) must carry identification cards or a letter of authorization from the bidding firms to

establish their credentials for attending the proposal opening.

To facilitate the examination, evaluation, and comparison of proposals, OCAC may, at its discretion, seek clarifications from the bidder regarding its proposal. Any such clarifications shall be provided in writing, and no modifications to the price or substance of the proposal will be entertained, sought, or permitted.

5.12. Evaluation Procedure

a OCAC reserves the right to form an Evaluation Committee for scrutinizing bidder responses.

b The Evaluation Committee, appointed by OCAC, will thoroughly assess RFP responses and accompanying documents. Failure to submit essential supporting documentation may result in rejection.

c Decisions and interpretations made by the Evaluation Committee during the bid evaluation process are deemed final. Correspondence outside the evaluation process will not be entertained.

d The Evaluation Committee may arrange meetings with bidders to seek clarifications on their submissions.

e OCAC holds the authority to reject bids based on any identified deviations.

f Each response will be evaluated according to the criteria outlined in the RFP.

g During the initial scrutiny, incomplete details will render bids non-responsive. Non-compliance with tender fee, EMD format, improper submission, absence of the Letter of Authorization / Power of Attorney, suppression of details, incomplete information, subjective or conditional offers, and deviations from the RFP clauses will lead to disqualification.

h A list of responsive bidders, adhering to all RFP terms, will be compiled by the Evaluation Committee. These eligible bids will undergo further evaluation.

i. The Evaluation Committee will assess the completeness of bids, identify computational errors, and verify overall orderliness.

ii. Detailed Bill of Quantity (BOQ) and Bill of Material (BOM) must be submitted as an unpriced bid in the technical proposal.

iii. Clarification meetings may be conducted, and results will be published on the specified website.

iv. The Evaluation Committee's responsibilities extend to decisions related to the RFP Document and project execution.

v. The proposal opening will occur in the presence of bidder representatives who must sign a register as evidence of attendance.

vi. The proposal will undergo the following evaluation:

- Pre-Qualification Evaluation: Bidders will be evaluated as per the pre-qualification criteria mentioned in this RFP. Bidders who qualify the pre-qualification criteria will be considered for technical evaluation.

- Technical Evaluation: Bidders will be evaluated as per the technical evaluation criteria mentioned in the RFP. The bidders who qualify the technical evaluation criteria will be called for presentation.
- The bidders who score 70 or more marks in the technical evaluation will be considered for financial bid opening. Financial bids of the bidders who have scored 70 or more marks in technical evaluation will be opened and evaluated as per clause 6.2.

6. Evaluation Criteria

6.1. Pre-Qualification Criteria

The bidder must meet the mandatory pre-qualification requirements as outlined in the following table.

Only those bidders who fulfil all the mandatory pre-qualification criteria shall be considered for technical evaluation. Proposals submitted by bidders who do not meet any of the pre-qualification criteria shall be rejected.

The bidder to furnish Power of Attorney / Board Resolution, and all the undertaking as per the annexure, without these documents the bid may be rejected.

In case of consortium, consortium agreement on non-judicial stamp paper (Rs 100) along with power of attorney to the lead bidder should also be furnished.

Sl.	Parameter	Specific Requirements	Documents to be furnished
1.	Legal entity	Responding Firm/ Company should be: ▪ Registered as a Company/LLP under Companies Act, 1956/2013 OR Partnerships Firm registered under LLP Act, 2008. ▪ Have been operating for at least last 10 (Ten) financial years as on date of bid submission date. ▪ Registered with Goods and Services Tax Network (GSTN).	▪ Copy of Certificate of Incorporation/ Registration ▪ Copy of the work order/completion certificate as documentary proof of operation of 10 years ▪ Copy of GST Registration certificate.
2.	Financial: Turnover	Average annual turnover of the bidder during the last three financial years, as per the last published audited balance sheets, should be at least INR 300 Crores from System Integration business in the three (3) financial years: FY 2022–2023, FY 2023–2024, and FY 2024–2025. In case of consortium, lead bidder must satisfy this clause.	CA Certificate for turnover along with copy of audited balance sheets with CA's Registration No and seal.
3.	Financial: Net worth	The average net worth of the Bidder should be Positive for last three years: FY 2022-2023, 2023-2024, 2024-2025. In case of consortium, lead bidder must satisfy this clause.	• CA Certificate for Net Worth with CA's Registration No and Seal. • Copy of audited profit and loss account/ balance sheets of the last three financial years, highlights the requisite figure related to positive net worth profitability.

Sl.	Parameter	Specific Requirements	Documents to be furnished
4.	Project Execution Strength	The bidder must have experience in executing System Integration Projects for any Government Department / Government Agency / PSU/ Autonomous Body in India during last ten (10) years as on the bid submission date, with project values as specified below: ▪ One (1) project not less than ₹110 Cr. OR ▪ Two (2) projects not less than ₹80 Cr each OR ▪ Three (3 projects not less than ₹55 Cr each (Orders executed in collaboration with consortium partners will also be considered. In such cases, the bidder must provide documentary evidence specifying the value of the work executed by them). In the case of a consortium, the experience of the Lead Bidder shall be considered for compliance with this clause.	Copy of work orders with client certification/FAT along with project citation as per the format enclosed in Annexure 23
5.	Datacentre Project experience	Bidder should have experience of supply, installation, and commission of Datacentre IT equipment (i.e. supply, installation and commissioning of IT equipment such as servers, Network devices, storage, and system software) for any Government Department / Government Agency / PSU/ Autonomous Body in India in last Ten (10) Years ending 31-10-2025 with minimum order value of ₹ 55 Crore. In the case of a consortium, the experience of the Lead Bidder shall be considered for compliance with this clause.	Copy of work order or MSA along with documentary evidence of FAT/Ongoing/ Go Live along with project citation as per the format enclosed in Annexure 23

Sl.	Parameter	Specific Requirements	Documents to be furnished
6.	Technical Manpower Strength	The Bidder should have technically qualified workforce of at least 100 having minimum qualification of B.E/B. Tech/MCA/MSC(IT)/MBA or higher as date of bid submission. The workforce should have the following certification. • CDCP / CDCMP / equivalent • ITIL or equivalent • CCNA / CCNP / JNCA / JNCP or equivalent • CISSP / CISM / CEH or equivalent • CISA / ISO/IEC 27001 or equivalent • AWS / Azure / Google Cloud or equivalent • OS Certification (RHCE / MCSE / OCP or equivalent) • Database Certification (Oracle / Microsoft / IBM / PostgreSQL /MySQL or equivalent • Storage Certification (Dell EMC / NetApp / IBM HPE / Hitachi or equivalent) The bidder shall ensure that its organization collectively possesses resources certified in all the above categories. A single resource may hold one or more certifications; however, the absence of certification in any category shall render the bidder non-compliant and disqualified (All the certifications should be from any Government institutions/ OEM/accreditation partners of EC-Council/PECB/ITIL) In the case of a consortium, the experience of the Lead Bidder shall be considered for compliance with this clause.	Certificate from HR/ Director Head (in Company letter head) showing the details of resources with qualification and certification as per the format enclosed in Annexure 21
7.	Certifications	Bidder must have the following certifications at the time of bidding: a) ISO 9001:2015 or latest. b) ISO/IEC 20000:2018 or latest. c) ISO/IEC 27001:2015 or latest. In the case of a consortium, the experience of the Lead Bidder shall be considered for compliance with this clause.	Copy of valid certificates during the bid validity period.
8.	Mandatory undertaking	The bidder shall: a) Not be insolvent, bankrupt, or being wound up, not have its affairs administrated by a court or judicial officer, not have its business activities suspended and must not be the	Self-certification/Declaration duly signed by authorized signatory on company letter head.

Sl.	Parameter	Specific Requirements	Documents to be furnished
		subject of legal proceedings for any of the foregoing reasons. b) They, including their directors and officers, have not been convicted of any criminal offence related to their professional conduct or for making false statements or misrepresentations regarding their qualifications to enter into a procurement contract within the five years preceding the commencement of the procurement process, nor have they been otherwise disqualified through debarment proceedings. In the case of a consortium, both the Lead Bidder and the Consortium Member shall provide the mandatory undertaking.	
9.	Acceptance of Scope of Work	a) Bidder should accept the entire scope of work (including services) as mentioned in the Scope of work. b) Bidder must quote all the products/equipment mentioned in the Bill of Materials. Otherwise, the bid will not be considered.	As per format eclosed in the Annexure 2, 8 and 20
10.	Local presence	The bidder should have an office in Odisha. However, if the presence is not there in the state, the bidder should give an undertaking for the establishment of an office, within one month of the award of the contract.	Self-certification with office location addresses to be submitted OR declaration for establishment of an office in case LoI has been awarded. The document should be on the bidder's letterhead signed by the authorized signatory.
11.	EMD	Rs 4,00,00,000.00 (Rupees Four Crore only)	In the form of DD/BG issued by any nationalized/scheduled bank having branch in Bhubaneswar in favour of OCAC payable at Bhubaneswar and with validity for 6 months from the date of submission of bid. (In case of DD validity will be for 3 months)
12.	Blacklisting	The Bidder should not be under a declaration of ineligibility for corrupt or fraudulent practices on the date of bid submission by any State Government, Central Government, Central Public Sector Undertaking (PSU), or autonomous body in India	Self-declaration as per the format enclosed in the Annexure 7
13	Integrity Pact	Bidder must submit integrity pact in ₹100 stamp paper	As per the format enclosed in the Annexure 22

6.2. Technical Bid Evaluation Scoring Matrix

6.2.1. Mandatory Technical Compliance

The bidder must furnish tender specific Manufactures Authorization Form (MAF) for items mentioned at Section 13.9 Annexure- 9. The technical compliance of the specifications must be submitted in respective OEM letter head supported by product literature and data sheet with cross-compliance. Without MAF and technical compliance sheet the bid will be rejected

6.2.2. Technical Evaluation Criteria

The bid will be evaluated based on the following criteria:

Sl.	Description	Max. Score	Scoring Mechanism	Documents to be furnished
1.	Average Annual Turnover of the Bidder from System Integration Business in last three (3) financial years: FY 2022-2023, 2023-2024, 2024-2025. In case of consortium, only the average annual turnover of the lead bidder shall be considered for evaluation of this clause.	10	• ₹300 Crore - 5 marks • Additional 1 Mark for each additional ₹50 Cr subject to maximum to 10 marks.	CA Certificate for Turnover along with copy of audited balance sheets with CA's Registration No and Seal.
2	The bidder must have experience of System Integration Project for any Government Department / Government Agency / PSU/ Autonomous Body in India during last 10 years as on bid submission date. In the case of a consortium, the experience of both the Lead Bidder and the Consortium Member shall be considered for evaluation for this clause.	10	• Each Projects of order value more than ₹110 Cr – 5 Marks • Each Project of order value between ₹80 Cr to ₹110 Cr – 3 marks each • Each Project of order value between ₹55 Cr to ₹80 Cr – 2.5 marks each (Projects that have been assessed under one technical evaluation criterion shall not be reconsidered or evaluated again under any other technical evaluation criterion.) Maximum Marks capped at 10 Marks.	Copy of work order or MSA along with documentary evidence of FAT/Ongoing/ Go Live along with project Citation as per enclosed format in Annexure 23
3.	Bidder should have experience of supply, installation, and commission of Datacentre IT equipment (i.e. supply, installation and commissioning of IT equipment such as servers, Network devices, storage, Security Devices, and system software) for any Government Department / Government Agency	20	Datacentre IT Experience • Each Projects of order value of more than ₹55 Cr – 5 Marks Maximum Marks capped at 15 Marks for the above clause.	Copy of work order or MSA along with documentary evidence of FAT/Ongoing/ Go Live along with project Citation as per the format eclosed in the Annexure 23

Sl.	Description	Max. Score	Scoring Mechanism	Documents to be furnished
	/ PSU/ Autonomous Body in India in last Ten (10) Years ending 31-10-2025. In the case of a consortium, the experience of both the Lead Bidder and the Consortium Member shall be considered for evaluation for this clause.		and Additional 5 Marks for one project that includes Datacentre Non-IT experience (Projects that have been assessed under one technical evaluation criterion shall not be reconsidered or evaluated again under any other technical evaluation criterion.)	
6.	Project Team. In the case of a consortium, the resources of both the Lead Bidder and the Consortium Member shall be considered for evaluation for this clause.	30	• **Please Refer Appendix-I**	-
7.	Technical Proposal and Presentation	30	• Understanding of Scope and Objectives-**3 Marks** • Solution Architecture and Design-**10 Marks** • Implementation Approach-**5 Marks** • Operations, Maintenance, and SLA Management Plan-**3 Marks** • Security, Compliance, and Data Protection Strategy-**3 Marks** • Innovation and Value Addition-**2 Marks** • Project Governance, Risk Management, and Quality Control-**2 Marks** • Integration with Existing OCAC Infrastructure (OSDC Bhubaneswar)-**2 Marks**	Bidder to mention clearly in Technical Proposal and Presentation

Note:

1) Financial bids of those bidders who achieve technical score of **70** or more marks will be opened.
2) Manufactures Authorization Form (MAF) is mandatory, and the bidder should furnish MAF for all components as mentioned in the respective Annexure. If the bidder fails to furnish the MAF, their bid will not be considered for evaluation. The MAF format is enclosed in Annexure 9.

The OEM support undertaking and technical specification compliance format are enclosed in Annexure 10 and 11. The format for warranty certificate and no deviation are enclosed in Annexure 13 and 14. The bidders should ensure these details are provided, as per the format in their bid. Without these documents the bid may be rejected

Appendix -I

Project Team Composition and Scoring (30 Marks)

Sl. No.	Role	Minimum Qualifications Required	Max. Marks	Scoring Mechanism	Supporting Documents Required
1	**Project Manager**	• B.E. / B.Tech. / MCA / MSc (IT) with at least **10 years** of experience in IT infrastructure / datacentre implementation projects. • PMP / PRINCE2 / ITIL v4 Foundation certified	5	• B.E. / B.Tech. / MCA / MSc (IT) – 2 marks • MBA - 1 Marks • PMP / PRINCE2 / ITIL v4 Foundation – 1 Marks • Any Datacentre certification - 1 Marks Max. marks - 5	CV as per Annexure 18 along with, Degree Certificate, PMP/PRINCE2/ ITIL and other certificate copy.
2	**Storage Administrator**	• B.E. / B.Tech. / MCA/ MSc (IT) with **5+ years** of experience in enterprise storage management. • SNIA SCSP / SCSE / OEM (NetApp / Dell EMC / HPE / IBM / Pure) Certified.	4	• B.E. / B.Tech. / MCA / MSc (IT) – 0.5 marks • Work Experience 5 to 8 Years - 0.5 Marks • Work Experience of more than 8 years – 0.5 Marks • Certification - 0.5 Marks 2 Resources to be proposed. Max 2 marks per resource.	CV as per annexure 18 along with Certification copies.

Sl. No.	Role	Minimum Qualifications Required	Max. Marks	Scoring Mechanism	Supporting Documents Required
3	**Network Administrator**	• Diploma / B.E. / B.Tech./ MSc (IT) with **5+ years** of experience in network configuration, routing, and switching. • CCNA / CCNP / JNCIA / JNCP Certified	4	• B.E. / B.Tech. / MCA / MSc (IT) – 0.5 marks • Work Experience 5 to 8 Years - 0.5 Marks • Work Experience of more than 8 years – 0.5 Marks • Certification - 0.5 Marks 2 Resources to be proposed. Max 2 marks per resource.	CV as per annexure 18 along with Certification copies.
4	**Cloud Administrator**	• B.E. / B.Tech. / MCA / MSc (IT) with **4+ years**' experience in cloud infrastructure • AWS / Azure / Google Cloud. Associate or Professional Certification	4	• B.E. / B.Tech. / MCA / MSc (IT) – 0.5 marks • Work Experience 4 to 7 Years - 0.5 Marks • Work Experience of more than 7 years – 0.5 Marks • Certification - 0.5 Marks 2 Resources to be proposed. Max 2 marks per resource.	CV as per annexure 18 along with Certification copies.

Sl. No.	Role	Minimum Qualifications Required	Max. Marks	Scoring Mechanism	Supporting Documents Required
5	**Security Administrator**	• B.E. / B.Tech. / MCA / MSc (IT) with **5+ years** of experience in network & datacentre security. • CISSP / CISM / CEH / ISO 27001 Lead Implementer	2	• B.E. / B.Tech. / MCA / MSc (IT) – 0.5 marks • Work Experience 5 to 8 Years - 0.5 Marks • Work Experience of more than 8 years – 0.5 Marks • Certification - 0.5 Marks	CV as per annexure 18 along with Certification copies.
6	**Database Administrator**	• B.E. / B.Tech. / MCA/ MSc (IT) with **5+ years** of experience in database setup and maintenance. • Oracle Certified Professional (OCP) / Microsoft SQL Server Certified / PostgreSQL Certified	2	• B.E. / B.Tech. / MCA / MSc (IT) – 0.5 marks • Work Experience 4 to 7 Years - 0.5 Marks • Work Experience of more than 7 years – 0.5 Marks • Certification - 0.5 Marks	CV as per annexure 18 along with Certification copies.
7	**System Administrator**	• B.E. / B.Tech. / MCA/ MSc (IT) with **5+ years**' experience in server and OS management • RHCE / MCSE / OCP / VCP	4	• B.E. / B.Tech. / MCA / MSc (IT) – 0.5 marks • Work Experience 4 to 7 Years - 0.5 Marks	CV as per annexure 18 along with Certification copies.

Sl. No.	Role	Minimum Qualifications Required	Max. Marks	Scoring Mechanism	Supporting Documents Required
				• Work Experience of more than 7 years – 0.5 Marks • Certification - 0.5 Marks 2 Resources to be proposed. Max 2 marks per resource.	
8	**Helpdesk Support**	• B.E. / B.Tech. / Diploma with **3+ years**' experience in server and OS management	2	• B.E. / B.Tech. / Diploma - .5 Marks • Work Experience of - 0.5 Marks 2 Resources to be proposed. Max 1 marks per resource.	CV as per annexure 18
9	**Data Centre Facility Engineer**	• B.E. / B.Tech / Diploma (Electrical/Mechanical) with **5+ years**' experience in data centre facility operations. • BICSI DCDC / CDCMP / CDCP / Equivalent	3	• B.E. / B.Tech. / Diploma - .5 Marks • Certification - .5 Mark 3 Resources to be proposed. Max 1 marks per resource.	CV as per annexure 18 along with Certification copies.

- **Only full-time employees** of the bidder (on payroll) will be considered.
- **CVs and certificates** must be submitted for verification.

Note:

i. This information is for the vendor's internal reference and need not be submitted with the bid.

ii. Vendors must furnish relevant credentials for each of the above points for scoring.

iii. OCAC retains the right to verify the accuracy of documentary evidence provided by the bidder concerning the successful operation and performance

of qualifying projects, and the bidder is responsible for obtaining the necessary permissions for verification.

iv. The solution demonstrated will be evaluated using a pre-set questionnaire.

v. The vendor must provide supporting documentation such as product technical architecture, describing various technical parameters.

vi. The overall proposal, implementation methodology, and adherence to the project plan will be assessed.

vii. Bidder's experience in building their own in-house Data Centre or captive Data Centre for commercial use will not be considered.

viii. The Product offered should meet all the technical and functional specifications given in the “Specification Section”.

ix. All the compliances should be submitted on OEM Letterhead.

x. Response except “Yes” or “No” is not acceptable. If any bidder provides a response other than “Yes” or “No” the same will be treated as Not Available i.e. NA.

xi. Bidders whose proposals are fully compliant with all items listed in the Technical Proposal Compliance Sheet and who meet all specified technical and functional requirements shall be considered technically qualified.

xii. All technical compliance statements shall be submitted by the Original Equipment Manufacturer (OEM) on their official letterhead and must be supported by relevant data sheets, with the corresponding parameters clearly highlighted.

xiii. The Evaluation Committee reserves the right, at its sole discretion, to accept or reject any deviations from the stated requirements.

7. Evaluation of Bids and Award of Contract

7.1. Technical Evaluation:

A comprehensive evaluation of the bids will be conducted to ascertain the competence of bidders and the responsiveness of technical aspects to RFP requirements. Bids will be scored based on defined parameters.

Each bidder will have a 15-minute time slot to present Approach and Methodology, project components, and proposed resources. Technically qualified bidders will be invited for commercial bid opening, followed by commercial evaluation. Bids must score a minimum of 70 marks in Technical Score for eligibility to open the financial proposal.

7.2. Financial Evaluation Methodology (LCS):

a. The financial bids/ cover of the bidders who qualify in technical evaluation and scores 70 or more marks shall be opened at the notified time, date, and place by the members of the designated Committee in the presence of the bidders or their representatives who choose to be present.
b. The financial bid cover letter should be submitted in an appropriate format as per Annexure 19 followed by financial bid details**.**
c. The process of opening financial bids/ covers shall be similar to that of technical bids.
d. The names of the bidders, the rates given by them, and conditions put, if any, shall be read out and recorded.
e. Only fixed price financial bids indicating total prices for all the components specified in this bid document will be considered.
f. Prices quoted in the Bid must be firm and final and shall not be subject to any modifications, on any account whatsoever except applicable tax rates. The Bid Prices shall be indicated in Indian Rupees (INR) only.
g. The bid price will include all taxes and leaves mentioned separately.
h. Any conditional bid would be rejected.
i. If there is no price quoted for certain material or service, the bid shall be declared as disqualified.
j. Financial bids for those Bidders who are technically qualified in the technical evaluation will only be opened. All other commercial bids will not be opened. The financial evaluation shall be done based on the details submitted by the bidder as per the format provided. The bidders shall be sorted in ascending order as L1, L2, and L3 etc.
k. The bidder who has quoted the least cost (L1) shall be selected as the successful bidder.

7.2.1. Correction of Arithmetic Errors in Financial Bids

The Proposal evaluation committee shall correct arithmetical errors in substantially responsive Bids, on the following basis, namely: -

a. 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, unless in the opinion of the Proposal Evaluation Committee there is an obvious misplacement of the decimal point in the unit price, in which case the total price as quoted shall govern and the unit price shall be corrected.

b. If there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail, and the total shall be corrected; and

c. If there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to clause (a) and (b) above.

7.3. Deviations and Exclusions

Bids must strictly adhere to RFP requirements. A No Deviation Certificate as per Annexure 14 is to be submitted by the bidders. Deviations may result in rejection.

7.4. Rejection of Bids

Bids will be rejected for various reasons, including:

a. Assumptions, presumptions, or key points submitted with the bid.

b. Non-compliance with eligibility criteria or RFP terms.

c. Incorrect information, incomplete bids, or deviations.

d. Canvassing, erasures, or multiple make/models for a unique item.

7.5. Notification of Acceptance of Proposal

Before the Proposal's validity period expires, OCAC will notify the selected Bidder in writing via speed post, fax, or email about the project acceptance.

8. General Conditions of Contract

8.1. Definition of Terms

a. **Acceptance of System:** Upon installation, rollout, and deployment of trained manpower, the system will be considered accepted by the Client. This acceptance is contingent upon the successful execution and completion of all activities defined in the Scope of Work, evidenced by an Operational Acceptance Certificate.

b. **Applicable Law(s):** Refers to any governmental restrictions, laws, regulations, etc., applicable to the relevant party during the contract's execution.

c. **Approval:** OCAC will support SI in obtaining and maintaining regulatory licenses, clearances, and approvals necessary for service provision. SI bears the costs, and both parties provide necessary cooperation and information.

d. **Bidder:** The organization submitting a proposal in response to the RFP.

e. **Client:** Odisha Computer Applications Centre (OCAC), the project owner, to be executed in Bhubaneswar.

f. **Clause:** A provision in the General Conditions of Contract (GCC).

g. **Contract:** The agreement between the Client and SI, including all specified documentation.

h. **Contract Agreement:** The formal agreement between the Client and SI, recorded in a signed form.

i. **Contract Value:** The price payable to SI for fulfilling contractual obligations.

j. **Commercial Off-The-Shelf (COTS):** Ready-made software products available for sale or license to the public.

k. **Day:** Working day as per the calendar of Government of Odisha/OCAC.
l. **DR Cum DC Site:** The location for delivering, installing, and maintaining services specified in the Scope of Work.
m. **Deliverable:** Work product to be submitted by SI as part of the Service, listed in the Scope of Work.
n. **Document:** Any recorded text, image, data, or electronic document.
o. **Effective Date:** The date on which the Contract Agreement is duly executed.
p. **Force Majeure:** As defined in GCC Clause 7.18.
q. **GoI:** Government of India.
r. **GoO:** Government of Odisha.
s. **Go-Live:** Project commissioning after all Data Centre components, including training, as per the Scope of Work.
t. **Goods:** Equipment, subsystems, hardware, software, or other items SI supplies, installs, and maintains.
u. **LoA:** Letter of award issued to the selected Bidder.
v. **Performance Bank Guarantee:** 10% of the total project value submitted by the successful bidder to OCAC within 15 days of the Letter of Intent/Award, valid for at least 90 days beyond the contract period.
w. **OEM:** Original Equipment Manufacturer of supplied equipment/software.
x. **Services:** Work performed by SI under the RFP and contract.
y. **Service Level(s):** Parameters, targets, and performance criteria for Services and Deliverables described in the RFP and SLA.
z. **Service Level Agreement or SLA:** The agreement specified in the RFP.

8.2. Right to Terminate the Process

a. OCAC may terminate the RFP process at any time without assigning reasons.
b. This RFP is not on offer, and OCAC makes no commitments for a business transaction.

8.3. Language of Proposal & 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 Bidder should also be in English, and the correspondence between the Bidder & OCAC shall be in English language only. The correspondence by Fax / E-mail must be subsequently confirmed by a duly signed copy (unless already signed digitally).

8.4. OCAC's Right to Accept and Reject Proposals

Notwithstanding anything else contained in contrast in this RFP Document, OCAC reserves the right to accept or reject any Bid or to annul the bidding process fully or partially or modify the same and to reject all Proposals at any time prior to the award of work, without incurring any liabilities in this regard.
OCAC may terminate the RFP process at any time without assigning any reason. OCAC makes no commitments, expresses, or implies that this process will result in a business transaction with anyone.
This RFP does not constitute an offer by OCAC. The bidder’s participation in this process may result OCAC selecting the bidder to engage towards execution of the contract.

8.5. Modification and Withdrawal of Bids

The Bidder may be allowed to modify or withdraw its submitted proposal any time prior to the last date prescribed for receipt of bids, by giving a written notice to OCAC.

The Bidder's modification or withdrawal notice shall be prepared, sealed, marked, and dispatched in a manner like the original Proposal.

After the last date for receipt of bids, no modification of bids shall be allowed. No bid may be withdrawn in the interval between the deadline for submission of bids and expiration of the of bid validity period specified. Withdrawal of a bid during this period will result in Bidder’s forfeiture of bid security/EMD.

No written, oral, telegraph or telephonic proposals modifications will be acceptable.

8.6. Contacting OCAC

Any effort by a Bidder to influence the proposal evaluation, proposal comparison or contract award decisions at OCAC level may result in the rejection of the proposal.

8.7. Knowledge of Site Conditions

The SI’s undertaking of this Contract shall be deemed to mean that the SI possesses the knowledge of all data Centre related requirements as stipulated in the Tender Document including but not limited to environmental, demographic, and physical conditions and all criteria required to meet the design of the data Centre.

8.8. Failure to Agree with Terms & Conditions of the Contract

Failure of the SI to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event OCAC may award the contract to the next best value SI or call for new bids from the interested bidders or invoke the PBG of the most responsive SI. However, SI shall be allowed to submit minor deviations without any cost implications and allow for opportunity to mutually discuss its terms and conditions. The final decision in such an occurrence lies with OCAC.

8.9. Governing Law & Jurisdiction

The Contract shall be governed by and interpreted in accordance with the laws of India. The High Court of Judicature at Cuttack and Courts subordinated to such High Courts shall have exclusive jurisdiction in respect of any disputes relating to the tendering process, award of Contract and execution of the Contract.

8.10. Exit Management

System Integrator shall comply with all applicable statutes. OCAC shall not be liable in any manner whatsoever for any non-compliance on part of the System Integrator of the applicable laws and in the event of any claim of whatsoever nature arising thereof, the entire burden shall be strictly borne by the System Integrator.

System Integrator shall maintain all requisite records, registers, account books etc. related to this project which are obligatory under any applicable law in connection with the Services being rendered or work being performed to OCAC and shall provide such information as may be required under any law to any authority.

The SI shall document and submit a detailed Exit Management Plan (EMP) at OCAC for approval within 90 days post signing of the contract. The Exit Management Plan shall be re-drafted/ reviewed by SI on an annual basis and need to be submitted to OCAC.

8.11. Purpose of Exit Management Plan

a. This clause sets out the provisions which will apply upon completion of the contract period or upon termination of the agreement for default of the System Integrator. The Parties shall ensure that their respective associated entities, in case of OCAC, any PMU/Agency appointed by OCAC and in case of the System Integrator, the sub- contractors, carry out their respective obligations set out in this Exit Management Clause. Exit Management criteria will be a part of the Master Service Agreement with detailed information about exit criteria and exit management plans.

b. The exit management period starts exactly 30 days before, in case of expiry of contract, or on the date when the contract comes to an end and up to a period of 30 days in case of termination of contract, or on the date when the notice of termination is sent to the System Integrator.

c. At the beginning of the exit management period, the System Integrator shall ensure that.

d. All Project Assets including the hardware, software, documentation, and any other infrastructure shall have been cured of all defects and deficiencies as necessary so that the DR-DC Project is compliant with the Specifications and Standards set forth in the RFP, Agreement and any other amendments made during the contract period.

e. The System Integrator delivers relevant records and reports pertaining to the DR-DC Project and its design, engineering, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the Divestment Date.

f. On request by OCAC , or any PMU/Agency appointed by OCAC, the System Integrator shall effect such assignments, transfers, licenses and sub-licenses related to any equipment lease, maintenance or service provision agreement between System Integrator and any PMU/Agency, in favour of OCAC, or any PMU/Agency appointed by OCAC, if it is required by OCAC, or any PMU/Agency appointed by OCAC, and is reasonably necessary for the continuation of services by OCAC, or any PMU/Agency appointed by OCAC;

g. The System Integrator complies with all other requirements as may be prescribed under Applicable Laws to complete the divestment and assignment of all the rights, title, and interest of the System Integrator in the DR-DC Project free from all encumbrances and free of any charge or tax to OCAC or its nominees.

h. During the Exit Management period, The System Integrator will allow OCAC, GoO or any third party appointed by OCAC, GoO, access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable OCAC, GoO or any PMU/Agency appointed by OCAC, GoO to assess the existing services being delivered.

i. Promptly on reasonable request by OCAC, GoO or any PMU/Agency appointed by OCAC, GoO, the System Integrator shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with the “Contract”, the Project Plan, SLA and scope of work, relating to any material aspect of the services (whether provided by the DR-DC System Integrator or sub-contractors appointed by the System Integrator). OCAC, GoO

or any PMU/Agency appointed shall be entitled to copy all such information. Such information shall include details pertaining to the services rendered and other performance data. The System Integrator shall permit OCAC, GoO or any PMU/Agency appointed to have reasonable access to its employees and facilities as reasonably required by OCAC, GoO or any PMU/Agency appointed to understand the methods of delivery of the services employed by the System Integrator and to assist appropriate knowledge transfer.

j. Before the end of exit management period, the System Integrator will assist in a successful trial run of Network administration, Facility management including helpdesk management by OCAC, GoO or by any PMU/Agency appointed.

k. Hand Over of Assets/ Documents; SI shall hand over the peaceful possession of Project Assets in good and working condition with detail list showing the name of the equipment and with configuration to the Purchaser/replacement SI as authorized by Purchaser customer within 30 days of the date of serving of notice or within the Transition Period.

l. The SI shall provide all such information available with it during the contract execution or during the operation & management phase as may reasonably be necessary within a reasonable period not exceeding 30 days of the date of serving of notice or within the Transition Period.

m. Existing SI will hand over the documents to OCAC or new SI, pertaining to the operation of DR-DC

8.12. Statutory Compliances

The SI shall not exist from the contract within stipulated time of five (5) years after Go-Live. However, if SI decides to opt out of the contract prematurely it has to notify the authority six months in advance through a written letter, SI will not seek ownership rights over the equipment and its PBG will also be forfeited.

If the SI exits from the contract during the execution within the stipulated time period, then OCAC reserves the right to terminate the contract and may ask the bidder with L2 price to match the price of L1 and execute the remaining work as per RFP scope of work.

8.13. Severability and Waiver:

If any provision of this Agreement, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid, or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision by a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision. No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement of any right, remedy or provision of this Agreement shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision or the exercise or enforcement of any other right, remedy or provision.

a. If any provision is deemed illegal or unenforceable,
b. No waiver of rights, remedies or provisions unless explicitly stated.

8.14. Applicability of Liquidated Damages

The System Integrator shall accomplish the scope of work under this RFP / Agreement as per the Project Timelines and as per the Service Level Agreements. If the System Integrator fails to achieve the Project Timelines (Section 10.3 of the RFP) or if it fails to achieve the Service Levels Agreement (SLA) (Section 11 of the RFP) for any reason whatsoever, the System Integrator shall be liable to pay liquidated damages as provided in Section 11 Service Level Agreement of the RFP. OCAC shall have the right to determine such extent of fault and liquidated damages in consultation with System Integrator and any other Party as it deems fit. Payment of liquidated damages shall be the sole and exclusive remedies available to OCAC The Liquidation damage shall be capped at 10% of the total contract value (TVC). If the liquidation damage exceeds 10% of the TVC, OCAC may terminate the bidder.

8.15. Dispute Resolution

OCAC and the System Integrator shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with this Agreement. All negotiations, statements and/or documentation pursuant to these disputed matters shall be without prejudice and confidential (unless mutually agreed otherwise). The time and resources costs of complying with its obligations under this provision shall be borne by respective Parties. All Arbitration proceedings shall be held at Bhubaneswar, Odisha, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English. non-settlement of the dispute, same shall be referred to the Commissioner-cum- Secretary to Government, E&IT Department, Government of Odisha for his decision and the same shall be binding on all parties, unless either party makes a reference to arbitration proceedings, within sixty days of such decision.

Informal Negotiation:

OCAC and the System Integrator commit to resolving disputes amicably through direct informal negotiations. All discussions and documentation related to disputes are confidential and without prejudice, unless mutually agreed otherwise. The respective parties bear the time and resource costs associated with meeting the obligations of this provision.

8.16. Arbitration

Any and all disputes, controversies and conflicts ("Disputes") arising out of this Agreement between the Parties or arising out of or relating to or in connection with this Agreement or the performance or non-performance of the rights and obligations set forth herein or the breach, termination, invalidity or interpretation thereof shall be referred for arbitration in terms of the Arbitration and Conciliation Act, 1996 or any amendments thereof. Prior to submitting the Disputes to arbitration, the Parties shall resolve to settle the Dispute/s through mutual negotiation and discussions. In the event that the said Dispute/s are not settled within thirty (30) days of the arising thereof, the same shall finally be settled
and determined by arbitration in accordance with the Arbitration & Conciliation Act ,1996 or any amendment thereof. The place of arbitration shall be Bhubaneswar, and the language used in the arbitral proceedings shall be English.

The arbitral award shall be in writing and shall be final and binding on each Party and shall be enforceable in any court of competent jurisdiction. None of the Parties shall be entitled to commence or maintain any action in a court of law upon any Dispute arising out of or relating to or in connection with

this Agreement (infringement of IPR Excepted), except for the enforcement of an arbitral award or as permitted under the Arbitration & Conciliation Act ,1996

In case of non-settlement, disputes will be referred to the Commissioner-cum-Secretary to Government, E&IT Department, Government of Odisha, unless party initiates arbitration proceedings within sixty days of such decision.

Arbitration proceedings will be held in Bhubaneswar, Odisha, and conducted in English.

8.17. Resolution Attempts:

Prior to arbitration, the parties will attempt to settle disputes through mutual negotiation for a period of thirty days.

Unsettled disputes will be subject to arbitration under the Arbitration and Conciliation Act, 1996, in Bhubaneswar, with proceedings conducted in English.

The resulting arbitral award will be final, binding, and enforceable in any court of competent jurisdiction.

8.18. Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the SI or OCAC which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affects the performance of the contract, such as:

Neither Party shall be responsible to the other for any delay or failure in performance of its obligations due to any occurrence commonly known as Force Majeure which is beyond the control of any parties, including, but is not limited to, flood, explosion, thundering, acts of God or any Governmental body, public disorder, riots, embargoes, or strikes, acts of military authority, epidemics, lockouts or other Labour disputes, insurrections, civil commotion, war, enemy actions.

If a Force Majeure arises, the System Integrator shall notify promptly within a reasonable time frame to OCAC in writing of such condition and the cause thereof. Unless otherwise directed by OCAC, System Integrator shall continue to perform his obligations under the Agreement as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

The System Integrator shall be excused from the performance of his obligations in whole or part as long as such cases, circumstances or events shall continue to prevent or delay such performance. Neither Party shall have any liability to the other Party in respect of the termination of this Agreement because of an event of Force Majeure.

In case of a Force Majeure, all Parties will endeavour to agree on an alternate mode of Performance to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure.

System Integrator shall be paid for supply and services till the last date of termination in case of force majeure.

If a force majeure condition arises, the System Integrator shall promptly notify the other party, specifying the nature of the condition. If the force majeure event continues for more than 30 days and services remain suspended, either party shall have the right to terminate this Agreement by providing written notice.

Force Majeure events excuse parties from performance obligations.

The System Integrator must promptly notify OCAC of Force Majeure conditions and continue performance to an extent feasible.

8.19. Confidentiality

OCAC may allow the System Integrator to utilize Confidential Information, and the System Integrator shall maintain the highest level of secrecy, confidentiality, and privacy with regards to such Confidential Information. The System Integrator shall use its best efforts to protect the confidentiality and propriety of Confidential Information.

Additionally, the System Integrator shall keep confidential all the details and information with regards to the Project, including systems, facilities, operations, management, and maintenance of the systems/facilities. The System Integrator shall use the information only to execute the Project.

OCAC shall retain all rights to prevent, stop and if required take the necessary punitive action against the System Integrator regarding any forbidden disclosure.

The System Integrator may share the confidential information with its employees, affiliates, agents, and subcontractors but only strictly on a need-to-know basis in order to accomplish the scope of services under this Agreement. Upon request of OCAC, the System Integrator shall execute a corporate non-disclosure agreement (NDA) with OCAC in the mutually agreed format provided by OCAC shall ensure that all its employees, agents and sub-contractors are governed by confidential obligations similar to the one contained herein. The SI and its antecedents shall be bound by the NDA. The SI will be held responsible for any breach of the NDA by its antecedents/ delegates/ employee/ subcontractors etc.

To the extent the System Integrator shares its confidential or proprietary information with OCAC for effective performance of the Services, the provisions of the confidentiality Clause (I) to (iii) shall apply mutatis mutandis on OCAC.

The Bidder shall not use Confidential Information, the name, or the logo of the OCAC except for the purpose of providing the Service as specified under this contract.

The System Integrator agrees to maintain confidentiality of OCAC's information and project details.

Confidential information can be shared on a need-to-know basis with employees and affiliates.

Breach of confidentiality may lead to punitive actions.

8.20. Fraud and Corrupt Practices:

a. The SI and their respective officers, employees, agents, and advisers shall observe the highest standard of ethics during the Selection Process. For this purpose, the definition of corrupt and fraudulent practices will follow the provisions of the relevant laws in force. Notwithstanding anything to the contrary contained in this RFP, OCAC shall reject a Proposal without being liable in any manner whatsoever to the SI, if it determines that the SI has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice (collectively the “Prohibited Practices”) in the Selection Process. In such an event, OCAC shall, without prejudice to its any other rights or remedies, declare the SI ineligible, either indefinitely or for a stated period of time, forfeit and appropriate the Proposal Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the Authority for, inter alia, time, cost and effort of the Authority, in regard to the RFP, including consideration and evaluation of such SI Proposal.

b. Without prejudice to the rights of OCAC under Clause above and the rights and remedies which OCAC may have under the Loi or the Contract Agreement, if an SI or Systems Integrator, as the case may be, is found by OCAC to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the Loi or the execution of the Agreement, such SI shall not be eligible to participate in any RFP or RFP issued by OCAC for a period of two (2) years from the date such SI, as the case may be, is found by OCAC to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

c. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:

d. “Corrupt practice” means Engaging in any manner whatsoever, whether during the Selection Process or after the issue of the Loi or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Loi or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of OCAC in relation to any matter concerning the Project;

e. “fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process; the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of OCAC who is or has been associated in any manner, directly or indirectly with the Selection Process or the LoA or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of OCAC, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or

f. “Coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person s participation or action in the Selection Process.

g. “Undesirable practice” means establishing contact with any person connected with or employed or engaged by OCAC with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or having a Conflict of Interest; and

h. “Restrictive practice” means forming a cartel or arriving at any understanding or arrangement among SIs with the objective of restricting or manipulating a full and fair competition in the Selection Process.

i. Prohibits corrupt, fraudulent, coercive, undesirable, and restrictive practices during the selection process.

j. OCAC may reject a proposal and declare the System Integrator ineligible in case of prohibited practices.

8.21. Taxes and Duties

All payments will be subject to tax deduction at source as required by prevailing tax rates. Any changes, revisions, or enactments in duties such as GST, taxes, or any CESS during the validity of the Bids and the contract period by Central/State/Other Government bodies will be considered and applied after due consideration. Taxes at the time of supplying goods and services shall be applicable as per the law.

For goods supplied from outside the Purchaser's country, the System Integrator (SI) shall be entirely responsible for all applicable taxes, license fees, and other levies imposed outside the Purchaser's country. The basic price quoted item-wise by the bidder to OCAC shall include all taxes, duties, and charges payable by the bidder except for GST, CGST plus OGST, or IGST, as applicable, which shall be quoted alongside the basic price for all items. However, when quoting the basic price against the package/works, the SI should adjust the quoted price for Input Tax Credit (ITC).

8.22. Audit, Access, and Reporting

The System Integrator shall grant access to OCAC or its nominated agencies to all data related to OSDR. This includes data in the possession or control of the System Integrator, subcontractors, agents, and suppliers, relating to the provision of services as outlined in the Audit, Access, and Reporting Schedule. OCAC may engage external Third-Party Auditors (TPA)/ Designated agencies to conduct audits and verify MIS reports/QGR data submitted by the SI. The cost of TPA audits shall be borne by OCAC.

An Internal Audit Team constituted with CT Member/OCAC officials will perform internal audits of DR Cum DC ISO processes (ISO 27001 and ISO 20000) on a half-yearly basis, with audit findings reported to the Project Manager-CT/OCAC within one month of completion.

8.23. Ownership

Products and Fixes: COTS products, solutions, and fixes provided will be licensed as per the terms of the accompanying license agreement. OCAC will own all exclusive developments meeting the functional requirements of this Agreement.

All IT Hardware and Software: All hardware and software must be procured in the name of OCAC, which will be the owner of all items upon handover.

Training and Other Material: Ownership of all Intellectual Property Rights (IPR) in documents, artifacts, and training material made during the Agreement will lie with OCAC.

8.24. Safety Regulations

The Successful Bidder shall ensure the safety of OCAC personnel and property during the project. The Bidder is responsible for material/equipment transportation, with penalties for damage to property/OCAC Tower building. Compliance with safety measures under applicable law is the responsibility of the Successful Bidder.

8.25. Warranty of Equipment

The Bidder must provide a warranty valid for Five (5) Years from the date of Go-Live, for all supplied equipment, as per the financial bid format in the RFP.

Products supplied under the RFP should not reach the end of support before 7 years from the date of FAT or start of O & M services

8.26. OEM Certificate of Equipment

The bidder must furnish Manufacturer Authorization Form (MAF) from all the OEMs. The certificate should state the bidding company's authorization to offer the equipment and a commitment to provide spares support during the comprehensive warranty period. If spares are being stored by an authorized supplier of the OEM, such OEM must also submit a certificate stating that the OEM shall take over maintenance responsibility if their authorized supplier fails during the comprehensive warranty period. Complete contact details of the OEM, including the name, designation of contact person, postal address, email ID, and telephone & FAX numbers, must be provided for verification by the buyer. Failure to provide this information may result in blacklisting or barring from future tenders.

8.27. Comprehensive AMC of Equipment

The selected bidder is responsible for operating and maintaining DR Cum DC throughout the entire contract period, covering all recurring expenditures such as AMC for support equipment, operating staff salaries, and incidental expenses related to project implementation.

The selected bidder must ensure periodic AMC for support equipment to keep it in working condition during the contract period, bearing the associated expenditure. However, consumables may be reimbursed based on actuals, subject to approval from OCAC.

All IT hardware and software must be procured in the name of OCAC as the owner of the project. All items will be handed over to the OCAC under this contract upon the successful completion of the final acceptance test.

8.28. Spares and Performance of Equipment

In the Technical Proposal, the Bidder must specify a comprehensive list of spares to be maintained, meeting the various SLA parameters outlined in the tender.

The Successful Bidder is obliged to guarantee the supply of spares for all equipment under the scope of supply for a minimum period of 5 years from the date of awarding the contract. Additionally, they guarantee that the discontinuity of production of any item offered as part of the system will not affect the maintainability of the system for a period of 5 years from the start date of operation and maintenance support of the data Centre.

8.29. Change Order and Contract Amendment

OCAC reserves the right to order the selected bidder through Notice, in accordance with the "Notices" clause, to make changes within the general scope of the Contract, including drawings, designs, or specifications, delivery location, and related services.

Any change causing an increase or decrease in the cost or time required for the selected bidder's performance under the Contract will result in an equitable adjustment to the Contract Price or the Delivery and Completion Schedule, or both. Claims for adjustment under this clause must be asserted within thirty (30) days from the date of the selected bidder's receipt of the Purchaser's change order.

Prices for any related services not included in the Contract shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the selected bidder for similar services.

8.30. Contract Extension

The contract may be extended on a yearly basis, up to a maximum of two years, with mutually agreed terms and conditions between the bidder and OCAC. This extension should be finalized three months before the expiry date.

8.31. Termination and Effects of Termination

This Agreement shall be terminated by either party upon the happening of all or any of the following events: -

Upon either Party being declared insolvent or bankrupt. Upon either Party committing a material breach or being in default of all or any of the major and significant terms, conditions, covenants, undertakings, and stipulations of this Agreement. In case the material breach is remediable the aggrieved Party shall give notice in writing of such default in observance or performance of any of the terms or conditions of this Agreement, to the Party in default. If the Party in default effectively remedies such breach or default within the period, not being less than 60(sixty) days, designated by such notice then the Agreement shall remain in force. Where the default by the System Integrator is as a result of or consequent to technical non- feasibility, which requires to modify/alter the scope of work so as to replace the technical non-feasible deliverable, with a feasible deliverable, then such default shall not be considered a default by the System Integrator under the provisions of this clause

By mutual agreement in writing between the parties.

a) Termination for Breach- In the event of the breach of any of the major and significant terms and conditions of this Agreement by the system integrator, OCAC shall be entitled to terminate this agreement by giving 30 days' notice. The decision of OCAC as to such breach shall be final and binding on the system integrator. In the event of breach of any of the major and significant terms and conditions of this agreement by the system integrator, OCAC will give 30 days' notice to system integrator to cure the breach of the terms and conditions of the agreement then in that case System Integrator must cure within 30 days. In case the breach continues till/after expiry of such cure period, OCAC will terminate the agreement.

b) Effects of Termination

c) Upon expiration or termination of this Agreement:

i. The System integrator shall:
   - Notify forthwith the particulars of all project assets.
   - Deliver forthwith actual or constructive possession of the assets free and clear of all encumbrances and execute such deeds, writings and documents as may be required for fully and effectively divesting the Bidder all of its rights, title and interest in the DR cum DC project.
   - Deliver relevant records and reports pertaining to the DR cum DC project and its design, engineering, operation, and maintenance including all operations & maintenance records and manuals pertaining thereto and complete as on the date of termination or expiration. And
   - Shall expeditiously settle the accounts.

ii. In the event OCAC terminates this Agreement pursuant to any material breach by the System

Integrator to complete its obligations under this Agreement, Performance Bank Guarantee furnished by SI may be forfeited for reasons, to be recorded in writing.

iii. Upon termination (or prior to expiry/ upon expiry, as the case may be) of this Agreement, the Parties will comply with the Exit Management Clause set out in this Agreement

iv. OCAC agrees to pay the System Integrator for all charges for Services / Equipment provided by it and accepted by OCAC till effective date of termination.

v. All payments under this clause shall be payable only after the System Integrator has complied with and completed the transition and exit management as per the Exit Management Clause approved by OCAC. In case of expiry of the Agreement, the last due payment shall be payable to the System Integrator after it has complied with and completed the transition and exit management as per the exit management clause approved by OCAC.

vi. SI immediately upon termination, discontinue providing any or all of the services contemplated hereunder.

vii. OCAC shall upon termination, by under no obligation to make any payments to System Integrator forthwith, except for any payments that may be due and payable to SI in respect of satisfactory services already completed as per scope.

9. Detailed Scope of Work

The broad specified scope of work to be undertaken by the **"Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha"** for the period of 5Y6M years (For an estimated implementation period of 6 Months plus 5 Years Operation from FAT), has been outlined below.

The broad scope of work for the SI during the period of contract/ engagement would include the following for the sites, for which work order may be given:

a. Design, Supplying, installation, and configuration, testing and commissioning of computer infrastructure (hardware & software) such as Servers, Operating systems, and virtualization etc.

b. Supply, installation, configuration, testing and commissioning of Network infrastructure like, Router, High availability, including laying, testing, and commissioning of inter-rack and intra-rack structured cabling (OFC and copper cable).

c. Supply, installation, configuration, testing and commissioning of Storage Area Network with Enterprise Class Storage system, Unified storage SAN switches, Tape Library, backup and restore, including laying of FC cables.

d. Design, Supply, installation, and configuration, testing and commissioning of security infrastructure (hardware & software) such as D-DoS, Firewall, XDR etc.

e. Design, Supply, Installation and Commissioning, final acceptance test (FAT) of Non-IT & IT Infrastructure for Disaster Recovery Centre cum data centre.

f. Five years on-site comprehensive maintenance and provisioning of services of all the ICT Infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance by OCAC.

g. System Integrator to get the following Disaster Recovery Centre Certification before Go-Live and

all related costs for the certification will be borne by System Integrator:

i. ISO/IEC 27001
ii. ISO/IEC 20000
iii. ISO/IEC 9001
iv. ISO/IEC 27017
v. ISO/IEC 22301

h. The cost of sustenance audit for the above certification shall be the responsibility of the successful System Integrator for the entire contract period.
i. Testing & Commissioning
j. Post-Implementation: Management & Maintenance
k. Security management
l. Training in IT infrastructure, SLA, Various Disaster Recovery Centre etc.
m. Onsite support for Disaster Recovery Centre Operations on 24x7x365 basis by qualified and trained engineers/personnel for a period of five years to ensure more than 99.982% service availability as per Tier 3 standard.

Requirement Gathering Phase

The System Integrator will be responsible for preparation of detailed project plan. The plan shall address, at the minimum, the following:

a. Define an organized set of activities for the project and identify the interdependence between them.
b. Resource planning and loading for each phase/activity. This must also indicate where each resource would be based during that phase, i.e. onsite at the OCAC office at System Integrator premises.
c. Establish and measure resource assignments and responsibilities.
d. Highlight the milestones and associated risks.
e. Communicate the project plan to stakeholders with meaningful reports.
f. Measure project deadlines and performance objectives.
g. Project Progress Reporting: During the implementation of the project, System Integrator should present weekly reports.

This report will be presented in the meeting. The report should include, at the minimum, undermentioned:

i. Results accomplished during the period (weekly)
ii. Cumulative deviations from the schedule date as specified in the finalized Project Plan.
iii. Corrective actions to be taken to return to the planned schedule of progress.
iv. Plan for next week.
v. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of System Integrator.
vi. Support needed.
vii. Issues/Concerns
viii. Risks/Showstoppers along with mitigation

h. Identify the activities that require the participation of client personnel (including the Program Management Unit etc.) and communicate their time requirements and schedule early enough to

ensure their full participation at the required time

Based on the understanding and its own individual assessment, System Integrator shall develop & finalize the FRS document in consultation with OCAC and its representatives. While doing so, System Integrator at least is expected to do following:

a. System Integrator shall conduct a detailed survey and prepare a gap analysis report, detailed survey report of the physical and DR infrastructure requirements. System Integrator shall duly assist the department in preparing an action plan to address the gaps.
b. System Integrator shall develop and follow standardized template for requirements capturing and system documentation.
c. System Integrator must maintain traceability matrix from inception stage for the entire implementation.
d. System Integrator must get the sign off from user groups formed by OCAC.
e. For all the discussions with the OCAC team, System Integrator shall be required to be present at the OCAC office with the requisite team members.

Implementation Phase

- **Design Phase**

System Integrator shall build the solution as per the Design Considerations and requirement of OCAC. The solution proposed by System Integrator should comply with the design considerations requirements as mentioned therein.

System Documentation: System Documentation both in hard copy and soft copy to be supplied along with licenses and shall include but not limited to following. Documentation to be maintained updated and submitted to OCAC regularly:

i. Conceptual Design Brief: High-level layout, tier classification, scalability goals
ii. Detailed Architectural Drawings: Floor plans, elevations, hot/cold aisle layouts
iii. Software Requirement Specification (SRS)
iv. MEP Schematics: Mechanical, electrical, plumbing system designs
v. Fire Protection & Safety Plans: Wall ratings, suppression systems, evacuation routes
vi. Environmental Impact Assessment: Sustainability metrics, LEED targets
vii. High level design of whole system
viii. Low Level design for whole system
ix. Any other explanatory notes about the system
x. Traceability matrix
xi. RACI Matrix (Responsible, Accountable, Consulted, and Informed)
xii. Technical and product related manuals
xiii. Installation guides

The above documents will be part of the solution design phase.

- **Supply/ Installation**

The selected System Integrator would be required to undertake all the necessary work required towards completion of Non-IT & IT infrastructure for DR-DC. The selected System Integrator shall procure and

install all relative components, installation shall mean to install and configure / integrate every component and subsystem component, required for functioning of DR-DC.

- **Testing and Final Acceptance Criteria**

SI shall demonstrate the following mentioned acceptance criteria prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. SI may propose further detailed Acceptance criteria which the OCAC will review. Once OCAC provides its approval, the Acceptance criteria can be finalized. In case required, parameters shall be revised by OCAC in mutual agreement with System Integrator and the revised parameters shall be considered for acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.

Disaster Recovery Plan should be able to identify those applications and customers that are critical to the business and the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO. The Recovery Time Objective is the length of time a business can be without data processing availability and the Recovery Point Objective (RPO) is how old the data will be once the systems are recovered.
Disaster Recovery Plan should include:

- Plan Scope and Objectives
- Business Recovery Organization (BRO) and Responsibilities (Recovery Team Concept)
- Major Plan Components - format and structure
- Scenario to Execute Plan
- Escalation, Notification and Plan Activation
- Vital Records and Off-Site Storage Program
- Personnel Control Program
- Data Loss Limitations
- Plan Administration (general)

The Disaster Recovery Plan should be developed to accomplish the following objectives:

- Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
- Assess damage, repair the damage, and activate the repaired data Centre.
- Recovering data and information is imperative to the operation of critical applications.
- Manage the recovery operation in an organized and effective manner.
- Prepare technology personnel to respond effectively in disaster recovery situations.

- **Disaster Recovery Testing /Drill**

The purpose of Disaster Recovery testing is to specifically identify and document the task plan and procedures to be implemented in a testing environment. This Test Plan includes test parameters, objectives, measurement criteria, test methodology, task plan charts and timelines to validate the effectiveness of the current Disaster Recovery Plan. The Disaster Recovery Plan will be tested to ensure that the business can continue the critical business processes in the event of a disaster. It is very important that the Recovery procedures are executable and accurate. Another benefit of testing the plan

is to train the personnel who will be responsible for executing the Disaster Recovery Plan. The important issue is not that the test succeeded without problems, but that the test results and problems encountered are reviewed and used to update or revise the current Disaster Recovery Plan procedures. Testing can be accomplished by executing the disaster implementation plan or it may be desirable to execute a subset of the plan. When performing a Disaster Recovery Test, it is very important to use only that information which is recalled from the off-site storage facility. This is to ensure the following:

Simulate the conditions of an actual Disaster Recovery situation.

a. Completeness of the disaster recovery information stored at the Records Retention Site.
b. Ensure the ability to recover the intended functions.

This test plan includes the following areas:

c. Schedule
    i. Planning Sessions
    ii. Pre-Test Technical Review
    iii. Debriefing
d. Introduction
    i. Preface
    ii. Scope
    iii. Recovery Site
    iv. Primary Test Objectives
    v. Secondary Test Objectives
    vi. Exclusion (if applicable)
    vii. Test Assumptions, Dependencies and Success Criteria
e. Pre-Test Planning
    i. Activities
    ii. Issues
    iii. Concerns
f. Test Timeline
    i. Planned start and stop time of test and tasks.
    ii. Actual start and stop time of test and tasks (to be completed during the test)
g. Critical Test Checkpoints
    i. Activity
    ii. Recommendation
    iii. Responsible party
h. Problem Log Test
    i. Document any problems encountered prior to the test.
    ii. Record any deviations from Test Plan.

- **Post Disaster Recovery Testing Review**

The purpose of this Post Disaster Recovery Test Review is to identify any problem areas and any recommendations for improvement to the plan. The Post Test Review document includes the following areas:

a. **Highlights**
   i. Overall Test Results
   ii. Test Dates
   iii. Disaster Recovery Back-up Site
   iv. Local Access Suite
   v. Test Participants

b. **Test Objectives**
   i. Primary Test Objectives
   ii. Secondary Test Objectives
   iii. Exclusions (if applicable)

c. **Timeline**
   i. Planned task, start and end times and duration
   ii. Actual task, start and end times

d. **Problems Encountered During the Test**
   i. Problem Log
      - Actual Problem
      - Assigned to
      - Target Date for Resolution
      - Status
      - Resolution
      - DR Process or Technical
   ii. Problem Summary
      - Follow Up to Pre-Test Problems
      - Follow Up to Suggestions for Improvement/Recommendations from Last Year's Test
      - Detailed Summary and Observations
      - Recommendations for Next Year's Test

9.1. Non-IT Infrastructure requirements

a. The following specifications represent the overarching design expectations for the DR-DC infrastructure. These are indicative in nature and do not encompass the complete scope. The successful bidder is required to:
b. Comply with industry-recognized data centre design best practices and standards, including but not limited to Tier classifications, uptime targets, security protocols, and sustainability benchmarks.

c. Incorporate flexibility and scalability in the design to accommodate future growth and emerging technology requirements.
d. This section serves as a directional framework. Final execution must be in strict conformance with both the explicit requirements stated in the RFP and the prevailing industry standards.
e. The scope includes the supply, installation & commissioning of any material or equipment including civil works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project.
f. The solution shall comprise of supply, installation, testing, commissioning training and handing over of all materials, equipment, hardware, software, appliances, and necessary labour to commission said system complete with all the required components strictly as per (but not limited to) the latest IS, IEC, IEEE, ASHRAE, NBC etc. codes.
g. The bidder shall provide detailed design, documentation, make, and model, efficiency including user, system, and operation manuals along with the necessary diagrams, design drawings and details bifurcation of Bill of Quantity (BOQ) along with details description. The shop drawing (to be submitted before execution or as on when required) may include but not be limited to the following
    - Site layout
    - Equipment placement layout
    - All drawing for Electrical scheme including single line diagram
    - All GA drawings of equipment
    - Piping schematic
    - Grounding and Earth pits
    - Lighting
    - Furniture placement
    - DG fuel pump
    - Complete HVAC system
    - Networking cabling
    - Trenches, cable trays and raceways
    - Shafts
    - Panel GA drawing
    - Fire detection and suppression system
    - Aspirating smoke detection, water leak detection, rodent repellent, CCTV, access control system
    - DCIM schematic
    - Reflected ceiling plan
    - Sectional views

As and when required, the successful bidder has to submit the coordinated drawing for the solution.

a. The bidder shall be responsible for performing verification tests at their factory and at site to ensure all proposed software and hardware are functioning as per design at their own cost.
b. The bidder shall take the necessary clearance / approval of the drawings, design, quality of material,

make and model of the quoted material etc. prior to the execution of the project

The server farm area load density will be as follows

- Low Density - 60% of racks = 7.5 KW
- Medium Density - 20% of racks = 10 KW
- High Density - 20% of racks = 12 KW

The minimum specified scope of work to be undertaken by the bidder for Design, Supply, Installation, testing, Commissioning, Operations and Maintenance of the proposed DR-DC at Keonjhar as per the scope mentioned below. The selected bidder shall ensure an uptime more than 99.982% on a quarterly basis for period of five years after Go Live.

The minimum specified work to be undertaken by the bidder for setting up and operating the proposed Disaster Recovery Centre DR-DC, has been categorized as under:

a. Develop appropriate design, make all required approval, Supply Installation Testing and commissioning including associated works of the proposed DR-DC at Keonjhar
b. Data & Application migration from currently working at State Data Centre to DR-DC
c. Operations and Maintenance services for the complete Infrastructure at DR-DC at Keonjhar for a period of 5 years from the date of successful acceptance by OCAC.

Note: The bidders are requested to submit their proposals for these Schedules in the same bid which would be combined for evaluation purposes.

The scope shall comprise the design, supply, construction and testing of the proposed Disaster Recovery Centre building including all enabling works. All Works shall be carried out as per the proposed design and specifications and in accordance with the requirements of all relevant Indian standard codes.

The indicative scope of work (Area/Room wise) is illustrated below. Please note that the descriptions below are indicative in nature. The bidders should evaluate the site physically to understand the actual work requirement to complete the package before bidding for the same.

Indicative Logical Schematic

a. Present an indicative schematic of the DR-DC design architecture, illustrating major IT components provisioned by the Bidder.

b. Describe the compute environment, the approximate number of racks, and the common network/security infrastructure for both environments.

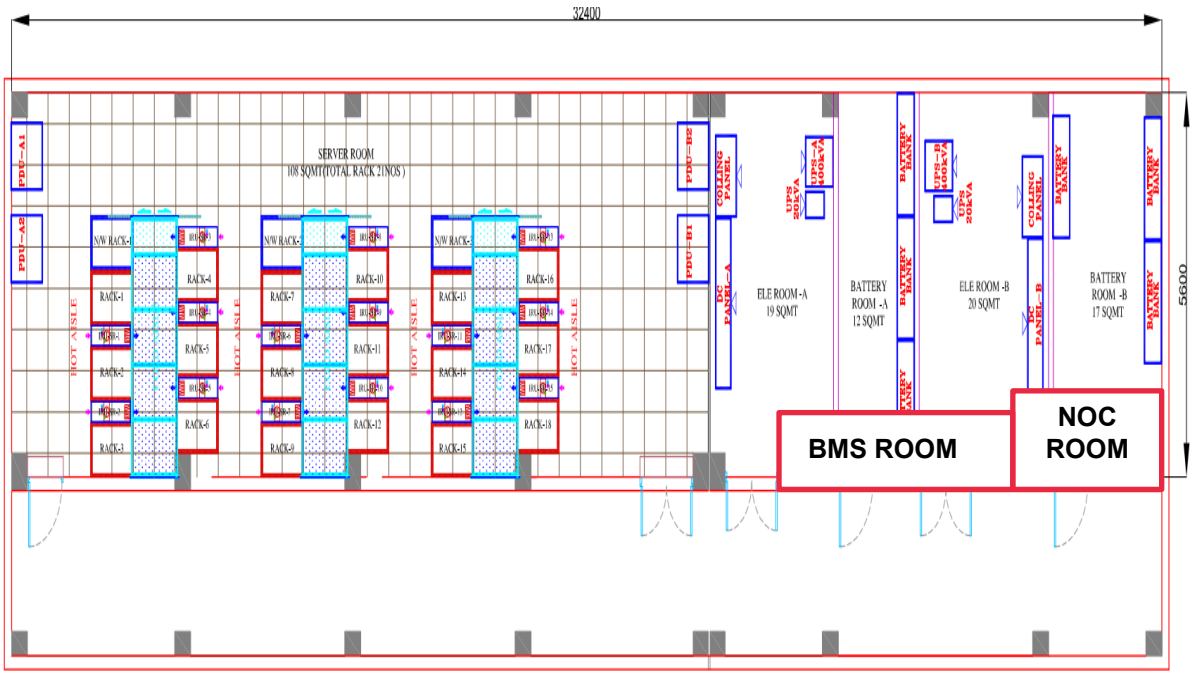


Fig: DR-DC Centre Layout

Utility Room:

The bidder is advised to do a detail site survey of the Site, take measurements, and list out all the work required for disaster recovery centre design and specifications and in accordance with the requirements of all relevant Indian standard codes.

The indicative scope of work (Area/Room wise) is illustrated below. Please note that the descriptions below are indicative in nature. The bidders should evaluate the site physically to understand the actual work requirement to complete the package before bidding for the same.

The guide is advised to do a detailed site survey of the Site, take measurements, and list out all the work required for Disaster Recovery Centre room to make it better in terms of facility, manageability, and operability.

The scope for the area is mentioned here but not limited to the following.

a. Exhaust fans are to be installed in the panel room for 5 to 6 air changes in an hour.

b. Fire Extinguisher of a minimum of 4.5 Kgs suitable for such an area to be provided in the rooms. One for the Transformer area and as per requirements for panel room.

c. Dismantling existing Wall, Doors, Window, or any structure of any material if required & removal of equipment such as panels, cables Debris from the site and storing, / disposing the same at a location as intimated by client will be in the bidder's scope

Campus Surroundings:

a. Existing trenches may be used for laying cables if any. In the process, there may be chances of breakage of trench covers. The same must be replaced by the Bidder with equal specification.

b. Cable Trenches: if there are any existing cable trenches available & may be used, however the bidder should evaluate & propose if there will be need to create new cable trenches. In case it is required the same may be proposed. In case trenches are required, the specification must be same as existing ones except the size of the trench.

c. HSD Tank: Two no's of 5 KL underground HSD tanks need to be installed for the required DG sets for which suitable space to be identified & piping for the same should be done up to the DG sets. The DG fuel pipeline must have intrinsically safe Fuel meters with connectivity feature to DCIM. The meters must be integrated with DCIM tool. Each DG fuel consumption to be measured. Redundant pumps and piping to be installed as per Uptime Tier guidelines.

d. Placement of Outdoor Area for PACs & CACs: It is proposed that AC ODUs on a platform of steel structure (using ISMB, ISMC of adequate size to cater the load) of 5 Meter height on the back side of the building adjacent to the GF floor of the building (DR-DC floor) level. The bidder should plan for the structure design accordingly. The bidder must submit a drawing and design for the platform duly authorized by a certified structural consultant.

Disaster Recover Centre Area

a. **Skirting:** Skirting needs to be created whenever required.

b. **Ceiling:** Server farm area will have no ceiling. However, a 23 mm nitrile rubber has to be pasted under the roof for thermal insulation. The workmanship should be such that it looks neat and clean without any tears, overlapping, exposed roof, or non-aligned joints. The bidder must propose ceiling in the support area (BMS Room). However high quality modular mineral fiber celling with min 0.5 NRC may be accepted.

c. **Flooring:** DR-DC server farm area has to have raised floor of calcium sulphate material. The height must be 300mm from the floor. The floor tile UDL must be 1500 kg/Sq. Mtr and point load 450 KG. Nitrile rubber Insulation 19/13 mm (minimum) under floor and true ceiling including skirting of desired specification must be laid in the server farm area for insulation. The floor for BMS room has to be with carpet tiles etc.

   Supply and installing 500mm x 500mm or 300mm x 1200mm carpet tiles with secondary backing of P.V.C The rate shall include cutting, trimming, fixing, and clearing away of residual material to a location as directed. The rate shall also include supplying and laying of a protective layer of PVC sheet of 50 microns thickness, held together with scotch tape. The laid carpet to be vacuumed after the removal of protective cover/on commissioning. In case the stains are observed in the carpet after the protective layer is removed, because of inadequate protection, the same shall be shampooed and made good to the satisfaction of the project managers. Skirting of above up to 4 inch All the power Rooms must be of antistatic anti-static vinyl tiles flooring of the required specification.

Providing and laying of 2mm thick anti-static vinyl tiles of approved quality and colour, of Armstrong or equivalent make in areas as indicated in the detailed drawing. The anti-static surface resistance shall be as per STP standards. This shall also include providing copper grid work connected to the earthing as an additional connectivity to achieve anti-static properties. The sample of the anti-static vinyl tile shall be approved by the Architect. Cost to include copper earthing strips at every 90cm spacing and 3" aluminium skirting.

d. **Partitions and walls:** Providing and fixing minimum 132 mm thick 2 hours fire rated gypsum board partitions with 2 Nos. x 15mm thick fire line board on both sides of 72mm GI floor channel and 70mm GI stud as per specifications. Suitable smoke seals should be used. Fire line boards should conform to IS:2095 – 1996-Part-I. This item includes all tools, tackles, material, Labour, fixture adhesives sealants etc. for the complete work.
   i. **Fire Rating:** Use minimum 1-hour fire-resistance-rated walls for IT rooms; doors should be ¾-hour rated.
   ii. **Material Selection:** opt for non-combustible materials like gypsum board with metal studs, concrete panels, or modular fire-rated partitions.
   iii. **Smoke & Heat Containment:** Install automatic fire/smoking dampers in air ducts passing through partitions.
   iv. **Modular Enclosures:** For flexibility and energy efficiency, consider modular wall systems that support hot/cold aisle containment and physical security.
   v. **Compliance & Certification:** Ensure all materials and designs comply with local fire codes, and are certified under standards like UL 60950-1 for IT equipment safety

e. **Doors and Windows:** The doors requirement is given in the table below:

Sl. No	Door details	Type
01	Main entry disaster recovery Centre	Double leaf fire rated door 1500x2400
02	Main entry ups/battery	Double leaf fire rated door 1200x2400
03	Main entry BMS room	Single leaf fire rated door 1000x2400

The above list is indicative only & the bidder may propose additional doors of desired specifications if required as per the actual site conditions.

There will be Designer privacy film on every glass Door. The design shall be approved by OCAC. Bidder may decide to erect/not erect wall on the support area side east side as per requirement of their design. However, all the openings on the top and bottom of the gap between the glass fade and the building must be closed with MDF board for ply board with smooth finish.

f. **Paint and polish:** Server farm area walls, power room wall BMS Rooms, ups/battery room have to be must have premium emulsion paint of min 3 coats over and above putty and primer wherever required. All metallic exposure parts must be painted with Anti-Rust enamel Paint.

g. **BMS Room Furniture**: Should be rectangular desk-based workstation of standard fitting of size

1000mm x 600mm, height 750mm. 25mm thick tabletop at 750mm level finished in laminate with 2mm thick PVC edge binding. Spines of the panel should have raceways to carry the LAN & electrical cables at two levels. The workstation should include a FABRIC pinup board and glass writing board. Workstation shall at least have 2 nos. LAN ports, 1 USB-B &1 USB-C port for charging and 4 nos. 5/15 Amp power sockets. The design, colour and quality shall be approved by the purchaser.

h. **BMS room Chair:** BMS room chair must be ergonomically designed in such a manner that long hour seating does not become tiring.
i. **Shoe Rack:** A shoe rack must be supplied with 20 pairs of slippers to be placed near the entrance of the server room.

***Note:** Bidders shall visit the site to assess and validate all specified requirements. The above-mentioned are minimum requirement, bidder to access and quote, no additional charges will be borne by the OCAC.

Diesel Generators

The required power of 750KVA from the transformer till the DR-DC area including main LT panel.

a. For captive power back-up system, Diesel power generators must be proposed with all its ancillary supplies such as Buffer storage and Day tanks, Exhaust system, Fuel piping system etc. The diesel generator must be Disaster Recovery Centre continuous type.
b. It is proposed that 500kVA Disaster recovery centre continuous rated diesel Generator set is offered.
c. The generators will be in N+1 configuration.
d. Exhaust systems need to be erected as per CPCB. norms. In case a self-supporting structure is required for exhaust, the same must be proposed.
e. Adequate fuel pump mechanism is required for pumping fuel from the tank to the generators. The pumps and pipes must be redundant & as per desired standards.
f. Intrinsically safe fuel meters must be installed on the fuel pipeline with provision of sending real time consumption data to monitoring tools such as DCIM.
g. Basal body temperature (BBT) of suitable rating from the generators may be installed with appropriate support structure as per site requirement
h. Fresh DG foundation needs to be created as per OEM requirement.

MV Panels

a. The entire building must have a comprehensive power distribution design where the LT panel will be an integral part. The same will be used to feed power to the critical and non-critical areas. These panels may include Main LT panels, Distribution panels, Power factor panels etc. For the server farm area, there will be two LT panels placed in different rooms to provide physical redundancy. The panels will be fully compartmentalized (form 4b) and modular.
b. Bidders need to design the capacitor bank & propose installation of desired rating of capacitor banks.
c. The DG sync panel shall be installed near the DG yard.
d. LT panel should not be single point failure. It should be in redundant LT panels to be proposed

by the bidder.

e. All interconnecting cables must be proposed. All panels must be typing 4B from factor panels.

f. The bidder should propose additional auxiliary panels/DBs as per the disaster recovery Centre standard such as Emergency lighting DB, Lighting DB, Raw power DB etc. for better distribution of power in a Disaster Recovery cum Data Centre facility.

g. The DG Synchronization panel as per the scheme is proposed to be placed near the DG. Since it will be outdoors, the panel must have an impressive protection level not less than IP 66. This should be placed on a PCC foundation 1 meter above ground level.

UPS & Battery Systems

a. For uninterrupted power supply UPS with battery bank of required rating must be proposed for the Critical and Non-Critical load. The UPS must be modular and can be scaled up vertically and horizontally including static bypass switch. A separate UPS bank with VRLA batteries must be provisioned for non-IT equipment.

b. UPS systems will be in N+1 configuration.

c. The UPS system will be placed in two different UPS rooms with its individual battery banks.

d. The UPS system must be connected to DCIM for real-time performance monitoring.

e. UPS system must be modular in such a manner that the modules can be replaced safely without any arching.

f. The Bidder must submit a battery calculation sheet.

g. The bidder must propose UPS systems with minimum footprint.

h. The UPS must be with maximum efficiency. The output power factor must be closest to unity.

Cable, Bus Bar Trunks, and Terminations

a. Cables and Bus bars of different types and sizes as per the required design for connecting all required components from source to load or vice-e-versa with termination at both ends. Indoor bus bars to be installed inside the server farm for Rack power.

b. The UPS Input & Output cables till the Rack and the cables feeding Cooling machines shall be Copper & rest all cables shall be Aluminium.

c. The bidder must submit cable schedule as per the following format.

Cable Schedule

The bidder must submit a detailed schedule of cables and bus bars in the following format.

Sl. No	From	To	Max Amp	Cable Ampacity	Cable Size in sq. mm	No of cores	Type of core	No of runs	Insulation	Length	Qty
01	A	B	500	700	185	3.5	AL	2	XLPE	50	100

Description of headers:

a. From – The point from where cable/BBT is starting to – The point from where the cable/BBT is ending

b. Max Amp – The maximum load current per phase that the cable/BBT must carry Cable Ampacity – The maximum current per phase the cable/BBT can handle Cable Size: Size of the cable in sq. mm

c. No Cores: Number of cables per segment (e.g. 1, 2, 3, 3.5, 4 etc.) Type of Core: The metal type used (e.g. Aluminium, Copper)
d. No of Runs: Number of cable segments that must run between two segments Insulation: Insulation of the cable (e.g. PVC, XLPE etc.)
e. Length: The distance between starting and end point of the segment. Total cable quantity (Length x no of Runs)

Cable/Conduit/Bus bar Laying

a. The bidders are strongly advised to maintain data consistency between Electrical Single line diagram, Cable schedule and Bill of quantity always in the solution document. The Electrical Single line diagram must be prepared in detail showing all the components. All the components must be uniquely labelled.
b. All cabling inside the server hall will be over the top of the racks.
c. Track busway continuous BBT must be used for IT racks. From the UPS Output panel till the end feed unit of bus bar cable will be used on cable tray.
d. All conduits inside the server hall will be MS type. No PVC conduct will be accepted. However, the conduits if laid inside the wall can be PVC with FRLS type.
e. There must be raw power provisions inside the server hall at regular intervals for facility maintenance.
f. All cables must be tagged with unique names. The tag must be long lasting and durable. Tagging must be on both sides.
g. All cable entry to the panels must be with double compression glands. The glands must be chosen as per the cable core metal.
h. Cable installation must be as per IE rules considering pull strength, bending radius and insulation class.
i. All outdoor cables may be factory tested for insulation strength. However, standard test certificates will be accepted. All outdoor cables must be Cross-Linked Polyethylene (XLPE), and all indoor cables must be Flame Retardant Low Smoke (FRLS) Type.
j. All the wiring in the support area must be concealed. Sub-mains must be laid in PVC raceways buried under the Plain Cement Concrete (PCC) floor. The distribution to the desks must be through the furniture raceways from bottom.
k. There must be junction boxes on the floor under the carpets or on vitrified tile floors. It must be concealed but should be openable for maintenance.
l. UPS output cabling must have double neutral. Single core Cu cable must be used.
m. Cable end point insulation must be by heat shrink sleeved. Taping will not be allowed.

Illumination

a. Lights of various types as suitable for different floors including critical and non-critical areas are required to be done. Lux level inside server farm to be 500 lux measured at 1m from ground at all areas. Other areas should have 300 lux. Lux Level Map from manufacturers must be submitted before execution.
b. Bidder must propose LED lights of different sizes as suitable and approved by OCAC.
c. All the lights will have to have the occupancy sensors inside the Disaster Recovery Centre.

d. Bidder may propose different sizes of light as per the suitability and ambience required.
e. The light fixtures in the support area will be recess mounted on the ceiling. The lights on the server hall and power room may be suspended from the ceiling without compromising the aesthetics.
f. The size of fixtures can be chosen by the bidder so that the looks and ambience is not compromised

Wall Outlets, Outlets for Racks, Receptacles:

a. End point power outlets are required for all load points depending upon type and redundancy.
b. The wall distribution panels must be double door type and recessed on the wall.
c. The looping of raw power and UPS power points for the user is allowed. However, there were no more than 3 raw power points and more than 2 UPS power points looped for a single circuit.
d. The receptacles on the wall and on the desk must be highly durable and multi-pin type. Each desk must have 3 sockets, one for raw power and two for UPS power with proper levelling.

Grounding/ Earthing

a. Earth pits of different types, grounding bus bars/strips, Equi-potential grid for the critical area.
b. All earth pits irrespective of Neutral or Body must be Chemical Earthing.
c. Earth pits may be required for UPS systems and other items inside the Disaster Recovery Centre. The same may be proposed by the bidder.
d. The server hall must have grounding mesh in terms of copper strip or braided copper wire laid on the ground or above the ground on a matrix fashion to provide equipotential grids for all the equipment.
e. Each metal item inside the Disaster Recovery Centre must be grounded.
f. The earth strips must be copper for Neutral and GI for Body pits. All the Copper & GI earth strips must be insulated.
g. All the critical equipment (like UPS, DG set, Iso. Transformers etc.) earthing must be with copper strips of required specification.
h. All the earth pits must be covered with required standard of earth pit covers with recommended load bearing specifications of OEM.
i. Interconnection of earth strips must be by welding in alloy material or by non-corrosive nuts and bolts.
j. Earth pits must be connected to the ground for redundancy and equip-potential.
k. The complete earth works like excavation, refilling & RCC covers of the desired standard will be in bidder’s scope.

Cable Pathways

a. Various pathways such as underground trench, cable trays, Raceways, junction boxes, ladder trays, and Cable baskets required to be there for the entire facility.
b. For trenches, the complete earth works like excavation, refilling & RCC covers of the desired standard will be in bidder’s scope
c. Cables must be taken to the Disaster Recovery Centre from the ground area by designated path / route only. All cables must be tagged.
d. Inside the Disaster Recovery Centre all cables must run over the rack on cable tray.

e. Inside the Electrical room all cables must run cable trays over the top.
f. Cable tray must be factory made with pre-galvanized finish.
g. Cable fills in any tray must not be more than 60%.
h. All cables and wiring must be neatly dressed and tagged with unique identity.
i. The power cable must be used for taking cables from outside to inside the floor. While working on the shafts, adequate care must be taken not to disturb other cables running inside them.
j. In case of redundant path for taking cables from outside to inside of power room of disaster recovery Centre, a self-supporting structure may be erected outside but adjacent to the wall of the building made of off GI angles/members.

Wiring

a. Wiring of all load points, wall outlets, Lights, and all other points where connection is required.
b. All along the Disaster Recovery Centre area, wiring colour codes must be used for single phase, three phase and Ground. All wires and cables must be tagged with unique identity.
c. No jointing of cables or wires are allowed without proper factory-made jointing kit.
d. The bidder must submit the following in various stages of the project:
e. Complete unpriced BOQ according to the bidder's solution- To be submitted along with technical bid.
f. Single line diagram – To be submitted along with bid. The single line diagram has to be in detail showing unique notations for every component such as breakers, indicators, CTs, bus bars, cable rating etc.
g. Cable schedule as per the format. – To be submitted along with bid.
h. Lux level calculation – To be submitted along with bid.
i. Cable and panel datasheets – To be submitted long with bid.
j. Shop drawings for cable pathways, wiring, and RCP – Before execution.
k. Coordinated drawing – Before start of execution.

Precision Air Conditioning

i. Technical areas such as Server farms and Power rooms will have precision cooling systems.
ii. The server farm is proposed to have 21 racks where each rack size is considered to be 800mm x 1200 mm.
iii. There will be cold aisle containment for racks.
iv. All other racks will also have in-row cooling as well. It is up to the bidder to design and suggest either hot aisle or cold aisle containment. The room void load (max room temp to be 30+/-2 degree) must also be considered while calculating and sizing the in-row PAC rating. That the ambient temperature has to be as per Uptime's requirement. The return temp must be considered as per the supply and load. Accordingly, the number of PAC units on a POD must be calculated.
v. The cold aisle containment should be proposed in such a manner that a maintenance corridor is created in between the PACs and the rack row. This can be possible by proposing sliding doors on the one side (PAC side) hot aisle of the row.
vi. Fan section of in row PAC should be independently connected to utility UPS in such a manner that during EB power failure the fan of PAC should run without interruption.
vii. All the refrigerant piping must run on the side of the wall below the raise floor.

viii. Pipes have to be properly insulated. The exit of the pipes on the wall must be through factory made sealing blocks with fire rated material.

ix. The outdoor stand to be placed as per the standard practice.

x. Adequate safety barriers must be taken care of on the platform on all sides. A portable fire extinguisher must be installed on the platform.

xiv. Humidifier line can be taken from building water pipeline with a valve.

xv. For the DR-DC support area, the entire area to be provided with a VRV/VRF system where the outdoor units will be placed on the ODU platform.

xvi. Bidder must submit a heat load calculation along with detail BOQ in the technical bid.

xvii. Bidder must submit a detail table of selection of various ratings of indoor units with their cooling capacity in terms of CFM, power consumption and size.

xviii. The power room will have PAC units (floor standing) without heater and humidifier. Bidder must consider the equipment heat load, room area load and latent heat for selection of rating of the units.

xix. Power room PAC will be redundant as per Uptime guidelines.

xx. Bidder has to submit a detail bill of material with prices for each and every item.

xxi. All the AC (PAC & VRF) units must have provisions to connect to DCIM. It must also be connected to the fire alarm system for tripping during fire.

xxii. Bidder must propose thermal insulation (under deck insulation) on the server hall floor and ceiling and on the support area. The thickness of the insulation must be min 23 mm and material to be nitrile rubber.

xxiii. It may be possibility that the pipes from the indoor units of the DR-DC support area have to run through the server hall under the raise floor. This may be avoided. In case it is a must then, the same may be done with proper workmanship.

xxvi. Power to each PAC indoor units will be from two different HVAC panel. The bidder may propose an ATS with two inputs and one output for each PAC in case the PAC do not have provisions for 2 inputs as per best practice.

Safety, Security, Surveillance and Monitoring System

Addressable Fire Alarm System (AFAS)

i. Entire facility should have fire detection, annunciation & Alarm system. Different types of detectors such as fire, smoke and heat detectors or combinations of all to be installed and wired to a control panel in a zonal fashion.

ii. This system must be integrated with the central monitoring system. The fire panel must have redundant components inbuilt.

iii. The fire hydrant on the people support area side will have to remain connected to the main system.

iv. The nozzles of hydrant system in the support area should be extended to the false ceiling level.

v. The AFAS system will have manual call points, hooters, and all other accessories for complete fire detection system.

vi. There must be a provision to connect the system to the building’s main fire alarm system

vii. Illuminated exit signs must be installed on all possible points.

viii. Emergency evacuation laminated chart of A3 must be displayed at all important locations.
ix. A fireman's boot, safety jacket, goggles, gloves, hammer, Axe etc. must be kept in a steel fabricated case with front face visible.
x. Detectors must be placed on all voids.
xi. A detailed table of items must be submitted with quantity and type of items.
xii. The design will be as per NFPA and local fire codes whichever is applicable.
xiii. Hooter with strobes is to be installed at least 4 points in the Disaster Recover Centre area.
xiv. The bidder should submit a detailed design sheet as per the OEM recommendations along with the bid.

Aspiration Smoke Detection System or Very Early Smoke Detection System

i. VESDA system may be required in the server farm area & power rooms for early detection of smoke with a facility of alarm.
ii. The system must be digital, and the panel must be installed inside the BMS room
iii. The sampling pipe has to run over the PACs and below the floor if required.
iv. The detectors have to be placed inside the containment as well.
v. The bidder should submit a detailed design sheet as per the OEM recommendations along with the bid.

Gas Based Fire Suppression System

i. The technical area such as Server farm area, UPS room, Panel and battery room must have a fire suppression system with an alarm such that in case of fire the gas agent gets released through the nozzles and suppress the fire fully without damaging the electronic devices.
ii. There will be three separate suppression systems. One for server hall and one each for 2 power rooms.
iii. The suppression nozzles must be placed on all voids and including the inside of containment.
iv. The cylinder has to be seamless type.
v. In case there is a flooding of gas during execution and before the site handover bidder needs to replace the gas at its own cost.
vi. Placement of cylinder bank is shown on the layout.
vii. The gas-based suppression system must be integrated into the fire alarm system
viii. Pressure on the cylinder must be maintained throughout the contract period.
ix. There should be provision for integration & monitoring of cylinder level pressure in DCIM.
x. The bidder should submit a detailed design sheet as per the OEM recommendations along with the bid.

Close Circuit Television System (CCTV)

i. Surveillance of inside and outside of the facility must be done with different types of IP cameras such as fixed/Dome/PTZ high-definition cameras with facility of motion-based recording for one month in inbuilt HDD. The CCTV system should cover all the areas concerned with DR-DC.
ii. The cameras inside the server hall to be for all the aisles including the containments.
iii. No area must be left out of surveillance except the washrooms, manager cabins, and bunk bedroom.

iv. The staircase, ODU platform, DG area, HSD tank area, Utility area must be covered under CCTV system
v. All cameras must be powered by CAT6A from POE switch.
vi. At least three PTZ cameras must be offered for outdoors in addition to fixed cameras.
vii. Recording must be archived for 6 months in an external drive supplied by the bidder.
viii. At least a month's recording must be available in NVR in inbuilt HDD.
ix. All recordings must be motion based inside the server hall. However, inside the Power rooms it must be continuous.
x. The boundary wall behind the building on the Disaster Recovery Centre portion also needs to be covered under CCTV.
xi. The bidder should submit a detailed design sheet as per the OEM recommendations along with the bid.

Access Control System

i. Access to the facility must be controlled. Dual Electronic authentication on each entry to the critical area must be there. Physical access control (manned) also must be configured wherever required. The scope will include all the access control system mechanisms including authentication, prioritization, and monitoring. Turnstiles, flap barriers, swipe barriers are part of access control system scope.
ii. All the doors have to be controlled by access control hardware and software.
iii. All doors must have an entry and exit card reader.
iv. Server hall entry must be with biometric access from people's entry side and card reader entry from material entry side.
v. There has to be a full height turnstile on the entry of the server hall with an adjacent fire rated glass door.
vi. A full-height metal detector must be installed near the entry.
vii. An x-ray baggage scanner must be installed at the entry of the facility.
viii. A comprehensive visitor management system must be installed with computers, cameras, and card printers near the security area at the entry of the facility.
ix. Access control software and required computer has to be a part of the scope of the bidder.
x. A detailed design sheet as per OEM recommendations must be submitted along with the bid

Water Leak Detection System

i. Detection of water and other liquids at the pipes that are used for flow of the same or at the floors wherever there is possibility of water or liquid leakage with detection and alarm system
ii. The water leak detection cable must be run near all water pipelines inside the server hall and power room.
iii. Water leak detection system must be digital type with a hooter connected to the system.
iv. The complete system shall include an electronic System control panel, multiple control modules, distance type sensing cable and all required auxiliary accessories (such as hold down clip & Tag/Label for the sensing cable).
v. This system shall detect and locate multiple leaks simultaneously as well as cable break & power failure and activate the control panel alarm relays. The sensing cables shall be of such construction

that no metallic parts shall be exposed to the environment. The system shall be provided with the flexibility of custom "cut-to- length" sensing cable to meet the exact length requirement at each area of protection and with pre-connectors sensing cable components.

vi. Water leak detection systems must have capabilities to integrate with monitoring tools like DCIM.

vii. A detailed design sheet as per OEM recommendations must be submitted along with the bid

Rodent Repellent System (RRS)

i. Ultrasonic frequency based electronic system to repel rodents from the floors with help electronic wave emitters.

ii. The satellites of the RRS to be installed in all voids in the server hall, support area and power room.

iii. The RRS must be capable of integration with DCIM tool for monitoring the health of satellites & Transducers.

iv. A detailed design sheet as per OEM recommendations must be submitted along with the bid.

Data Centre Infrastructure Management Tool

A comprehensive tool to monitor all the services and products installed in the facility. All the field devices must be monitored though DCIM. Bidder to propose integration with the proposed DCIM system.

Visitor Management System

A comprehensive visitor management system needs to be in place for the proposed Data Centre. This must be image-based access. The software must be integrated with the Door access control system for unified authentication. Every visitor will be issued an Id card. The required hardware and software such as computer, a-card printer, camera, and software are part of the bidder scope.

Note: The bidder is not required to submit the drawings for any of the above systems with the bid. However, following documents are mandatory

- Design Sheet as per OEM recommendations.
- Bill of material with quantity and price.
- Datasheets.
- Compliance SOW and Requirement.

Network Passive Infrastructure, Racks, IPDU, etc.

- Fiber and copper cabling as per TIA/EIA guidelines
- Tier III compliant and Tier 4 ready design
- With standard certification.
- Fiber cabling will be through Fiber runner and copper cabling in the cable basket, all over the racks.
- All racks to be supplied are 800mm x 1200mm. All are perforated racks and 42U size.
- Each rack will have two numbers, iPDU's, those will be connected to DCIM for port level monitoring.
- The iPDU's will be connected to the tap of box of track busway system
- Each row must be provisioned with a network cum passive rack at end of the row
- Copper cables must run on cable basket and Fiber on fibre pathways/fibre runner.
- Cat6A cablings on the support area must run under the floor on PVC raceway.

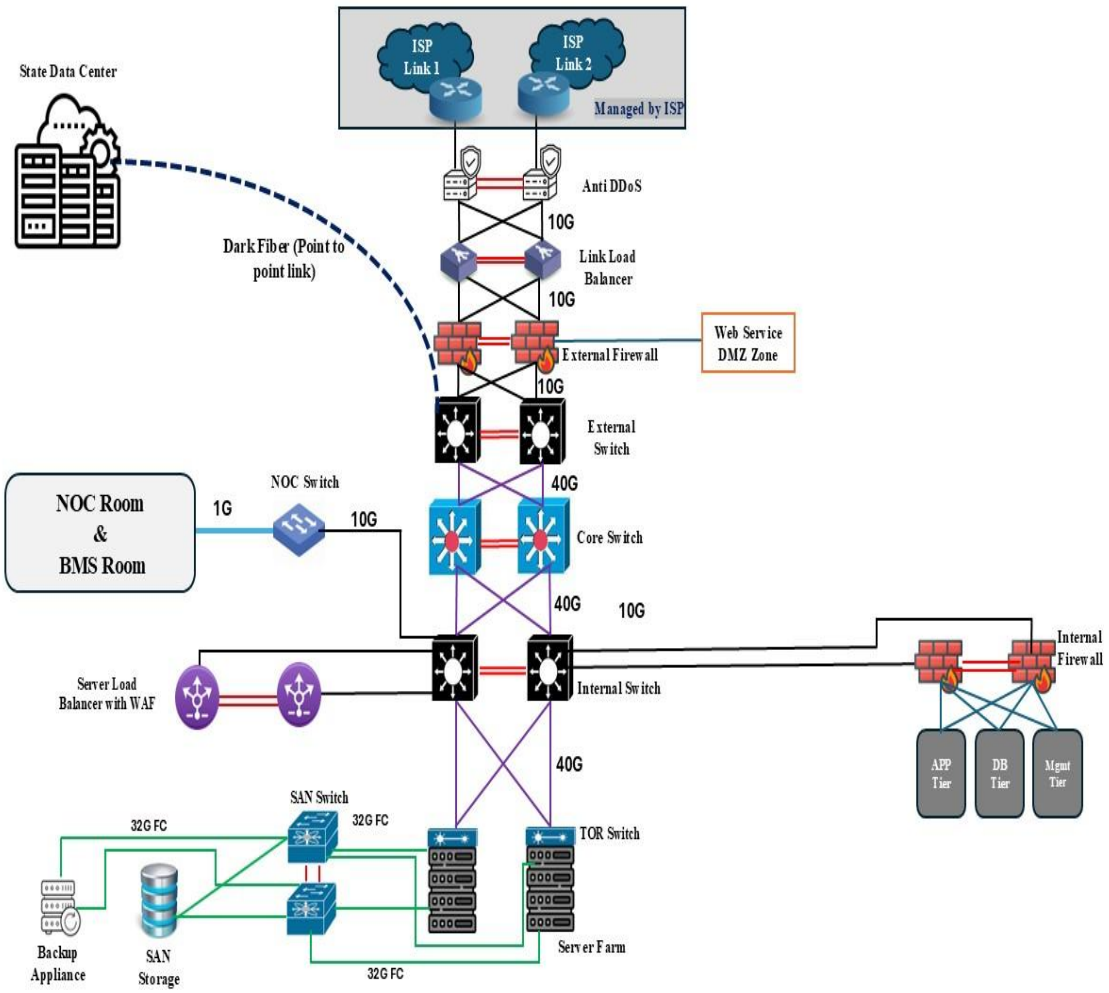
- Bunching and bending radius of the cable will be as per manufacturer standard.
- The racks that are not used or U space that is not used, will have blanking panels on them.

UPS

- Supply of UPS systems Unloading, shifting, Storing, Installation, Testing and Commissioning.
- Supply of Battery banks Unloading, shifting, Storing, Installation, Testing and Commissioning.
- Providing training to Client and maintenance team.
- Periodic maintenance.
- SLA adherence.
- Repair and Replacement if required.
- System Acceptance test at Factory and at Site. (full load condition).

9.2. IT Infrastructure requirements

Proposed Indicative Network Diagram of DR cum DC



The Next Generation DR-DC aims to meet OCAC's functional requirements as follows:

i. **Rapid Service Provisioning:** Enable prompt availability of services, minimizing administration efforts and bureaucratic obstacles.

ii. **Cyber Security**: Ensure a robust security framework, acting as a distributed layer 2 switch, Layer 3 router, and Stateless distributed firewall. Implement a zero-trust policy model to safeguard against various attacks, such as Unauthorized Access, Man-in-the-Middle attacks, Replay Attacks, Data Disclosure, and Denial of Service.

iii. **Consistent Services and Manageability**: Ensure consistency in manageability, troubleshooting, and security across physical and virtual networks to streamline administrative efforts and mitigate errors.

   a. Multi-vendor Service Integration: Validate seamless operation of infrastructure components from various vendors, covering security, load balancing, virtualization, and storage.

   b. Network Fabric: Employ a two-tier design architecture adaptable to changing enterprise needs. Leaf and Spine architecture, ensuring better utilization of the switching fabric. Establish redundant dark fiber connections linking existing and proposed DR-DC.

   c. Compute: Implement a high-density compute setup with next-generation rack servers capable of Anything-as-a-Service deployment. Propose detailed quantity for the provisioned cloud servers.

   d. Visibility: Ensure deeper visibility into the fabric, enabling efficient monitoring of latency, packet drop, and traffic across the entire data Centre infrastructure.

- **DR-DC Core Layer & Aggregation Layer**

The data centre core connects to the aggregation layer using high-speed Layer 3 links. The data centre networks are summarized, and the core injects the default route into data centre aggregation. The data centre core layer is a best practice component of larger data centre networks.

Core Switches should be included in the following features.

a. There should be scalable architecture with hot-plug redundancy for power supplies and fans/rotors.

b. Switch should support at least wire-speed full-duplex switching bandwidth to avoid any bottle neck.

c. Support 100Gig interface to meet future requirements.

d. Must support Virtual Extensible LAN (VXLAN) is a network virtualization technology scalability problem with large deployments.

e. Must offer Layer 3 Routing protocols like OSPF, BGPv4 along with IPv6 from day1.

- **Access Layer / Server Farm**

The data centre access layer's main purpose is to provide Layer 2 and Layer 3 physical port density for various servers in the Disaster Recovery centre. In addition, data centre access layer switches provide high-performance, low latency switching and can support a mix of oversubscription requirements. Advantages of Layer 2 access are support for NIC teaming and server clustering that requires network connections to be Layer 2 adjacent or on the same VLAN with one another.

Access Switches should be min below features.

a. Should have required 10Gig access ports and 100Gig for uplinks to core switch with hot-plug redundant power supplies and fans/rotors.
b. Must support Virtual Extensible LAN (VXLAN) is a network virtualization technology scalability problem with large deployments.
c. Must offer Layer 3 Routing protocols like OSPF, BGPv4 along with IPv6 from day1.

Go-Live Preparedness and Go-Live

a. SI shall prepare and agree with OCAC, the detailed plan for Go-Live (in line with OCAC implementation plan as mentioned in RFP).
b. SI shall define and agree with OCAC the criteria for Go-Live.
c. SI shall submit signed-off FAT report (issue closure report) ensuring all issues raised during FAT are being resolved prior to Go-Live.
d. SI shall ensure that Go–Live criteria as mentioned in User acceptance testing of Project are met and SI needs to take approval from OCAC team on the same.
e. Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

9.3. Handholding and Training Phase

To strengthen the staff, structured capacity building shall be undertaken for identified resources of OCAC and stakeholder departments. It is important to understand the training needs to be provided to each staff personnel of NOC Centre, DR-DC, BMS. These officers shall be handling emergency situations with very minimal turnaround time. The actual number of trainees will be provided at design stage.

a. SI shall prepare and submit detailed Training Plan and Training Manuals to OCAC for review and approval.
b. Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
c. SI shall also be responsible for full capacity building. Training and capacity building shall be provided for all individual modules along with their respective integrations.
d. Types of Trainings: Following training needs is identified for all the project stakeholders.

- **Administrative Training**
  a. System Administration Helpdesk, BMS Administration etc.
  b. Master trainer assistance and handling helpdesk requests etc.
- **Senior Management Training**
  a. Usage of all the proposed systems for monitoring, tracking, and reporting,
  b. MIS reports, accessing various exception reports
- **Post-Implementation Training**
  a. Refresher Trainings for senior officials
  b. Functional/Operational training and IT basics for new operators
  c. Refresher courses on System Administration
  d. Change Management programs.

9.4. Operations and Maintenance

- **Operation & Maintenance of OCAC DR-DC**

The Bidder is responsible for Disaster Recovery Services to ensure continuity of operations in the event of failure of primary DC. The Bidder shall design and document an efficient DR solution in line with the requirements of the project and as per the "RPO of 30 Minutes" and "RTO of 1 Hour" requirements. The Bidder shall analyse relevant details before designing the DR Solution and offer dashboard to monitor RPO and RTO.

- **Switchover Strategy**

a. This strategy should include the components of the system that come into play when a planned switchover is made to the DR site for drill or planned maintenance purposes
b. During DR system testing / drills, planned maintenance of the equipment at the primary site, and other similar conditions, a planned auto switchover might need to be made to the DR site
c. Switchover will be a planned activity. It might need to be executed at short notice in the case of emergent maintenance needs.
d. There should be no data loss in case of a switchover. Switchovers should be possible for any one application or for all applications simultaneously.

- **Switchback Strategy**

This strategy should include the components of the system that come into play when system operation switches back to the primary site after being operated for a time from the DR site. The following two cases should be covered. Complete Disaster (destruction of equipment / data at Primary site or interruption in service of long duration): In this case, the primary site must be set up afresh.

a. Partial Disaster (interruption of service from primary for less than 30 days without destruction of equipment / data at primary site): In this case, the primary site has to be started up in sync with the DR site
b. Switchback from planned switchover: In this case, the primary site has to be started up from the state that existed at the time of switchover, but the overall process should be smooth

As soon as the facilities at the primary sites have been restored, the applications need to be switched back to the primary sites from the DR site

a. Switchback should be a planned activity. There should be no data loss in the event of a switchback.
b. In case of Partial Disaster as described in para above, "primary – primary conflict" between the DR and primary site at the time of primary system restart should also be resolved automatically.

Particular attention should be paid to the review of the recovery equipment configurations to ensure that the business has the required equipment to restore business functionality as quickly and smoothly as possible. These reviews will require the time and attention of all Plan holders and team members, especially those that have hardware and network responsibilities.

9.4.1. Management of DR-DC

The selected bidder will provide 24 x 7 x 365 operating and maintaining services for a period of 5 years from the date of Go Live for DR-DC. SI needs to deploy requisite mix of L1, L2 and L3 resources (on

24X7 basis) for management of entire ICT infrastructure deployed at DR-DC. All resources deployed in the project should be employees of SI and be Indian citizens subject to requisite approval from OCAC. All the required resources proposed for the project need to be dedicated to the project. Any change in the team once deployed will also require approval from OCAC. It is expected that resources have a proven track record and reliability. Considering the criticality of the project, OCAC may ask for security verification (Police verification) of every resource deployed on the project and SI need to comply the same before deployment of the resource at the project. At all times, the SI need to maintain the details of resources deployed for the project to OCAC and keep the same updated. A detailed process in this regard will be finalized between OCAC and SI. The SI shall maintain an attendance register for the resources deployed. Attendance details of the resources deployed also need to be shared with DR-DC monthly. DR-DC reserves the right to interview resources deployed for Operations and maintenance and assess the suitability of the resource for the role. In case a resource is not found suitable, SI will change the resource on request of DR-DC. SI shall comply with this.

The scope of work for Non-IT & IT ICT infrastructure and maintenance includes the following:

1. Non-IT management Services
2. System Administration and Management Services
3. Network Management Services
4. Server and Storage Administration and Management Services
5. Security Administration and Management Services
6. Physical security services
7. Backup & Restore Services
8. Helpdesk Services
9. Database Management
10. Preventive Maintenance Services
11. Corrective Maintenance Services
12. Asset Management Services
13. Configuration/ Reconfiguration Management Services
14. Vendor Management Services
15. EMS/NMS or other system
16. Threat Management
17. Certifications
18. Patch Release Update management (patch update for all software components possible and must give a report every fortnight to OCAC)
19. DC operations to be following industry leading ITSM frameworks like ITIL,
20. ISO 20000, ISO 22301, ISO 9001, ISO 27017 & ISO 27001
21. Ensure compliance with relevant SLA’s
22. 24x7 monitoring & management of availability & security of the infrastructure and assets.
23. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process.
24. Ensure overall security – ensure installation and management of every security component at every layer including physical security.

25. Prepare documentation/policies required for certifications included in the scope of work.
26. Preventive maintenance plan for every quarter
27. Performance tuning of system as required.
28. Design and maintain Policies and Standard Operating Procedures
29. User access management
30. Other activities as defined/to meet the project objectives.
31. Updated Documentation.
32. Utilization Threshold for balancing performance and energy efficiency.

Note: Recommendation for CPU /Memory Utilization Threshold: 60-70%.

During operations phase the SI needs to submit proof of renewal of support for all IT infrastructure products and other system software's for whom it is mandated to have OEM support. This needs to be submitted on an annual basis and needs to be verified before release of 2nd quarter payment of each year.

9.4.2. System Maintenance and Management

SI shall be responsible for tasks including but not limited to setting up servers, Network, security devices configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It should be noted that the activities performed by SI may also be reviewed by OCAC.

SI shall provision skilled and experienced manpower resources to administer and manage the entire system at the Disaster Recovery Centre.

a. On an ongoing basis, SI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
b. SI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.
c. SI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with DR-DC and based on the industry's best practices/frameworks. SI shall also create and maintain adequate documentation/checklists for the same.
d. SI shall be responsible for managing the usernames, roles, and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. SI shall be required to set up the directory server. Logs relating to access to the system by administrators shall also be kept and shall be made available to DR-DC on a need basis.
e. SI shall implement a password change mechanism in accordance with the security policy formulated in discussion with DR-DC and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.
f. The administrators shall also be required to have experience in the latest technologies to provide the existing and applicable infrastructure on a requirement-based scenario.

9.4.3. Network Administration

a. Network Switches/Routers shall support all the relevant routing protocols like BGP, OSPF, IPsec (site to site) etc.
b. The solution shall have features to create and manage virtual networks, switches, routers,

and other networking components.

c. The solution should have the ability to dynamically scale network resources up or down based on changing business requirements and traffic patterns.
d. The solution should have a centralized management portal or dashboard to provision, configure, and manage network resources.
e. The solution should have a feature to control and prioritize network traffic, ensuring that critical applications receive the necessary bandwidth and performance. (QoS)
f. The solution should have traffic optimization features, such as load balancing and content delivery, to improve application performance and user experience.
g. The solution should have real-time monitoring and analytics tools to gain insights into network performance, identify bottlenecks, and troubleshoot issues.
h. The solution should have Built-in redundancy and failover mechanisms to ensure network availability and minimize downtime.
i. The solution shall have features to support compliance with industry regulations and data protection standards related to network security and data privacy.

9.4.4. Communication Link

a. Bidder shall provide or facilitate the links provisioning of DDoS protected aggregated (ILL) Internet Leased Lines / MPLS / P2P Links / IFTAS Links/ any other Links that are provisioned by OCAC in the near future.
b. The aggregated ILL should have a bare minimum of 2 ISPs with different backbones.
c. Bidder shall suggest and provide communication link layout of all locations considering redundant links.
d. Bidder shall provide dashboard containing live status of all links, bandwidth etc. of all locations.

9.4.5. System Administration

a. 24*7*365 monitoring and management of the servers in the DR-DC.
b. SI shall also ensure proper configuration of server parameters and performance tuning on a regular basis. SI shall be the single point of accountability for all hardware maintenance and support the ICT infrastructure. It should be noted that the activities performed by SI may be reviewed by DR-DC.
c. SI shall be responsible for operating system administration, including but not limited to management of users, processes, preventive maintenance, and management of upgrades including updates, upgrades, and patches to ensure that the system is properly updated.
d. SI shall also be responsible for installation and re-installation of the hardware(s) as well as the software(s) in the event of system crash/failures.
e. SI shall also be responsible for proactive monitoring of the applications hosted.
f. SI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to always ensure their availability to DR-DC.
g. DR-DC shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall

undertake actions in accordance with the results of the log analysis. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals. SI shall refer to the CERT-In Guidelines to ensure their alignment with the practices followed.

h. The system administrators shall adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.

i. The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting.

j. The system administrators shall provide integration and user support on all supported servers, data storage systems etc.

k. The system administrators shall be required to trouble shoot problems with web services, application software, server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance, and activity of all servers.

l. The system administrators should be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.

m. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.

n. The administrators will also be required to have experience in the latest technologies to provide the existing and applicable infrastructure on a requirement-based scenario.

9.4.6. Storage Administration

a. SI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric/switches, tape library, etc. It should be noted that the activities performed by SI may be reviewed by DR-DC.

b. SI shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

c. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.

d. The storage administrator will be required to create/delete, enable/disable zones in the storage solution.

e. The storage administrator will be required to create/delete/modify storage volumes in the storage solution.

f. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.

g. To facilitate scalability of solution wherever required.

9.4.7. Database Administration

a. SI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.
b. SI shall be responsible for performing physical administrative functions such as reorganizing the database to improve performance.
c. SI shall be responsible for tuning the database, ensuring the integrity of the data, and configuring the data dictionary.
d. SI will follow guidelines issued by DR-DC in this regard from time to time including access of database by system administrators and guidelines relating to security of database.
e. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.
f. In addition to restrictions on any direct change in Data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.
g. The bidder shall undertake tasks of managing changes to database schema, creation/alteration of Database, disk space, storage, user roles, parallel distribution of data on storage to balance the I/O load.
h. The bidder shall periodically perform configuration checks and fine-tune the databases with respect to performance and proactive identification of potential problems.
i. The bidder shall provide performance monitoring, Maintenance and tuning of the databases on a regular basis as well as proactive health check-ups.
j. The bidder shall manage database upgrade, patch upgrade, patches, and updates as and when required with planned minimal downtime.
k. The bidder shall provide database performance and health reports to the OCAC as per standards.
l. The bidder shall assign rights on database for different users as per the requirement with necessary approval from OCAC or concern authority.
m. The bidder shall upload / create/alter users and assign privileges and Roles as per the requirement with necessary approval from OCAC or concern authority.
n. The bidder shall create logical objects/procedures/triggers/functions/packages in the database on the request of designer/developer of the applications.
o. The bidder shall be responsible for taking database backups, restoration, and recovery of Database as per the policy.
p. The backup policy would be framed by the system Integrator, keeping in view of the severity of different databases and MTTR. The policy would be approved by the Tendering Authority and gradually be updated as per requirements.
q. The bidder shall be responsible to maintain optimum utilization of all the equipment's w.r.t. database operations and keeping close watch on optimum performance of Hardware/OS/Network software/processes/database objects with detecting contention, wait

state and queue of jobs on the equipment's/memory objects/ processes/ Network/ I/O/ storage/concurrent load on the devices, etc. and implementing necessary measures to rectify the issues. A performance matrix must be provided by the System Integrator to the Tendering Authority monthly and when required.

r. The bidder shall implement monitoring of uses of devices/objects/users as and when required.

s. The bidder shall be responsible for implementing Database Audit of devices/ objects/ transactions/ users to identify malicious/suspected activities such as and when required through database tools or writing their own scripts.

9.4.8. Backup/Restore/Archival

a. SI shall be responsible for implementation of backup & archival policies as finalized with DR-DC. The SI is responsible for getting acquainted with the storage policies of DR-DC before installation and configuration. It should be noted that the activities performed by SI may be reviewed by DR-DC.

b. SI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups, and ensuring adherence to related retention policies.

c. SI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by DR-DC or in case of upgrades and configuration changes to the system.

d. SI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. SI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.

e. SI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fireproof cabinets (onsite and offsite as per the detailed process finalized by during project implementation phase).

f. BaaS shall include the automated and scheduled backup of data from various sources, including servers, databases, files, and applications

g. Bidder shall provide Backup solution with different features, like snapshots of VMs, Disk based backup, DB backup, File system, data and software maintained, incremental/ differential and full back up of all data, restoration of data as and when required

h. Bidder shall retain multiple versions of backed-up files and data, allowing users to restore to specific points in time

i. Bidder shall ensure Data deduplication techniques to reduce storage costs by eliminating redundant data across backups

j. The bidder shall also provide 24 x 7 support for file and volume restoration requests at the Data Centre(s).

9.4.9. Network monitoring

a. The bidder shall provide services for management of network environment to maintain

performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by bidder may be reviewed by OCAC.

b. The bidder shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
c. The bidder shall also be responsible for break fix maintenance of the LAN cabling within DR-DC etc.
d. The bidder shall also provide network related support and will coordinate with connectivity of DR-DC/other agencies who are terminating their network at the DR-DC for access of system.

9.4.10. Security Management

a. Performing security services on the components that are part of the DR-DC environment as per security policy finalized with DR-DC
b. IT Security Administration – Manage and monitor safety of information/data
c. Reporting security incidents and resolution of the same.
d. Proactively monitor, manage, maintain & administer all security devices and update engine, signatures, and patterns as applicable.
e. Managing and monitoring anti-virus, anti-malware, phishing, and malware for managed resources.
f. Ensuring 100 percent XDR coverage with patterns not old more than period agreed on any given system
g. Ensuring APT (Advanced Threat Protection)
h. Reporting security incidents and co-ordinate resolution
i. Monitoring centralized pattern distribution (live update) and scan for deficiencies
j. Maintaining secure domain policies
k. Secured IPsec/SSL/TLS based virtual private network (VPN) management
l. Performing firewall management and review of policies on at least quarterly basis during first year of O&M and then after at least on a half-yearly basis
m. Providing WAF (Web Application Firewall)
n. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/ software and alerting DR-DC as appropriate
o. Performing patch management using software distribution tools for all security applications including content management system, antivirus, and VPN
p. Providing root cause analysis for all defined problems including hacking attempts
q. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and provide the same to DR-DC
r. Maintaining documentation of security component details including architecture diagram, policies, and configurations
s. Performing periodic review of security configurations for inconsistencies and redundancies against security policy

t. Performing periodic review of security policy and suggest improvements
u. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected
v. Policy management (firewall users, rules, hosts, access controls, daily adaptations)
w. Modifying security policy, routing table and protocols
x. Performing zone management (DMZ)
y. Sensitizing users to security issues through regular updates or alerts – periodic updates/ Help DR-DC issuance of mailers in this regard
z. Performing capacity management of security resources to meet business needs
aa. Rapidly resolving every incident/problem within mutually agreed timelines
bb. Testing and implementation of patches and upgrades
cc. Network/device hardening procedure as per security guidelines from DR-DC
dd. Implementing and maintaining security rules
ee. Performing any other day-to-day administration and support activities

9.4.11. Compliance to SLA

The bidder shall ensure compliance to SLAs as indicated in this RFP and any upgrades/major changes to the software shall be accordingly planned by SI ensuring the SLA requirements are met at no additional cost to the DR-DC.

a. The bidder shall ensure compliance with uptime and performance requirements of project solution as indicated in the SLA and any upgrades/major changes to the Data Centre shall be accordingly planned by SI for ensuring the SLA requirements.
b. The bidder shall be responsible for the measurement of the SLAs at the Data Centre level as well as at the user level with the help of the enterprise monitoring tool on a periodic basis.
c. Reports for SLA measurement must be produced by DR-DC officials as per the project requirements.

9.4.12. Warranty support

a. The bidder shall provide comprehensive and on-site warranty / AMC support for 5 years from the date of Go-Live for the infrastructure deployed on the project. The bidder needs to have OEM support for these components and documentation in this regard needs to be submitted to DR-DC on an annual basis.
b. The bidder shall provide the comprehensive & onsite manufacturer's warranty with respect to proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. The bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
c. The bidder shall provide a performance warranty in respect of the performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

d. The bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period the bidder shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the DR-DC in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.

e. During the warranty period SI shall maintain the systems and repair/replace at the installed site, at no charge to DR-DC, all defective components that are brought to the bidder's notice.

f. The bidder shall carry out Corrective Maintenance for maintenance/ troubleshooting of supplied hardware/ software and support infrastructure problems including network (active/passive) equipment, security, and rectification of the same. The bidder shall also maintain complete documentation of problems, isolation, cause, and rectification procedures for building knowledge base for the known problems in centralized repository, accessible to DR-DC team as well.

i. Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions. The SI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.SI shall have to stock and provide adequate onsite and offsite spare parts and spare components to ensure that the uptime commitment as per SLA is met. Any component that is reported to be down on a given date should be either fully repaired or replaced by a temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). The SI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of Data Centre.

10. Project Bill of Quantity

The BOQ mentioned below is indicative. Bidder may visit the proposed location of the DR cum DC and propose the BOQ as per their solution. SI's are requested to share a detailed BOQ based on their proposed solution.

10.1. BOQ of non-IT & IT items

NON-IT INFRASTRUCTURE			
S. No	**Components**	**UOM**	**Qty**
1	Interior Works	Lot	1
2	Structural Works	Lot	1
3	Transformer with associated components (750 kVA)	Nos	2
4	Diesel Generator with associated components (500KVA)	Nos	3
5	Electrical Works - Electrical Panels, DG Sync Panel, Incomer / Outgoing cabling, PDUs, Earth Pits, Sockets, HSD Tanks, HSD Electrical panel, and wiring	Lot	1

6	Modular UPS - IT with associated components (400kVA)	Nos	2
7	UPS non-IT with associated components (40 kVA)	Nos	2
8	Precision Air Conditioner(40TR)	Nos	3
9	HVAC Works	Lot	1
10	VRV	Lot	1
11	Fire Detection	Lot	1
12	Fire Suppression	Lot	1
13	Security & Surveillance	Lot	1
14	Rodent Repellent	Lot	1
15	Access Control System	Lot	1
16	Water Leak Detection System	Lot	1
17	Building Management System	Lot	1
18	Rack & PDU (all the racks)	Lot	1
19	Structural Cabling (all the racks)	Lot	1
20	Passive items (Cat6 cables, Patch panels, IO, Patch Cord etc.,)	Lot	1
21	Civil Work if required	Lot	1

IT INFRASTRUCTURE

S. No	Components	UOM	Qty
1	Server Type-A	Nos	12
2	Server Type-B	Nos	2
3	STORAGE (2 PiB Usable)	Nos	1
4	SAN SWITCH	Nos	2
5	SWITCH TYPE 1	Nos	2
6	SWITCH TYPE 2	Nos	4
7	SWITCH TYPE 3	Nos	4
8	SWITCH TYPE 4	Nos	2
9	BACKUP APPLIANCE	Nos	1
10	BACKUP SOFTWARE	Nos	1
11	SERVER - BACKUP & UTILITY	Nos	1
12	VIRTUALIZATION	Nos	1
13	DB -MS-SQL – (4C License)	Nos	4
14	OS – Windows	Lot	1
15	DRM Tool (30 VM’s)	Lot	1
16	Tape Library	No	1
17	OS-Linux	Lot	1
18	Extended Detection and Response	Nos	250

19	NGFW – Internal	Nos	2
20	NGFW – External	Nos	2
21	DDoS	Nos	2
22	Link Load Balancer	Nos	2
23	Server Load Balancer with WAF	Nos	2
24	Observability Tool	Lot	1
25	Workstation	Nos	6
26	IP KVM Switch with Display (48-Ports)	Lot	1
27	Printer	Nos	2

"The Exchange Rate Variation (ERV) clause shall apply only in cases where the number of users increases after one year or where the contract period is extended beyond the original term of five (5) years. The base exchange rate shall be the RBI reference rate as on the last date of bid submission. Adjustment on account of ERV shall be applicable only when the exchange rate variation exceeds ±2.5%. Exchange rate fluctuations up to ±2.5% shall be borne by the bidder and no adjustment shall be payable for such variation".

10.2. Manpower Requirements

S. No	Components	UOM	Qty
1	Project Manager	Nos	1
2	Storage Administrator	Nos	2
3	Network Administrator	Nos	2
4	Cloud Administrator	Nos	2
5	Security Administrator	Nos	1
6	Database Administrator	Nos	1
7	System Administrator	Nos	2
8	Helpdesk Support	Nos	2
9	Datacentre facility engineer	Nos	3

Note: The above table represents only the O&M Manpower requirement. The listed resources to be deployed before the start of the O&M phase. During the Implementation phase SI must deploy requisite manpower to ensure timely completion of the project

10.3. Project Timelines

The project duration will be 6 months of Implementation after the Go-live it will be 5 Years of operations & maintenance i.e. in total it **is 5.6 years**

T is the date of signing of the contract

Deliverables/Milestones	Timelines
Inception Report	T+1 Month
Solution Designing	T+2 Month
Delivery of IT & Non-IT Infrastructure components	T+3 Months
Installation & Commissioning of IT & Non-Infrastructure components	T+5 Months
Final Acceptance Test & Go-Live of DR-DC.	T+6 Months
Operations and maintenance for 5-year payable quarterly	Go Live + 60 Months

10.4. Payment Schedule

For payment, the cost quoted by the bidder for Non-IT Infrastructure (A), IT Infrastructure (B), Other Cost (C) and Support services (D) in the commercial proposal shall be considered as Cost of implementation and maintenance of the DR-DC.

Sl.No.	Payment Schedule	Fee Payable	Remarks
1	Solution Designing - P0	10% of the cost quoted for implementation and maintenance of the DR- DC	On successful approval of the solution by the committee / OCAC appointed Nodal Agency
2	On Delivery of equipment and Site readiness- P1	20% of the cost quoted for implementation and maintenance of the DR-DC.	Payable on successful check of all the equipment by OCAC appointed Nodal Agency on Submission of respective invoices
3.	Successful installation of all the equipment & commissioning of DC - P2	30% of the cost quoted for implementation and maintenance of the DR-DC	On submission of approved Installation & commissioning reports Payable on final acceptance test
4	Go Live of DC - P3	35% of the cost quoted for implementation and maintenance of the DR-DC.	Against submission of quarterly Report
5.	Operations and Maintenance – P4	5% of the cost quoted for implementation and maintenance of the DR-DC in equal quarterly instalments (QGRs) for entire duration of the O&M Phase	Against submission of quarterly O&M Report.
6.	Manpower - P5	Equal quarterly instalments (QGRs) of the manpower support cost quoted by the bidder	Against submission of quarterly attendance sheet

11. Technical Specifications

11.1. Non-IT

11.1.1. UPS – 400 KVA

Sl. No.	Requirement	Mandatory / Desired	Compliance (Yes/No)	Cross Reference
1	Efficiency online mode to be ≥ 97 % along with PF Correction to Unity at Input & Harmonic Correction (THDI) to < 3% at Input and simultaneously Battery Charging also. From load range of 60 to 100%.	Mandatory		
2	Input Power Factor must be 0.99 at load >25%	Mandatory		
3	Total current harmonic distortion to be 3% or less at 100% rated load	Mandatory		
4	VRLA Battery and back up must be 15 minutes on full load per UPS at 0.9 load power factor considering mid of life of the battery. Battery sizing Calculation must be submitted duly endorsed by battery manufacturer. Battery sizing for backup calculation to be done considering End of life (EoL) for 10 years. Additional up to the 2 Battery bank should be commissioned for redundancy purpose of UPS backup as required.	Mandatory		
5	Battery System to be equipped with cell, module, bank level battery management system and to be monitored by Data Centre Infrastructure Management system with following certifications: Safety Cell UL1642, Module UL 1973, Seismic GR63 EMC IEC61000-6-2, 61000-6-4	Mandatory		
6	UPS must handle 100% unbalanced load	Mandatory		
7	▪ Nominal Voltage: ▪ Input: 380/ 400/ 415 VAC - Three Phase four ▪ wires + ground ▪ Output: 380/ 400, 415 VAC	Mandatory		

Sl. No.	Requirement	Mandatory / Desired	Compliance (Yes/No)	Cross Reference
	(Selectable) - Three Phase four wires + ground			
8	Each pluggable type, hot swappable and user replaceable Power module should have its own full rated rectifier, full rated inverter, static bypass switch & battery charging circuit.	Mandatory		
9	Each pluggable, hot swappable and user replaceable Power module should have its own full rated rectifier, full rated inverter & battery charging circuit. Static bypass switch should be for the Full capacity UPS for a single frame.	Mandatory		
10	Input Voltage Range: +/- 15% (On Full Load)	Mandatory		
11	No decrease in UPS capacity from 0.9 leading to 0.8 lagging of load power factor.	Mandatory		
12	Rectifier to be IGBT based and Inverter to be IGBT based (3 level or better) (Switching losses Shall be Less than 30% on IGBTs)	Mandatory		
13	The Modules should have Redundant variable speed fans and capable of maintaining the system in event of single fan failure.	Mandatory		
14	The Modules should be mounted on to safe back plane of separate AC and DC power without use of any interconnecting power cables.	Mandatory		
15	Noise level should be less than 75 dB on normal condition at 1 meter distance.	Desired		
16	Smaller footprint (Individual UPS Frame depth & width shall not exceed from 850 mm & 550 mm)	Desired		

Sl. No.	Requirement	Mandatory / Desired	Compliance (Yes/No)	Cross Reference
17	The UPS should have built in a facility through which it can be switched off immediately through a local switch or remote Emergency Power Off switch wherein the load is disconnected from the UPS under emergency conditions. Restarts are possible after manual inspection and removing the conditions of emergency and resetting the Emergency Power Off switch.	Desired		
18	UPS should have a wide choice of communication interfaces through SNMP / Modbus protocol using the RS232 / RS485 / Ethernet port.	Desired		
19	No deration in UPS capacity (KVA and KW) from 0 to 40ºC operating temperature	Desired		
20	The UPS should be **UL/CE** Listed.	Desired		
21	Phase Correction/Corrector required (Inbuilt or External)	Desired		
22	Back feed protection required (Inbuilt or External) at Mains as well as Bypass	Desired		

11.1.2. UPS – 40 KVA

Sl. No	Requirement	Mandatory	Compliance (Yes /No)	Remark (If any)
1	The UPS systems shall be sized to provide a maximum of 40kVA and a maximum of 36kW output at 0.9 output power factor.			
2	Load voltage and bypass line voltage will be 380/400/415 Vac, three phase and neutral. Input voltage will be 380/400/415 Vac, three phase.			
3	The battery system shall have a capacity of 30 kW for at least 15 minutes at 25ºC.			
4	The UPS to have minimum footprint and without isolation transformer.			
5	The battery will be installed on open racks.			

Sl. No	Requirement	Mandatory	Compliance (Yes /No)	Remark (If any)
6	The UPS should VFI classified (according to IEC 62040-3) producing an output waveform that is independent of both the input supply frequency and voltage.			
7	**UPS Module AC Input:** • Input voltage range for rectifier operation: 340-460 Vac (nominal-400 V AC) • Frequency Range: 47 – 53Hz • Power walk-in: 15 seconds • Input Power Factor: should be 0.9 at rated load.			
8	**UPS Module AC Output:** • Load Rating: 100% continuous load rating at 40ºC for combination of linear and non-linear loads as per IEC 62040-3 standard)			
	• Voltage Regulation: 1% steady state for balanced load, 5% for 100% unbalanced load as per IEC 62040-3, 5.3.1. • Nominal Output Power Factor: 0.9 for KW rating of UPS. However, UPS module should be able to operate for load power factor from 0.9 lag to 0.8 lead with suitable de-rating factor. • Frequency Regulation: ± 1Hz synchronized with bypass source, ± 0.01Hz free running or on battery operation. • Frequency Slew Rate: 0.1 up to1.0Hz per second (selectable) • Phase Imbalance: 120º ±1º el. for balanced or 100% unbalanced loads.			

Sl. No	Requirement	Mandatory	Compliance (Yes /No)	Remark (If any)
	• Voltage Transients: ± 5% for 100% output load step (as per IEC 62040-3). • Transient Recovery Time: ±1% of steady state output voltage within 20ms. • Voltage Distortion (at 100% rated load with crest factor 3:1): <5% (Th.D.). • Overload Capability at Rated Output Voltage: • 110% of rated load for 60 minutes. • 125% of rated load for 10 minutes. • 150% of full load for a minimum of 1 minute.			

11.1.3. Diesel Generator

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
1	The Diesel Generators must be Data Centre continuous rated. This essentially means supplying power continuously to a constant load for unlimited hours in a Data Centre application		
2	Voltage regulation: Random and no load to full load condition = ± 1%		
3	Engine Design must be multi cylinder, Turbo charged.		
4	Standard engine cooling system by 40ºC ambient radiator.		
5	Alternator design to be brushless, 4 pole, drip proof revolving type.		
6	Exciter must be PMG/AREP type.		
7	AC transfers THDV at no load to be <1.5% and at non distorting balanced linear load to be <5%		
8	Microprocessors based providing voltage regulation, engine and Alternator protection, operator interface and Isochronous governing. Synchronization to be attained through integrated controller only. No external controller is allowed. The system must be able to send all the data		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
	to DCIM through all possible and acceptable protocols.		
9	The engine should have a volumetric capacity of minimum 14 litter or higher.		
10	The offered PCC or any OEM recommended controller must have all engine/ alternator protection / synchronizing feature inbuilt inside genset controller		
11	Underground HS. D tank with pumps, piping, digital fuel meter and other accessories including fencing over the platform.		
12	Comprehensive Warranty of DG sets should be provided by single OEM for better coordination, maintenance & manageability.		

11.1.4. MV Panels

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
1	The main distribution boards shall be of standard, natural air cooled, well tested, and proven design which ensures maximum safety to personnel, maximum service reliability and economic operations for a lifetime of at least 20years. Design and construction shall be simple, well laid- out and shall provide good accessibility to components and parts.		
2	Unless specified otherwise, the form of construction for the main distribution board shall comply with Form-4b requirements of IEC 61439-1. And 2		
3	The electrical system for all main distribution boards shall be 415 / 380V, 50 Hz 3phase and neutral, 4-wire solidly earthed. The main distribution boards shall be suitable for operating voltage up to 690 V and Insulation voltage of 1000V		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
4	Unless specified otherwise, the fault level withstand capacity of the main distribution board bus bar system rated up to 5000Amps shall be 65KA RMS for 1second as minimum standard. The breaking capacity of the switching devices shall be 65KA as minimum standard. The type test certificate shall be submitted for consultant engineer verification, to prove the fault level withstand capacity of the main distribution boards. Even under extreme conditions of short circuit or mal operation there shall be no danger to persons in the vicinity of the assembly.		
5	All equipment and components of the main distribution boards shall be capable of continuous operation at their full current and voltage ratings and without detriment or malfunction at system continuous deviation of up to and including the following percentages of normal values.		
6	The enclosure system shall be **Modular** in nature with **Bolt** on construction.		
7	Load Bearing members and main Bus bar supports should be from OEM Only		
8	Panels should be tested for mechanical impact as per IEC62262 for IK09 with double door design		
9	Panels should be internal arc tested as per IEC-61641 for 65 KA at 0.3 secs		
10	The enclosure shall be powder coated to an approved colour. The painting process shall include removal of moisture on the sheet steel surface using and applying thermosetting polyester powder using automatic guns. Polymerization of the powder shall take place when the components are cured at about 180ºC, forming a continuous integrated		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
	coating. A uniform coating of at least 70-80 microns shall be provided.		
11	The pre-treated and powder coated sheet steel components shall be at least tested randomly at regular intervals for coating thickness measurement, adhesion test, bend test, impact test, hardness test, salt spray test etc.		
12	Main distribution board enclosure shall be fabricated of minimum **1.5mm** thick electro-galvanized sheet steel folded construction. The enclosure shall be of simple and robust construction designed for a variety of dimensions obtainable by means of standardized basic elements. Main distribution board shall consist of several enclosures of equal height and depth mounted side by side to form a composite board of uniform assembly.		
13	Unless specified otherwise, Main distribution boards shall be designed for front access for the purpose of operation and access to all components and shall suit front or rear access for cable connections and top or bottom for cable entries. Wherever required, enclosure shall be suitable for bus duct entry at the top. The access and entries shall be provided as per site requirements.		
14	Enclosure shall be readily suitable for future extension on either side without any modifications (after installation at site).		
15	The bar bus system should be designed as per the predefined guidelines provided by the original manufacturer. The bus bar system should be typed by the manufacturer at a reputed laboratory for short circuit withstand capacity. The neutral and earth bus bars shall also be type tested for the short circuit		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
	withstand capacity. The fault level rating of the bus bar system shall be as per the drawings however the minimum short circuit withstand capacity shall be 50KA RMS for 1second. Neutral bus bars shall be able to withstand a thermal stress of at least 50%, corresponding to the main phase bus bar rated short circuit withstand capacity.		
16	The bus bars shall be high grade electrolytic tin-plated copper (with 99.9% conductivity), rectangular and rigid construction. The phase bus bars, and neutral bus bars shall be arranged systematically in a bus bar chamber/ alley. The bus bars shall be colour sleeved throughout the length for phase identification (except for the distribution bus bars of the withdrawable sections). The bus bars shall be shrouded completely using metallic partitions and/or polycarbonate shrouds as applicable. The bus bar assembly shall be shrouded (at least IP20) by shrouds so that no live parts are accessible. Phase identification shall be done systematically. Use of Bakelite sheets for shrouding will not be permitted.		
17	Distance between the bus bars supports the bus bar system and the distance between different phases of bus bar system shall be as per manufacturer guidelines based on the type test results.		

11.1.5. Passive Networking

Sl. No	Requirement	Compliance (Yes/No)	Remark (If any)
A	**Architecture and General Construction**		
1	The system shall utilize “aligned key” adapters for every MPO mated connection, per TIA 604- 5, K=2.		

Sl. No	Requirement	Compliance (Yes/No)	Remark (If any)
2	The system shall guarantee correct Transmit/Receive polarity in any configuration or combination of system components.		
3	The system allows for the use of TIA compliant patch cords and trunk cables on both ends of every link, for both duplex and full-parallel applications.		
4	The system should support Fiber Performance calculators available at OEM website for verification of the designed fiber links against a given set of applications.		
5	The system shall support 50/125 Laser Optimized Multimode – available in OM4 and OM5 (Wide Band Multimode)		
6	The proposed system should have been Installed successfully in at least 3 data centres / any large facilities in India, in the last 2 years.		
B	**Pre-Terminated MPO Modules**		
1	LC Modules – 12-fiber or 24-fiber – Shall be available in 50-micron laser optimized OM4 and latest OM5 versions.		
2	The 12-fiber MPO male/female module shall have 6 pre-installed duplex LC adapters at the front routed to a pre-installed 12-fiber MPO “Aligned key” adapter at the back.		
3	The 24-fiber MPO male/female module shall have 12 pre-installed duplex LC adapters at the front routed to 2 pre-installed 12-fiber MPO “aligned key” adapters at the back.		
4	Cassettes shall have wiring patterns to enable use of same cassette on either end of link, for easy management and scalability or the cassettes (modules) should be one end polarity A and other end polarity B, for matching of link.		
5	The cassettes shall be UL or equivalent listed. Insertion Loss (MPO): <0.5 dB		
6	The vendor shall provide the application support guidelines for the system		

Sl. No	Requirement	Compliance (Yes/No)	Remark (If any)
7	The vendor shall have a proven track record of public demonstration of 40/100G.		
C	**Modular Panels and Shelves**		
1	The 1U / 2U shelf shall be equipped with a front trough and door for patch cord management and port labelling. Trough doors should have a clear view of the ports and labels inside.		
2	The 1U panel shelf shall house any combination of up to 4 pre-terminated modules to achieve up to 96 Fibers terminations per rack unit at a minimum. To be used in low density server rack end.		
3	The 2U/4U high density shelf shall support up to 144 duplex LC ports to be used in Network racks / SAN racks.		
4	1U / 2U /4U shelves shall have 1/2 stage slide out feature in the front for better inside access.		
5	Shelf shall support both side and rear entry of cables / trunk cords.		
D	**Pre-terminated Fiber Trunk Cable assemblies**		
1	All cables shall be constructed with one or more subunits, each with 12 Fibers surrounded by a jacket containing aramid yarn strength members.		
2	All cables should be Bend insensitive multimode OM4 or OM5.		
3	The trunk cables shall be available in 12 / 24 Fibers with MPO male/female connectors on either end.		
4	The Trunk cable shall have Method B enhanced Construction and Colour of the jacket to be as per TIA standards.		
5	The cable should have been tested for 40/100G		
6	Trunk Cable dia. Not more than 5.7 +/- 0.2 mm. LSZH jacket with IEC 60332-3 or equivalent or higher compliance.		
7	Trunk Cables have Flame Test Listing of NEC OFNR-LS (ETL) and c (ETL) or equivalent certified.		

Sl. No	Requirement	Compliance (Yes/No)	Remark (If any)
8	LC-LC OM4 / OM5 Patch cords shall be with Uni-boot construction for ease of access in high density panel ports.		
9	Uni-boot patch cords shall support field adjustable polarity reversal, without cord damage.		
10	The vendor should provide the application support table for the trunk and the associated system components.		
E	**Horizontal Cable – CAT6A UTP Cable –**		
1	The Cable should be 4 pair 23 AWG solid copper conductor and meet ANSI/TIA 568C.2 Category 6A Specifications and ETL verified.		
2	The cable shall be available in Low-Smoke, Zero Halogen (LSZH) compatibility and The LSZH version must comply with the following Fire Safety standards: 1) ISO/IEC 60332-3-22: Vertical Flame Spread 2) ISO/IEC 60754-2: Acidity 3) ISO/IEC 61034-2: Smoke Density LSZH cable with IEC 60332-3-22 and IEC60332-1 will also be acceptable		
3	NEXT - Minimum 3 db. above the standards.		
4	The cable must be compliance to ANSI/TIA 568-C.2 requirement for both long channel (100m) and short channel (15m) tests. Reports for both tests to be submitted.		
5	The cable and cordage shall be "UTP" components that do not include internal or external shields, screened components or drain wires. No Special Grounding requirements. The horizontal data cables shall be of shielded twisted pair cordage with eight (8) solid conductors formed into four individually twisted pairs		

Sl. No	Requirement	Compliance (Yes/No)	Remark (If any)
6	The horizontal cable shall have a unique print string on the cable jacket to access a full set of OEM factory tests available publicly for any time verification by client.		
F	**Requirement for CAT 6A Patch Panel**		
1	The ganged adapters should have an RJ45 jack in the front and Insulation Displacement Connector (IDC) at the rear of the module.		
2	Termination managers must be provided with a panel to provide proper pair positioning, control, and strain relief features to the rear termination area of the panel.		
3	3rd Party Verification test certificates shall be provided to show compliance to ISO/IEC 11801 Amendment 2 testing for Cat 6A components.		
4	The panel shall be equipped with removable rear mounted cable bundle managers.		
5	Insertion Life = 750 minimum insertions of an FCC 8-Position Telecommunications Plug		
G	**Requirement for CAT 6A LSZH U/UTP RJ45 Patch Cords-**		
1	CAT6A Patch Cords shall be constructed of 23/24 AWG solid core copper and equipped with 8- Pin modular plugs on each end.		
2	All cords shall be round, and consist of copper conductors, tightly twisted into individual pairs.		
3	Nominal cordage diameter shall not exceed 7.24 mm.		
4	Plugs shall be designed with an anti-snag latch to facilitate easy removal during move, add and change processes.		
5	LSZH jacket must comply with the following Fire Safety standards: ISO/IEC 60332-3-22: Vertical Flame Spread ISO/IEC 60754-2: Acidity ISO/IEC 61034-2: Smoke Density		

Sl. No	Requirement	Compliance (Yes/No)	Remark (If any)
6	The cordage shall be UTP components that do not include internal or external shields, screened components or drain wires.		
7	The patch cords will have an insertion life of 750 cycles minimum.		

11.1.6. DCIM

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
1	The proposed 100% web based DCIM should have the following modules: a) Inventory Manager b) Change planner c) Thermal Systems Manager d) Site Manager e) Power System Manager f) Energy Insight	Mandatory		
2	Proposed DCIM should have a single platform with combination of application server and database server with data collection engine.	Mandatory		
3	The solution should have symbols library more than 10000 vendor neutral symbols and preloaded with 1000 symbols. All managed device symbols must include physical dimensions, rated capacities, consumption of space, power and cooling and any other associated manufacturer's data.	Mandatory		
4	Proposed DCIM solution should support complex business process mapping based on requirement. Example: - commission, de- commission, add and modify.	Mandatory		

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
5	Thermal heat map - should visualize thermal data in the form of heat maps in a 3D rendering of the floor view. And should allow to view actual rack heat load and to help balancing and optimizing the system and generate reports	Mandatory		
6	DCIM should have the capability to customize dashboards as per customer requirement.	Mandatory		
7	Dynamic Single Line diagram should enable logical mapping from LT/ HT Panel to IT equipment and provide exact alert/alarm can be pinpoint problems through this solution.	Mandatory		
8	The solution shall support all levels of role-based access control and fine grain authorization for each functional department	Mandatory		
9	Proposed DCIM should be able to integrate with third party BMS solution	Mandatory		
10	Space, power, and cooling capacity management: End to End DC facility view to analyses data such as rack capacity, maximum rack space available, weight, and available space. in racks/DR floor to improve capacity.	Mandatory		
11	Proposed DCIM should have a Map view to have high level understanding on multi-location Data Centres	Mandatory		
12	DR design capability: Upload floor plan images and utilize drag-and-drop functionality to place equipment within the floor plan including detailed rack elevations with rack load, space utilization, relationship rules and inventory monitoring built in.	Mandatory		

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
13	At minimum DCIM should provide these reports (hourly, daily, weekly, monthly, quarterly, yearly): However, there should be an option to customize the reports as per the end user requirement anytime. Availability/Reachability Report, Total UPS load, Used UPS load, total cooling capacity, used cooling capacity, Total/Used/Available U- space (floor level & at rack level), Ambient and Inlet temperature, Energy Efficiency PUE/DCiE trend, rack level power consumption report, Alarm reports, quick access to information such as current capacity, asset lists and exact device location.	Mandatory		
14	The solution provides alert compression and advanced alerting algorithms including deviation from normal and time over threshold to help reduce false positive alarms.	Mandatory		
15	The solution will provide provisions to recommend the best location for a server in the rack layout, utilizing available space, cooling, and power capacity to optimize capacity utilization.	Mandatory		
16	Proposed DCIM shall provide mobile device capability preferably iOS/Android solution. It shall enable barcode and device recognition for easy inventory management. It should include an audit capability, so the user can scan and asset and quickly determine correct or incorrect placement of the device.	Desired		
17	Proposed DCIM solution should have capability to provide console management of Virtual and Physical	Desired		

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
	servers and serial devices.			

11.1.7. IPDU

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
1	Each rack should have two IPDUs with different chassis colour for source identification, and each IPDU should support the load up to 15kW.	Mandatory		
2	Each IPDU should be 3 phase 63A PDU for all racks.	Mandatory		
3	Intelligent PDU should have min. 18 numbers of hybrid outlets which can be utilized as either C13 or C19 outlet. All outlets should provide high retention to avoid accidental dislodging of power cords. All 15 KW racks iPDU to have 18 number of ports.	Mandatory		
4	Monitoring parameters – The IPDU should have monitoring capability at the Strip level, phase level, outlet/socket level monitoring Following monitoring parameters should be included phase and the outlet level. 1.) Voltage (V) 2.) Current (A) 3.) Power factor 4.) Active power (W/KW) 5.) Energy consumption (Kwh) The metering accuracy should be +/- 3% compliant to ANSI C12.1 and IEC 62053- 21 at 3% Accuracy	Mandatory		

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
	Class Requirements for outlet/socket, strip, and phase level.			
5	Each IPDU must have circuit breakers to protect the PDU and IT devices from damage caused by overload or short circuits. PDU must have 63Amp circuit breakers as per the IEC guidelines.	Mandatory		
6	The iPDU should have colour coded and alternate Phase outlets for simplified circuit and phase balancing, reducing cable runs for better airflow management.	Mandatory		
7	It should support High Operating temperature of 0 to 45 deg C to take care of high operating temperature at back of Rack.	Mandatory		
8	The IPDU should have 2 Nos. 1 Gigabit Network Ports. IPDU should support communication protocols including DHCP, HTTP, HTTPS, Ipv4, Ipv6, LDAP, NTP, RADIUS, RSTP, SSH, SMTP, SSL, SNMP (v1, v2, v3), Syslog and TACACS+. Communication modules should not be swappable, so that it can be replaced without powering off the PDU.	Mandatory		
9	PDU should support configuration of user defined thresholds, reports and email alerts and send it automatically to the configured users automatically on the scheduled time intervals.	Mandatory		
10	The IPDU should support grouping of 16 to 40 rPDU and rPDU sensors in the interconnected array to create the aggregated	Mandatory		

Sr. No.	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (if any)
	measurements like total rack power, average temperature, average humidity etc.			
11	IPDU should have separate reset buttons for reset to factory defaults and separate button to reset IP only, if other configurations are not to be altered.	Mandatory		
12	IPDU should have USB support for firmware upgrade, backup, restored device configuration or expanding logging capacity via USB storage device.	Mandatory		
13	IPDU should have LED indicators for each outlet and should have different colours to show the state of the outlet	Mandatory		
14	Each rack should have one sensor in the front of the rack to monitor temperature, humidity, dew point & airflow and one sensor in the rear to have temperature monitoring.	Mandatory		
15	The IPDU should have approvals from CE /VDE/ RoHS/UL.	Mandatory		
16	The IPDU input cable should have approvals from IEC, CE, EN & UL	Mandatory		
17	PDU should support Android or iOS app for easy and secure read of full power readings and should not use Bluetooth or Wi-Fi to prevent breach and should not have any additional license requirement.	Desired		
18	Sockets should be preferably coloured to clearly identify different circuits.	Desired		

11.1.8. Dry Type Transformers

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
1	The transformer should be designed so that they can deliver continuously its rated current under steady loading conditions without exceeding the temperature rise, assuming that the applied voltage is equal to the rated voltage and that the supply is at rated frequency.	Mandatory		
2	Dry type AN cooled transformer, can be overloaded according to IEC 60905 Loading guide for dry type transformers	Mandatory		
3	The core shall be constructed of the best quality, low loss, cold rolled, grain-oriented steel laminations insulated on both sides. Laminations shall be “step lap” overlapped to minimize core losses and noise. The entire core assembly shall be covered with heat retardant resin-based lacquer for corrosion protection before the coils are mounted	Mandatory		
4	All the wings shall be of high conductivity conductors of the best quality. The transformer shall have separate high voltage and low voltage windings. The insulation system of the windings shall consist of approved materials for assigned temperature class.	Mandatory		
5	The Fire, Environmental, and Climatic classes should be as stated below: Environmental Class: It shall be E2 in order to be able to withstand condensation or pollution or combination of both. **Climatic Class:** It should be C1 or C2: C1: Indoor installation. The transformer is suitable for operation at ambient temperatures not below – 5 deg C, but may be exposed during transport and storage to ambient temperatures down to – 25 deg C. C2: Outdoor installation. The transformer is A suitable for operation, transport, and storage at ambient temperatures down to – 25 deg C.	Mandatory		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
	Fire Class: It shall be F1. Transformers are subjected to fire hazard. Restricted flammability is required. Self- extinction of fire (poor burning is permitted with negligible energy consumption) shall take place within a specified period to be agreed between purchaser and manufacturer, unless specified by National Specification. The emission of toxic substances and opaque smoke shall be minimized. Materials and products of combustion shall be practically halogen-free and shall contribute with a limited quantity of thermal energy to an external fire.			
6	HV windings shall be vacuum cast with aluminium disk foil as conductor material and 180ºC (class H) insulation system temperature (copper foil can be also accepted). Winding design shall be adequate to allow for full encapsulation with filled resin under vacuum. The resin system shall be two components epoxy filled with a mixture of inorganic fillers improving its thermal, mechanical and fire behaviour properties. The single resin components and filler will be carefully stirred and degassed under vacuum in order to eliminate all air bubbles and then mixed together throughout a static mixer just before pouring them, under vacuum, into the mold that contains the coil (winding). The position of this mold shall be horizontal during the casting process that shall ensure the total elimination of air bubbles that could create air cavities and critical points of partial discharges. The surface of the encapsulated winding shall be smooth and completely closed and impervious to moisture and common industrial contaminants	Mandatory		
7	High Voltage Connections The HV cable terminals will be made of copper / aluminium material, located above the top of the connection bars.	Mandatory		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
	Each terminal will be drilled with a 13 mm hole ready for connection of cables. The HV delta connection will be made through copper bars protected by heat shrinkable tubing and flexible cables.			
8	Low Voltage Windings The LV windings will be of non-encapsulated design with aluminium foil wound (copper foil can also be accepted) together with an insulating pre-impregnated B-stage epoxy resin and thermally cured in an oven to achieve thermal, mechanical and moisture penetration properties that are comparable, for LV coils, with those of cast windings. In high polluted or aggressive environments, it is recommended to seal both edges (top and bottom), that will prevent the entry of dust or moisture inside the coil.	Mandatory		
9	LV connections The LV connections will be made from above onto bars located at the top of the coils on the opposite side to the HV connections. All the terminal connection bus bars shall have half round edges.	Mandatory		
10	Short – Circuit Withstanding The transformer shall be capable of withstanding, on any tapping, for two seconds (IEC value = 2 s), without damage, under service conditions, the thermal and mechanical effects of a short – circuit at the terminals	Mandatory		
11	**Thermal insulation class** The insulation system temperature for HV and LV winding will be 180ºC (class H). The average winding temperature rise for both HV (at rated tapping position) and LV windings at full load shall not exceed 115ºC (class H) (over an ambient temperature equal to 50 deg C)	Desired		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
12	**On Load Taping:** The transformer shall be provided with tapping links on the HV windings. Their position can be selected whilst the transformer is on circuit. Taping selection shall be by means of bolted links. The tapping range shall be: ▪ Plus 2.5% and 5% ▪ Minus 2.5% and 5% Tapping with connection cables is not accepted.	Desired		
13	**HV and LV windings assembly** The high and low voltage coils of each phase shall be supported and clamped by lower and upper blocks, each having rubber expansion blocks for thermal expansion. The position of the LV terminals shall be either at the opposite side of the HV terminals at the top or at the bottom of the transformer. The neutral bar terminal, if any, shall be at the same side as the LV phase terminal. The design of the complete assembly should be in a way that, if necessary, an exchange of separate high and low voltage coils can be done. High and low voltage coils can be done**.**	Desired		
14	**Noise level** Noise level shall be in accordance with the NEMA TR 1 / CENELEC standards.	Desired		
15	**Earthing terminal** Provision shall be made to connect external earthing at position close to the bottom the enclosure at two points. Earthing terminal shall be adequately dimensioned to receive the external earthing conductor/strip.	Desired		
16	**Internal earthing arrangement** All metal parts of the transformer except for the individual core laminations and associated individual clamping plates shall be maintained at some fixed potential. The bottom main core	Desired		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
	clamping structure shall be connected to the enclosure by copper cable.			
17	Standard enclosure The enclosure is made of bolt-on type sheets of steel of the bolt-on type with removable panels and supported from the transformer framework. Its removable base can be installed without having to lift the transformer. Central front and rear handle panels will be provided for access to the tap changer. The inlet outlet of cables is situated at the bottom of the enclosure through aluminium gland plates to be machined by the customer. For indoor applications the sheet steel will be painted in grey colour, RAL7035 with average 70m powder coating thickness; for outdoors applications will be painted in grey colour, RAL7035 with average 100 □m powder coating thickness.	Desired		

11.1.9. Fire Detection & Alarm System

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
1	2 loop panel with LCD display, per loop 250 Devices handling capacity of any combination, power supply and battery backup. If require Each Loop shall be able to configure in two physical loops.		
2	The fire alarm system shall be integrated with the access control system to deactivate all door locks in case of emergency.		
3	Instructions/signals from panels should also shut down the PACs in case of fire.		
4	The fire alarm system should also be integrated with the BMS through SNMP CARD/Modbus/BACnet interface to get all the alerts and alarm on the BMS		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
5	Each Loop with 250 device capacity capable to handle the following detectors and devices.		
6	Analogue Addressable Photo Type Smoke Detector with Detector base Server Farm Area		
7	Analogue Addressable Multi Criteria type Smoke Detector with Detector base for Utility area		
8	Intelligent Analogue Addressable Smoke Detector., UL Listed 268, software Programming only.		
9	Addressable single action pulls down type Manual call point.		
10	Addressable Monitor Modules		
11	Addressable Control Modules		
12	100 DB Sounder		
13	Integration with PAC and BMS System		
14	All cables must be FRLS type. All conduits must be metal type.		

11.1.10. Gas Based Fire Suppression System: - Suppression System (NOVEC 1230)

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
1	The bidder shall supply, install, test, and put in operation (NOVEC) 1230 based fire suppression system. The fire suppression system shall include and not be limited to a gas release control panel, CCOE approved seamless cylinders, discharge valve (with solenoid or pneumatic actuator), discharge pipe, non-return valve and all other accessories required to provide a complete operation system meeting applicable requirements of NFPA 2001 standards and installed in compliance with all applicable requirements of the local codes and standards.		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
2	The work under this system shall consist of design, supply, installation, testing, training & handing over all materials, equipment, software appliances and necessary labour to commission the said system, complete with all the required components strictly as per the enclosed tender specifications, design details. The scope also includes the supply, installation & commissioning of any material or equipment including civil works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project.		
3	The system design should be based on the specifications contained herein, NFPA 2001 & in accordance with the requirements specified in the design manual of the agent. The bidder shall confirm compliance with the above along with their bid.		
4	The system shall be properly filled and supplied by an approved OEM		
5	Generally, the key components* of the system shall be VdS or LPCB or FM/UL listed. The NOVEC 1230 gas shall:		
6	Comply with NFPA 2001 or ISO 14520 standard and have the approval from US EPA (Environmental Protection Agency) for use as a total flooding fire extinguishing for the protection of occupied space:		
7	Must have zero ozone depletion potential (ODP)		
8	Have a short life span in the atmosphere, with an atmospheric lifetime of less than 5 days		
9	Be efficient, effective and does not require excessive space and high pressure for storage;		

Sl. No	Requirement	Compliance (Yes /No)	Remark (If any)
10	The system shall be designed to take the minimum design concentration as per NFPA 2001(Latest Edition) guidelines & as applicable to class 'A' & C risks. The NOVEC 1230 agent shall be stored in seamless steel cylinders and dry nitrogen shall be added to provide additional energyto give the required rapid discharge. At the normal Operating pressure of 42bar/25 bar at 21Deg C, the agent is a liquid in the container.		
11	As per the regulations of the Chief Controller of Explosives (CCE), Nagpur, any system which has a working pressure above 19 bar (280 psi) will require the use of seamless cylinders that have been duly approved by the CCE, Nagpur.		
12	ROOM INTEGRITY TEST		
13	NFPA2001 states that the design concentration of a clean agent post discharge shall be maintained for a sufficient period of time to ensure there is no re- ignition of fire once suppressed. NFPA 2001 and 12A require an enclosure integrity test as part of the acceptance procedure for all clean agent systems. This includes halocarbon and inert agents. This comprehensive test and calculation predict The leakage area corresponds to the retention time of agent in the enclosure on discharge. Most specification state it must be ten minutes. The cylinders must have digital pressure gauge which must be Capable of integration with DCIM tool for remote monitoring		
14	Portable ABC /Co2 /Foam type Extinguisher for UPS, electrical room.		

11.1.11. Access Control System

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
1	The Integrated Access Control System's (ACS) primary function shall be to regulate access through specific doors, gates, or		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
	barriers to secure areas of the facility.		
2	An Intelligent System Controller (ISC) shall link the ACS software to all other fields of hardware. It should provide full distributed processing for access control and alarm monitoring operations. The controller should be 8 doors, 40,000 cards capacity, and 10000 events. Interface on RS232, RS485 and TCP/IP.		
3	A Dual Reader Interface Module (DRIM) shall be available for each controlled door and provide the ability to connect up to two card readers or entry devices		
4	Smart card readers at every Critical door for Entry and Exist. Biometric fingerprint Card reader for Critical door of Server room Door only for Entry Point and exist Smart card readers.		
5	Enterprise Version Server Software for Access control &Time and Attendance with capability to service Minimum 1 concurrent clients, Inclusive of One Server & One Client License.		
6	Shall be capable of communicating with centralized command software (BMS).		
7	Software shall Programmable functions, controller downloads and uploads, multi-level local and global anti-pass-back, integration with fire systems, grouping of escape routes, door security clearance, import and export utilities, etc.		
8	• Multiple layers of maps with interactive icons;		
9	• Alarm recognition and treatment;		
10	• Scheduled times for door clearance;		
11	• Send emails and SMS to select users. • Multiple card formats and facility codes;		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
12	• Flexible commands for card users such as temporary access level (shift changes) and provisional cards, card lock, penalties, card and event tracking, Double custody of access cards, etc. Control, multi-level locker and rack control with required Hardware controller		
13	SITC of Multi Format Card Readers		
14	SITC of Biometric + Smart Card Readers, shall have 2" IPS (In Plane Switching) touch screen LCD with Corning Glass scratchproof protective glass with Smart card reader module. Authentication shall be done in 1 second and the 1GB memory on board for user storage of minimum 5000 users with a card & 25000 events transaction log capability.		
15	SITC for Panic Bar with alarm for emergency exit doors.		
16	Time and attendance features such as login reports		

11.1.12. High Sensitivity Smoke Detection System

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
1	The panels shall be mounted inside the risk protected and there shall be a network of air sampling pipe work.		
2	The High Sensitivity Smoke detection consist of highly sensitive Laser-based Smoke Detectors with aspirators connected to networks of sampling pipes. The alarms are generated once the laser sensor receives smoke at a pre-determined obscuration level to activate and alert, Fire 1, Fire 2, and alert signal		
	Smoke Detectors with aspirators connected to networks of sampling pipes. The alarms are generated once the laser sensor receives		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
	smoke at a pre-determined obscuration level to activate and alert, Fire 1, Fire 2, and alert signal.		
3	The signal is extended to the Fire Alarm monitor Modules / BMS through Volt free contacts for further investigation.		
4	When required, it shall be possible to connect an interface card for open Protocol output to BMS system for online Monitoring with Software level integration.		
5	When required, an optional remote Display unit shall be provided to monitor each detector, and a Programmer shall be supplied to configure the system.		
6	The system shall include all equipment, appliances, and labour necessary to install the system, complete with highly sensitive LASER-based 7Smoke Detectors with aspirators connected to a network of sampling pipes.		
7	The Bidder shall also make provision in the Aspirating Smoke Detectors to trip PAC system and to shut fire dampers in the event of fire through the relay contacts.		
8	Codes and standards the entire installation shall be installed to comply one or more of the following codes and standards: NFPA Standards, British Standards, BS 5839 part :1		
9	Approvals All the equipment's shall be tested, approved, and/or listed by LPCB (Loss Prevention Certification Board), UK, FM Approved for hazardous locations Class 1, Div 2 UL (Underwriters Laboratories Inc.), US ULC (Underwriters Laboratories Canada), Canada Vds (Verband der Sachversicherer e.V),		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
	Germany		
10	The System shall consist of a highly sensitive LASER-based smoke detector, aspirator, and filter.		
11	It shall have a display featuring LEDs and Reset/Isolate button. The system should be configured by a programmer that is either integral to the system, portable or PC based.		
12	The system shall allow programming of: Multiple Smoke Threshold Alarm Levels Time Delays. Faults include airflow, detector, power, filter block and network as well as an indication of the urgency of the fault. Configurable relay outputs for remote indication of alarm and fault Conditions. It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modelling tool. Optional equipment may include intelligent remote displays and/or a high-level interface with the building fire alarm system, or dedicated System Management graphics package.		
13	Performance Requirements Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter Shall report any fault on the unit by using configurable fault output relays or via the graphics Software. Shall monitor for filter contamination. Shall incorporate a flow sensor in each pipe and provide staged airflow faults.		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
14	Materials and Equipment's Both Light Scattering and Particle Counting shall be utilized in the device as follows: The Laser detection Chamber shall be of the mass Light Scattering type and capable of detecting a wide range of smoke particle types of varying size. A particle counting method shall be employed for the purposes of Preventing large particles from affecting the true smoke reading. Monitoring contamination of the filter (dust & dirt etc.) to notify you automatically when maintenance is required. The Laser Detection Chamber shall incorporate a separate secondary clean air feed from the filter, providing clean air barriers across critical detector optics to eliminate internal detector contamination. The detector should not use adaptive algorithms to adjust the sensitivity from the set during commissioning. A learning tool shall be provided to ensure the best selection of appropriate alarm thresholds during the commissioning process.		
15	Detector Assembly The Detector, Filter, Aspirator and Relay Outputs shall be housed in a mounting box and shall be arranged in such a way that air is drawn continuously from the fire risk area by the Aspirator and a sample passed through the Dual Stage Filter and then to the detector. The detector should be LASER-based and should have an obscuration sensitivity range of 0.025 – 20% obs/m. The detector should have four programmable smoke alarm thresholds across its sensitivity range with adjustable time delays for each threshold between 0 - 60 seconds. The detector shall also incorporate the facility to transmit a fault through a relay. The detector		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
	should have a single pipe inlet that must contain an ultrasonic flow sensor. High flow fault (urgent and non-urgent) and low flow fault (urgent and non-urgent) can be reported. The filter must be a two-stage disposable filter cartridge. The first stage shall be capable of filtering particles in excess of 20 microns from the air sample. The second stage shall be ultra-fine, removing more than 99% of contaminant particles of 0.3 microns or larger, to provide a clean air barrier around the detector's optics to prevent contamination and increase service life. The aspirator shall be a purpose-designed rotary vane air pump. It shall be capable of allowing/ supporting for a single pipe run / multiple sampling pipe runs with a transport time of less than 90 seconds. Detectors shall be capable of supporting a single pipe run of 25m with a maximum transport time of 120 seconds or as appropriate standards dictate. The Assembly must contain relays for fire 1, Action and fault conditions. The relays should be software programmable (latching or non-latching). The relays must be rated at 2 A at 30V DC. Remote relays shall be offered as an option and either configured to replicate those on the detector or programmed differently. The Assembly shall have built-in event and smoke logging. It should store smoke levels, alarm conditions, operator actions and faults. The date and time of each event shall be recorded. Each detector (Zone) shall be capable of storing up to 18000 events.		
16	Displays on the Detector Assembly The detector will be provided with LED indicators. Each Detector shall provide the following		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
	features at a minimum. Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector. Smoke Dial display represents the level of smoke present. Fault Indicator. Disabled indicator. Buttons supporting the following features shall be accessible to authorized personnel. Reset – Unlatches all latched alarm and faults. Disable – Disables the fire relay outputs from actuating and indicates a fault.		
17	Sampling Pipe The sampling pipe shall be smooth bore with an outside diameter of 25mm and internal diameter of 21mm should be used. The pipe material should be suitable for the environment in which it is installed or should be the material as required by the specifying body. All joints in the sampling pipe must be airtight and made by using solvent cement, except at entry to the detector The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards. All pipes should be supported at not less than 1.5m centres, or that of the local codes or standards. The far end of each trunk or branch pipe shall be fitted an end cap and drilled with a hole appropriately sized to achieve the performance as specified and as calculated by the system design		
18	Sampling Holes Sampling Holes of 2mm, or otherwise appropriately sized holes, shall not be separated by more than the maximum distance allowable		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
	for conventional detectors as specified in the local codes & standards. Intervals may vary according to calculations. Each sampling point shall be identified in accordance with Codes or Standards. Consideration shall be given to the manufacturer's recommendations and standards in relation to the number of Sampling Points and the distance of the Sampling Points from the ceiling and roof structure and forced ventilation systems.		

11.1.13. IP based CCTV System

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
1	2 megapixel (1920 x 1080) resolution Indoor Camera with 1/2.9" 2.19M CMOS or better , Lens- 3.2 ~ 10mm varifocal lens or better ,Min 30fps@all resolutions (H.264), H.264, MJPEG codec supported, Multiple streaming and User Access 6 users at unicast , Auto Day & Night ,WDR -120dB or better, Tampering, Motion detection, Micro SD/SDHC memory slot Min support 32GB, PoE , Hallway view, IR Range 20m		
2	2-megapixel (1920 x 1080) resolution weatherproof bullet type camera with /2.9" 2.19M CMOS, Lens 3.2 ~ 10mm varifocal lens or better, Min 30fps@all resolutions (H.264), H.264, MJPEG codec supported, Multiple streaming and User Access 6 users at unicast, Auto Day & Night, WDR -120dB or better, Tampering, Motion detection, Micro SD/SDHC memory slot Min support 32GB, PoE, Hallway view, IR Range 30m, IP66 support		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
3	2MP (1920 x 1080) resolution outdoor PTZ camera with 1/2.8" 2M CMOS , Focal Length 5 ~ 100mm , zoom 20X , Pan- 360˚ Endless, Tilt Range200˚ ,Pan / Tilt Speed-P reset : 500˚/sec, Manual : 0.24˚/sec ~ 200˚/sec, Pre-set -300, Swing, Group , Trace, Tour (1ea), Auto run, ScheduleH.265, H.264, MJPEG codec support, Multiple streaming, auto Day & Night (ICR), HLC/ BLC WDR120 dB, with Built-in Gyro sensor, Tampering, Motion detection, Memory slot and support Min 256GB, IP66, IK10		
4	32CH, Max. 12MP Camera supported, 256Mbps network camera recording, Transmission Bandwidth 500Mbps, Support 4K video out on HDMI monitor, Simultaneous Playback Min 16CH Support Dual monitor video out, Support H.265, H.264, MJPEG compression, 8 internal HDDs support e-SATA / iSCSI external storage, backup from camera SD card & Failover support- N+N / N+1, Operating Temperature +0°C ~ +40°C, Humidity 20% ~ 85% RH or better.		
5	There should be provision of integration of CCTV system with DCIM tool in order to monitor the Camera, NVR, HDD status Remotely.		

11.1.14. Water Leakage Detection System

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
1	Control Panel with 4 x 20 LCD		
2	4 / 8 zones		
3	Sensing technology shall be only AC		
4	Isolate facility for each zone		
5	Common fire interface relay		
6	Fault relay		
7	Hooter output		
8	Zone alarm & fault LED Indication		

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
9	MODBUS RTU for BMS integration		
10	The complete system shall include an electronic System control panel, multiple control modules, distance type sensing cable and all required auxiliary accessories (such as hold down clip & Tag/Label for the sensing cable).		
11	This system shall detect and locate multiple leaks simultaneously as well as cable break & power failure and activate the control panel alarm relays. The sensing cables shall		

11.1.15. Ultrasonic Rodent Repellent System

Sl. No	Requirement	Compliance (Yes / No)	Remark (If any)
1	2x16 LCD		
2	System Healthy relay		
3	Mini Exhaust Fan		
4	RS485 MODBUS RTU for BMS Integration		
5	Test Transducer Menu		
6	Programmable Sweep Time & delay		

11.1.16. Physical Access Control System

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
1	X Ray baggage Scanner Technology should be based on Dual energy based isometric X-Ray imaging.	Mandatory		
2	The Baggage scanner should produce isometric view (virtual 3D view) of the objects scanned to have more detailed information, which are not visible in traditional single view baggage scanners, which generates only the top or bottom (2D) view of the scanned objects.	Mandatory		
3	Machines should generate the images in such a way that the depth of any scanned object can be visualized appropriately to further analyse the details of the object	Mandatory		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
	inside a baggage for better identification of harmful objects like Gun/Knife etc.			
4	Tunnel Size - Minimum 60 cm W (width) x Minimum 40 cm H (Height)	Mandatory		
5	Operating System: LINUX	Mandatory		
6	Equipment manufacturer should have ISO 9001 certified factory in India. Certificate to be submitted.	Mandatory		
7	Production licenses from AERB should be submitted.	Mandatory		
8	Preference for equipment manufactured by MSME registered OEM.	Mandatory		
9	Preference to OEMs as per Make in India Policy will be given.	Mandatory		
10	The conveyor belt speed should be between 0.2 and 0.3 meters per second. Conveyor movement bi-directional	Desired		
11	All machines should operate on 230 VAC, 50 Hz power supply	Desired		
12	Conveyor Capacity - 160 kg evenly distributed	Desired		
13	Through put should be 500 bags per hour	Desired		
14	Tube Voltage: Maximum 160 kVA	Desired		
15	Tube Current 0.3 to 1.2 mA (Must be Adjustable); Duty Cycle - 100%	Desired		
16	The X-ray beam divergence should be such that the complete image at maximum size of bag is displayed without corner cuts.	Desired		
17	The radiation level should not exceed the accepted health standard (0.1m R/Hr at a distance of 5 CM from external housing). Relevant certificate from AERB	Desired		
18	1. The operating temperature should be - 5° to 50° C (Test Certificate from NABL accredited Lab to be submitted at the time of bidding)	Desired		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
	2. Storage temperature - 20° to 60° C (Test Certificate from NABL accredited Lab to be submitted at the time of bidding) 3. Relative Humidity- 10 to 95% non-condensing			
19	Resolution: The machine should be able to display single un-insulated tinned copper wire of 42-SWG or 38-AWG	Desired		
20	Steel penetration: 30 mm or above	Desired		
21	Sensors > 1000 diodes, L-shaped detector (folded array type)	Desired		
22	Video display - 17" or better LCD Monitor High resolution, low radiation, flicker free, resolution at least 1280x1024, 24-bit true colour real time processing	Desired		
22	Health & Safety - The machine must comply with requirements of health and safety regulations with regards to mechanical, Electrical and radiation hazards. The supplier/manufactures should furnish Test Certificate from Atomic Energy Regulatory Board of India regarding radiation safety.	Desired		
23	Computer Specifications - 1. Processor: Intel i3 or better 2. Memory: 4GB RAM 3. Storage: 160GB HDD 4. Video Card: 512MB Graphic card	Desired		
24	Other Features 1. Multi energy imaging (4 colour palette) 2. Crystal clear images 3. Black & white viewing 4. Organic/ inorganic stripping 5. High penetration 6. Variable edge enhancement 7. Zoom 32 X or more	Desired		

Sl. No	Requirement	Mandatory / Desired	Compliance (Yes /No)	Remark (If any)
	8. Facility to view the previous bag 9. Manual image archive 10. Configurable image processing keys 11. Facility to count baggage 12. Date /time display 13. Have search indicator 14. Have facility of high-density alert (HDA) 15. Manual Scan facility 16. Automatic image archiving			
25	Film Safety: Guaranteed safety for high-speed films up to ISO1600. The machines should be film safe. In other words, photographic films must not be damaged due to x-ray examination	Desired		
26	Threat image projection (TIP)	Desired		
27	Input/ Output Rollers - 0.5 Mtr length each	Desired		

11.2. IT Infrastructure

11.2.1. Server Type 1 – Rack Server

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	Form factor	Maximum 2U rack mount server with Bezel, Bezel Locking Kit, Chassis Intrusion Detection Kit, Sliding rails, AC power cords and accessory patch cords (5 or higher meters).		
2	Processor	Minimum 2 X Latest 5th Generation 2.2GHz, 64-core minimum, 320MB or higher L3 cache, 4 UPI or higher. 64-bit x86 processor fully binary compatible with 64/32-bit applications and supporting hyper-threading. Number of		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		cores on a single die/socket will be treated as a single processor.		
3	Memory	2 TB RDIMM/LRDM, DDR5 DIMM in balanced configuration scalable up to 4TB. Minimum 6400 MT/s.		
		Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module.		
4	Memory RAS	Adaptive Double DRAM Device Correction (ADDDC), online spare, mirroring, and Fast Fault Tolerance.		
5	Storage	Tri-mode SAS/SATA/NVMe RAID controller with minimum 4GB or higher cache, & RAID 1/5/6/10/50/60 support. The offered controller must support mix-and-match up to 8 no's 12G SAS, 6G SATA, and 16G NVMe drives to the same controller.		
	Controller	Offered Storage controller must support:		
		a) Immutable Hardware root of trust		
		b) Expand & Move Logical Drive		
		c) Configurable stripe size up to 1 MB		
		d) Instant Secure Erase		
		e) Migrate RAID/Stripe Size		
		f) Modifying Cache Write Policy		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		g) SSD wear gauge.		
		h) Re-enable Failed Logical Drive		
6	Disk drives	2 x 960GB NVMe SSD for Boot/Hypervisor.		
7	Graphics	Video modes up to 1920 x 1200@60Hz (32 bpp).		
8	LAN port	4 x 1G (RJ-45), 2 x 2-port 25G (SR), 2 x 2-port 32G FC (SW)		
9	OS & Hypervisor Certification	Certified for latest version of Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Ubuntu, Microsoft Windows Server, HVM, and VMWare.		
10	Power supply	Minimum Hot Plug Redundant power supplies of maximum 2kW or better with minimum 94% or better efficiency.		
11	Fans/blower	Fully populated redundant (N+1) hot-swap fans system		
12	Other interfaces	Minimum 1 x 1Gbps Dedicated OOB system management port (RJ-45), 1 x video port, 4 x USB 3.0/higher ports		
13	Driver/ Software Utilities	All required device drivers for OS installation/System Configuration and Server Management. Offered server management software shall be with perpetual licensing.		
14	System Compliances	ACPI 6.3, PCIe 5.0, SMBIOS 3.2, UEFI 2.7, IPMI 2.0, AES, 3DES, SNMP v3, TLS 1.2, SMASH CLP, RESTful API, ASHRAE A3/A4		
		Continuous, proactive health monitoring as well as notification		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		of actual or impending component failure alerts on key internal server components such as CPUs, memory, temperature, fans, RAID controllers, hard drives (including cache modules) and power supplies.		
15	System BIOS	The system should boot with & run BIOS from the same server hardware OEM (manufacturer). All updates should happen only using quoted OEM's access controller & perpetual management software to enforce security.		
16	Server System Security	Immutable Silicon-based Hardware Root of Trust meeting to or exceeding FIPS 140-3 Level 3 requirements. TPM 2.0, CNSA		
		UEFI Secure Boot and Secure Start along with Runtime Firmware Validation		
		One-button/click Secure erase of NAND/user data		
		Server should have security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features		
		It should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		update of system software/firmware components. Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline.		
17	System management	System management software should be from the same server hardware OEM. System management software shall be with perpetual license.		
		Should provide a Server workload-performance advisor to enable/help in server tuning recommendations to improve server performance		
		System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using any USB/CD/DVD Drive. It should be capable of offering upgrades of software and patches from a remote client using Media/image/folder.		
		Server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
18	Serviceability	System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
19	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		
20	IDC Ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for server.		

11.2.2. Server Type II – Rack server with GPU

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	Form factor	Maximum 2U rack mount server with Bezel, Bezel Locking Kit, Chassis Intrusion Detection Kit, Sliding rails, AC power cords and accessory patch cords (5 or higher meters).		
2	Processor	Minimum 2 X Latest 5th Generation 2.2GHz, 64-core minimum, 320MB or higher L3 cache, 4 UPI or higher. 64-bit x86 processor fully binary compatible with 64/32-bit applications and supporting		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		hyper-threading. Number of cores on a single die/socket will be treated as a single processor.		
3	Memory	2 TB RDIMM, DDR5 DIMM in balanced configuration scalable up to 4TB. Minimum 6400 MT/s.		
		Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module.		
4	Memory RAS	Adaptive Double DRAM Device Correction (ADDDC), online spare, mirroring, and Fast Fault Tolerance.		
5	Storage Controller	Tri-mode SAS/SATA/NVMe RAID controller with minimum 4GB or higher cache, & RAID 1/5/6/10/50/60 support. The offered controller must support mix-and-match up to 8 no's 12G SAS, 6G SATA, and 16G NVMe drives to the same controller.		
		Offered Storage controller must support:		
		a) Immutable Hardware root of trust		
		b) Expand & Move Logical Drive		
		c) Configurable stripe size up to 1 MB		
		d) Instant Secure Erase		
		e) Migrate RAID/Stripe Size		
		f) Modifying Cache Write Policy		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		g) SSD wear gauge.		
		h) Re-enable Failed Logical Drive		
6	Disk drives	2 x 960GB NVMe SSD for Boot/Hypervisor.		
7	Graphics	Video modes up to 1920 x 1200@60Hz (32 bpp).		
		2 x NVIDIA L40S 48GB or latest or higher GPU accelerators from day 1.		
8	LAN port	4 x 1G (RJ-45), 2 x 2-port 25G (SR), 2 x 2-port 32G FC (SW)		
9	OS & Hypervisor Certification	Certified for latest version of Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Ubuntu, Microsoft Windows Server, HVM, and VMWare.		
10	Power supply	Minimum Hot Plug Redundant power supplies of maximum 2kW or better with minimum 94% or better efficiency.		
11	Fans/blower	Fully populated redundant (N+1) hot-swap fans system		
12	Other interfaces	Minimum 1 x 1Gbps Dedicated OOB system management port (RJ-45), 1 x video port, 4 x USB 3.0/higher ports		
13	Driver/ Software Utilities	All required device drivers for OS installation/System Configuration and Server Management. Offered server management software shall be with perpetual licensing.		
14	System Compliances	ACPI 6.3, PCIe 5.0, SMBIOS 3.2, UEFI 2.7, IPMI 2.0, AES, 3DES, SNMP v3, TLS 1.2,		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		SMASH CLP, RESTful API, ASHRAE A3/A4		
		Continuous, proactive health monitoring as well as notification of actual or impending component failure alerts on key internal server components such as CPUs, memory, temperature, fans, RAID controllers, hard drives (including cache modules) and power supplies.		
15	System BIOS	The system should boot with & run BIOS from the same server hardware OEM (manufacturer). All updates should happen only using quoted OEM's access controller & perpetual management software to enforce security.		
16	Server System Security	Immutable Silicon-based Hardware Root of Trust meeting to or exceeding FIPS 140-3 Level 3 requirements. TPM 2.0, CNSA		
		UEFI Secure Boot and Secure Start along with Runtime Firmware Validation		
		One-button/click Secure erase of NAND/user data		
		Server should have security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		It should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components. Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline.		
17	System Management	System management software should be from the same server hardware OEM. System management software shall be with perpetual license.		
		Should provide a Server workload-performance advisor to enable/help in server tuning recommendations to improve server performance		
		System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using any USB/CD/DVD Drive. It should be capable of offering upgrades of software and patches from a remote client using Media/image/folder.		
		Server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		delivering rapid resolution when system failures occur		
18	Serviceability	System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
19	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		
20	IDC Ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for server.		

11.2.3. SAN Storage

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	Architecture	a) Minimum four storage controllers/ Nodes configured in Active-Active mode.		
		b) Offered storage should support RAID6 or equivalent with automatic failover.		
		c) Failure of any controller should not affect the path availability and working connectivity between storage system and devices.		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		d) Offered system should be configured in such a way that single volume/disk shall be accessible by all the offered controllers.		
		e) Offered storage array should have 99.9999% data availability guaranteed architecture and All Flash end-to-end NVMe array only. Shall be marketed / Publish as All NVMe array on the vendor website.		
2	Capacity	Proposed storage must be offered with minimum 2PiB (±1%) usable capacity using NVMe SSD Drives in RAID 6 excluding all overheads like RAID parity and file system. Vendor shall use not more than RAID-6 (14+2) while configuring the solution. An additional global hot spare drive/capacity of same drive capacity for every thirty drives should be configured.		
3	Expandability	a) Offered storage should be scalable up to minimum 4PiB (±1%) usable capacity with the proposed storage configuration from DAY-1.		
		b) Proposed system to be configured in such a way that only NVMe drives would be required to meet the capacity scalability mentioned above.		
		c) Offered storage array shall be supplied with four controllers from day 1 without clustering/federation technology and it shall be truly shared, everything architecture so that all the existing drives shall be		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		physically visible and mapped across all 4 controllers.		
4	System	No single point of failure (NSPOF); Online firmware upgrades; Remote diagnostic support.		
	Availability			
5	Host Ports	Storage solutions should be supplied with minimum port configuration as follows:		
		a) FC Ports: 16 x 32 Gb		
		b) iSCSI ports: 4 x 10Gb		
		c) 4 x 10 Gbps ports for replication (In case proposed storage doesn't have native ports for replication, FCIP router shall be provided, if required at no extra cost to end-user).		
6	Backend Ports	The storage offered shall have at least 400Gb NVMe of enabled bandwidth for drive enclosure connectivity and shall preferably be scalable to 800Gb enabled bandwidth NVMe of ports.		
7	Controller	Minimum 1TB DRAM/Memory across all the controllers. Write operations shall be completely protected and there shall be no data loss in case of power failure		
	Memory			
8	Protocol	a) The storage solution should support FC and iSCSI for Block.		
	Support	b) The proposed storage must be based on NVMe architecture. The offered array should be end-to-end NVMe including NVMe based backend as well as NVMe over fabric for front-end connectivity.		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		c) Proposed storage should be configured with NVMe OF (NVMe over FC) protocol		
9	Chassis	Rack Mountable with Hot Swap Redundant Power Supply & Cooling Fans; All necessary cables and accessories to connect Storage System to Servers / SAN Switch		
10	Multi-Path	Should support Multipath from SAN to Server or vice versa. Any software required should be supplied		
11	Data-Encryption	Vendor offers data encryption using encrypted drives/controllers based on appropriate encryption licenses.		
12	Data-Efficiency	The storage array offered shall support the inline data efficiency engine (Thin provisioning, Thin Re-Claim, Deduplication & Compression) and shall be enabled by default. Vendors should have flexibility to enable and disable the data efficiency engine at the time of Volume creation. In the absence of Thin reclaim feature, Storage OEM to factor required proactive quarterly OEM services for thin reclamation at OS and Virtualization level. Relevant Service part codes to be submitted.		
13	DR-Support	a) Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively using software-based solution. MAF for the replication software solution		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		should be provided by storage OEM.		
		b) Offered Storage array shall support 3-DC solution natively where Primary site shall be able to replicate synchronously to near-by / Bunker location and at the same time, shall be able to replicate to Far location asynchronously. If vendors don't support this functionality natively, it needs to quote required hardware and software from DAY-1		
		c) Replication shall support incremental replication after resumption from link failure or failback situations.		
14	Thin-Provisioning	For effective on-prem/cloud deployment, storage offered should be supplied with thin provisioning to make the volume thin for an extended period for a complete array supported raw capacity.		
15	Snapshot/PIT-Copy/Clone	a) Offered Storage shall support making the snapshot/clones.		
		b) The storage array should have support for controller-based snapshots (At-least 1000 copies for a given volume).		
		c) Storage Array shall have functionality to re-claim the space from thin provisioned deleted snapshot.		
		d) Storage Array shall have functionality to create virtual lock for retention of read-only snapshots to		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		protect against accidental deletes and Cybercrime incidents.		
		e) Storage Array shall have integration with at least three independent Backup ISV apps such as Commvault, Micro Focus, Veritas, Veeam, etc. for efficient backup.		
16	OS & Clustering	RHEL, SLES, Windows Server, HVM, VMware, etc.		
17	Analytics	Cloud / On-Prem enabled Analytics engine shall have capability to provide following:		
		a) Analytics engine shall have the capability of proactive recommendation for arresting the issues / problems and proactive creation of support tickets.		
		b) Providing granular historical capacity and performance trend analysis.		
		c) Providing overall saturation level of the array while combining while analysing various parameters like IOPS, MB/sec, Block size etc.		
		d) Providing the status of at least top volumes where latency is extremely high.		
18	QOS – Quality of Service	1) Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units a t storage. It shall be possible to define different service / response time for different application logical units.		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		2) Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical unit of application running at storage array.		
		3) It shall be possible to change the quality-of-service Response time (In both milliseconds as well as Sub milliseconds), IOPS, bandwidth specification at real time.		
19	Performance	The proposed storage configuration shall provide minimum 350K+ IOPS with 70:30 RW ratio with 16KB block size with microsecond response time with all data efficiency features (Compression, Deduplication, Thin Provisioning) enabled. Vendors shall not use clustering/federation technology to meet this requirement.		
20	Performance Monitoring	Storage management software should provide real time monitoring and historical analysis of storage performance data such as total IOPS, read%, write %, cache-hit %, throughput, etc. for analysing performance of the systems.		
21	Software Features & Licensing	a) Proposed Storage subsystem shall be supplied with all features and licenses to achieve these functionalities from day 1.		
		b) Single GUI & WEB based remote management; Should be capable of creating, expand & move volumes dynamically; Support for dynamic LUN expansion. Management		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		Software and Licenses to be supplied for full capacity.		
22	VAAI	Storage must be complied with VMware API for Array Integration, and it should support following functionalities:		
		A) Offered storage array shall be tightly integrated with VMware and shall be certified for VVOL.		
		B) Offered Storage array VASA provider shall be certified by VMware for VVOL - Storage based replication.		
23	Container Integration	The Storage array offered shall be integrated with Red-hat OpenShift, Kubernetes and other industry K8 based container platform through CSI driver set. Vendors should support at least following functionalities through their CSI / CSP integration:		
		A. Shall support both Static and Dynamic provisioning		
		B. Shall be able to expand, re-size the persistent volumes given to stateful set applications.		
		C. Shall be able to create and delete the snapshots		
		D. Shall support CSI Raw block volume as well as CSI Volume cloning.		
		E. Support for both Fiber channel as well as ISCSI		
		F. Support for dynamic NFS provisioning to dynamically create persistent volumes		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		G. Should support major leading containerization service OEMs during integration/transition.		
24	OEM Ranking	The proposed Storage OEM must be rated as Leader's in the latest magic quadrants for Primary Storage by Gartner.		
25	Storage Replication	Proposed storage shall have native storage-based replication with existing 4-controller storage (HPE Alletra) at OCAC SDC, Bhubaneswar without using any additional hardware/software/middleware.		
		Proposed Storage shall have capability to provide true Active / Active Replication and Stretch clustering at metro distances for Zero RPO and RTO so that a given volume pair between both such storage-units can have concurrent access to both read and write operations simultaneously.		
		Proposed storage shall also have the capability to replicate the data to public cloud instance of the storage using native storage-based replication. A single-pane-of-glass management should be available for all such storage instances across DC, DR, and public-cloud.		
26	Multi-tenancy	Proposed storage shall be true multi-tenant and shall support at-least 128 tenants. Every tenant shall be treated as a separate logical storage array with its own user control access.		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		Proposed storage shall have built-in ransomware detection integrated into the storage operating system software.		
		Proposed storage can identify encrypted incoming I/O's in real time, generating quick alerts for potential ransomware threats using anomaly detection methods. This advanced detection technology is dynamic and adaptive, capable of detecting both traditional ransomware and newer.		
27	Cyber Resiliency	Ransomware detection is activated on a virtual storage volume in the source storage system, and it can also be enabled on the corresponding volume in the target replication storage system.		
		Proposed storage shall support integration with third-party security solutions, including security information and event management (SIEM) and extended detection and response (XDR).		
		Proposed storage must provide the capability to create compliant, immutable, read-only snapshots, which makes it impossible to modify or delete the snapshot and its base volume by the user, a system administrator, and the manufacturer.		
28	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their		

Sl. No	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		own support portal to log the case online and historical data about cases must be available in the same portal.		
		During Five Years on-site comprehensive OEM Warranty OEM should perform Storage OS, patches, Firmware, and related updates proactively. OEM should inform the client about the updates released from time to time.		
29	IPV6	All devices should be implemented with IPv6 ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		

11.2.4. SAN Switch

Sl.	Minimum Specification	Compliance (Yes/No)	Compliance with Cross reference Page No.
1	Proposed SAN switch shall be configured with 48 x 32G FC Ports. Minimum 5-mtrs OM4 Duplex LC-LC OFC patch cords need to be quoted for all active ports.		
2	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only.		
3	Proposed switch Should deliver 32 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 48 ports in an energy-efficient fashion.		
4	Proposed switch Should protect existing device investments with autosensing 8, 16, and 32 Gbit/sec capabilities.		
5	The proposed switch should be rack mountable. Rack-mount kit to be included.		
6	The proposed switch shall provide an aggregate bandwidth of 1.5Tbps end to end.		
7	The proposed switch should have support for web-based management and should also support CLI.		
8	Proposed switches shall provide enterprise-class availability features such as redundant and hot pluggable components like power supply and FAN.		
9	Five years of on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		
10	All devices should be IPv6 implementation ready from day 1. OCAC will bear no extra cost for IPv6 implementation.		

11.2.5. Network Switch (L3), Type 1

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	OEM Eligibility	a. OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on "Wired and Wireless" OR "DC Switching".		
		b. OEM must have India presence for last 5 years on both Sales and Support operation.		
2	Solution Requirement	a. The Switch should support non-blocking Layer 2 switching and Layer 3 routing.		
		b. The switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy.		
		c. Switch support in-line hot insertion and removal of different parts like transceivers/power supplies/fan tray etc. should not require switch reboot and disrupt the functionality of the system.		
		d. The Switch should function in line rate and should not have any port with an oversubscription ratio applied.		
		e. The switch should have a modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability.		
		f. The switch OS should support programmability through REST-APIs/REST-CONF, Python scripting.		
		g. Switch should be supplied with Indian standard compatible IEC C13/C14 3pin power cord suitable for PDU.		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		h. Switch should be supplied with the necessary patch code for HA.		
		i. posed solution should not be declared with End-of-Life, End-of-Sale, or End-of-Support by OEM on the date of final acceptance by OCAC.		
3	IPv6	a. Switch shall be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		
		b. Switch should support the complete STACK of IPv4 and IPv6 services		
4	Hardware & interface	a. 1U 19" Rack Mountable with mounting kit included.		
		b. The switch should have dual, redundant, field replaceable, hot-swappable power supplies and field-replaceable, hot-swappable fans with airflow.		
		c. The switch should have at least 32 ports of 40G/100GbE (QSFP+/QSFP28) ports.		
		d. All 100G ports shall have 100G Bi-Directional (BiDi) Transceiver modules suitable for MMF cables with LC interface. All the transceivers should be from the same OEM as the switch. The switch should have an RJ-45 serial or USB-C console port, RJ-45 Ethernet Management port and USB Interface.		
		e. Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source.		
5	Performance	a. The proposed switch should have a minimum of 16GB DRAM, 64GB		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		SSD/Flash and 32MB Packet buffer memory.		
		b. The switch should support a minimum of 90K IPv4 routes/30K IPv6 Routes and 8K IPv4/IPv6 Multicast Routes.		
		c. The proposed switch should have switched performance of 6.4 Tbsp. There should be nonblocking capacity including the services such as: Switching, IP Routing (Static/Dynamic), IP Forwarding, Policy Based Routing, QoS, ACL, and Other IP Services including IPv6 routing.		
		d. Switch should support Graceful Restart for OSPF, BGP etc.		
		e. The switch should support switch virtualization or VPC or equivalent feature for combining dual switches into single logical unit/fabric with active-active control planes.		
		f. The switch should support a minimum of 90K IPv4 routes/30K IPv6 Routes and 7K IPv4/IPv6 Multicast Routes.		
		g. The switch should support Data centre Bridging (DCB) capability supporting Priority Flow Control (PFC), Enhanced Transmission Service (ETS).		
		h. The Switch should support advanced telemetry and automation.		
		i. The switch should support powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses.		
6	Layer 2 features	a. The switch should support the Spanning Tree Protocol (STP/		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		RSTP/MSTP) for rapid protection and recovery.		
		b. The switch should support Link Aggregation Control Protocol (LACP).		
		c. The switch should support IEEE 802.1Q VLANs (4000 VLANs).		
		d. Switch should support Jumbo Frames up to 9K Bytes on Ports.		
		e. The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds.		
		f. Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures.		
		g. The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2).		
7	Layer 3 features	a. The switch should support IPv4 and IPv6 Static Routing.		
		b. The switch should support Open shortest path first (OSPF) for IPv4 and IPv6.		
		c. The switch should support Border Gateway Protocol 4 (BGP) for IPv4 and IPv6.		
		d. Switch should support basic routing features i.e., IP Classless, default routing and Inter VLAN routing.		
		e. The switch should support Multicast Routing using PIM-SM, SSM and Multicast Service Delivery Protocol (MSDP).		
		f. The switch should support dynamic VXLAN with BGP-EVPN and VRF.		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		g. Switch should be capable of working as DHCP server or relay.		
		h. The switch should support Equal-Cost Multipath.		
8	High Availability	a. Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy.		
		b. Switch should provide gateway levels of redundancy in IPV4 and IPV6 using HSRP/VRRP.		
		Switch should support BFD For Fast Failure Detection		
9	Quality of Service	A. Switch system should support 802.1P classification and marking of packet using: CoS (Class of Service), DSCP (Differentiated Services Code Point), Source/destination IP subnet, Protocol types (IP/TCP/UDP), and Source/destination TCP/UDP ports.		
		b. Switch should support different types of QoS features for real time traffic differential treatment using: Weighted Random Early Detection and WRR/DWRR, Strict Priority Queuing, Rate Limiting, Egress queue shaping.		
		c. Switch should support trusting the QoS marking/priority settings of the end points as per the defined policy		
10	Security	a. The switch should support Secure port access like 802.1x, Mac-auth, Port-Access Policy.		
		b. Switch should support an external database for AAA using: TACACS+ & RADIUS.		
		c. Switch should support DHCP Snooping.		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		d. Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy.		
		e. Switch should support Dynamic ARP/ equivalent Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.		
		f. Switch should support Spanning tree BPDU protection.		
		g. Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined.		
		h. Switch should support the MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed.		
		i. Switch should support the IP Source Guard to prevent a malicious host 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.		
11	Management	a. Switch should support embedded RMON/RMON-II for central NMS management and monitoring.		
		b. The switch should support sFlow or equivalent for traffic analysis.		
		c. The switch should provide advanced telemetry and automation features for monitoring, troubleshooting, and improving network operations.		
		d. The switch should have Command Line Interface (CLI) with a hierarchical		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		structure and SSH, Secure FTP/TFTP support.		
		e. Switch should support sending logs to multiple centralized syslog servers for monitoring and audit trail.		
		f. Switch should provide remote login for administration using: Telnet or SSHv2.		
		g. The switch should support Port mirroring.		
		h. The switch should support Precision Time Protocol (PTP)/NTP.		
		i. Switch should support Real-time Packet Capture using Wireshark in real time for traffic analysis and fault finding.		
		j. Switch should support basic administrative tools like: Ping & Traceroute.		
		k. Switch should support management and monitoring status using different types of Industry standard NMS using: SNMP V2c/V3 & SNMP MIB support.		
12	Certifications	a. The Switch series/Switch OS should be Common Criteria Certified (EAL or NDPP).		
		b. The switch should have RoHS compliance.		
		c. The switch should have safety/emissions certifications including UL/CUL 62368, VCCI Class A, IEC 62368-1		
13	Warranty	a. All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1.		

Sl.	Parameter	Minimum Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		b. Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		

11.2.6. Network Switch (L3), Type 2

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
1	OEM Eligibility	a) OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on "Wired and Wireless" OR "DC Switching."		
		b) OEM must have India presence for last 5 years on both Sales and Support operation.		
2	Solution Requirement	a) The Switch should support non-blocking Layer 2 switching and Layer 3 routing.		
		b) The switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy.		
		c) Switch support in-line hot insertion and removal of different parts like transceivers/power supplies/fan tray etc. should not require switch reboot and disrupt the functionality of the system.		
		d) The Switch should function in line rate and should not have any port with oversubscription ratio applied.		
		e) The switch should have a modular operating system with micro-services		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		or equivalent architecture providing superior fault tolerance and high availability.		
		f) The switch OS should support programmability through REST-APIs/REST-CONF, Python scripting.		
		g) Switch should be supplied with Indian standard compatible IEC C13/C14 3pin power cord suitable for PDU.		
		h) Switch should be supplied with the necessary patch cord for HA.		
		i) posed solution should not be declared with End-of-Life, End-of-Sale, or End-of-Support by OEM on the date of final-acceptance by OCAC.		
3	IPv6	a) Switch shall be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		
		b) Switch should support the complete STACK of IPv4 and IPv6 services		
4	Hardware & interface	a) 1U 19" Rack Mountable with mounting kit included.		
		b) The switch should have dual, redundant, field replaceable, hot-swappable power supplies and field-replaceable, hot-swappable fans with airflow.		
		c) The switch should have at least 48 ports of 10G/25GbE (SFP+/SFP28) ports and 6x40/100G ports.		
		d) 25G (SR) Transceiver modules shall be offered on all 25G SFP28 ports and all 100G ports shall have 100G Bi-Directional (BiDi) Transceiver modules suitable for MMF cabling with LC		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		interface. All the transceivers should be from the same OEM as the switch. The switch should have an RJ-45 serial or USB-C console port, RJ-45 Ethernet Management port and USB Interface.		
		e) Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source.		
5	Performance	a) The proposed switch should have a minimum of 16GB DRAM, 64GB SSD/Flash and 32MB Packet buffer memory.		
		b) The switch should support a minimum of 90K IPv4 routes/30K IPv6 Routes and 8K IPv4/IPv6 Multicast Routes.		
		c) The proposed switch should have switched performance of 3.6 Tbsp. There should be nonblocking capacity including the services such as: Switching, IP Routing (Static/Dynamic), IP Forwarding, Policy Based Routing, QoS, ACL, and Other IP Services including IPv6 routing.		
		d) Switch should support Graceful Restart for OSPF, BGP etc.		
		e) The switch should support switch virtualization or VPC or equivalent feature for combining dual switches into single logical unit/fabric with active-active control planes.		
		f) The switch should support a minimum of 90K IPv4 routes/30K IPv6 Routes and 7K IPv4/IPv6 Multicast Routes.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		g) The switch should support Data Centre Bridging (DCB) capability supporting Priority Flow Control (PFC), Enhanced Transmission Service (ETS).		
		h) The Switch should support advanced telemetry and automation.		
		i) The switch should support powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses.		
6	Layer 2 features	a) The switch should support Spanning Tree Protocol (STP/ RSTP/MSTP) for rapid protection and recovery.		
		b) The switch should support Link Aggregation Control Protocol (LACP).		
		c) The switch should support IEEE 802.1Q VLANs (4000 VLANs).		
		d) Switch should support Jumbo Frames up to 9K Bytes on Ports.		
		e) The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds.		
		f) Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures.		
		g) The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2).		
7	Layer 3 features	a) The switch should support IPv4 and IPv6 Static Routing.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		b) The switch should support Open shortest path first (OSPF) for IPv4 and IPv6.		
		c) The switch should support Border Gateway Protocol 4 (BGP) for IPv4 and IPv6.		
		d) Switch should support basic routing features i.e. IP Classless, default routing and Inter VLAN routing.		
		e) The switch should support Multicast Routing using PIM-SM, SSM and Multicast Service Delivery Protocol (MSDP).		
		f) The switch should support dynamic VXLAN with BGP-EVPN and VRF.		
		g) Switch should be capable of working as DHCP server or relay.		
		h) The switch should support Equal-Cost Multipath.		
8	High Availability	a) Switch should have provisions for connecting to 1:1/N+1 power supply for usage and redundancy.		
		b) Switch should provide gateway level of redundancy in IPV4 and IPV6 using HSRP/VRRP.		
		c) Switch should support BFD For Fast Failure Detection		
9	Quality of Service	a) Switch system should support 802.1P classification and marking of packet using: CoS (Class of Service), DSCP (Differentiated Services Code Point), Source/destination IP subnet, Protocol types (IP/TCP/UDP), and Source/destination TCP/UDP ports.		
		b) Switch should support diverse types of QoS features for real time traffic differential treatment using: Weighted		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		Random Early Detection and WRR/DWRR, Strict Priority Queuing, Rate Limiting, Egress queue shaping.		
		c) Switch should support trust the QoS marking/priority settings of the end points as per the defined policy		
10	Security	a) The switch should support Secure port access like 802.1x, Mac-auth, Port-Access Policy.		
		b) Switch should support an external database for AAA using: TACACS+ & RADIUS.		
		c) Switch should support DHCP Snooping.		
		d) Switch should support control plane i.e., processor and memory Protection from unnecessary or DoS traffic by control plane protection policy.		
		e) Switch should support Dynamic ARP/ equivalent Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.		
		f) Switch should support Spanning tree BPDU protection.		
		g) Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.		
		Switch should support MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed.		
		i) Switch should support the IP Source Guard to prevent a malicious host from spoofing or taking over another host's IP address by creating a binding table		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		between the client's IP and MAC address, port, and VLAN.		
11	Management	a) Switch should support embedded RMON/RMON-II for central NMS management and monitoring.		
		b) The switch should support sFlow or equivalent for traffic analysis.		
		c) The switch should provide advanced telemetry and automation features for monitoring, troubleshooting, and improving network operations.		
		d) The switch should have Command Line Interface (CLI) with a hierarchical structure and SSH, Secure FTP/TFTP support.		
		e) Switch should support sending logs to multiple centralized syslog servers for monitoring and audit trail.		
		f) Switch should provide remote login for administration using: Telnet or SSHv2.		
		g) The switch should support Port mirroring.		
		h) The switch should support Precision Time Protocol (PTP)/NTP.		
		i) Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding.		
		j) Switch should support basic administrative tools like: Ping & Traceroute.		
		k) Switch should support management and monitoring status using different type of Industry standard NMS using: SNMP V2c/V3 & SNMP MIB support.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
12	Certifications	a) The Switch series/Switch OS should be Common Criteria Certified (EAL or NDPP).		
		b) The switch should have RoHS compliance.		
		c) The switch should have safety/emissions certifications including UL/CUL 62368, VCCI Class A, IEC 62368-1		
13	Warranty	a) All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1.		
		b) Five years of comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		

11.2.7. Network Switch (L3), Type 3

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
1	OEM Eligibility	a) OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on "Wired and Wireless" OR "DC Switching."		
		b) OEM must have India presence for last 5 years on both Sales and Support operation.		
2	Solution Requirement	a) The Switch should support non-blocking Layer 2 switching and Layer 3 routing.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		b) The switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy.		
		c) Switch support in-line hot insertion and removal of various parts like transceivers/power supplies/fan tray etc. should not require switch reboot and disrupt the functionality of the system.		
		d) The Switch should function in line rate and should not have any port with oversubscription ratio applied.		
		e) The switch should have a modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability.		
		f) The switch OS should support programmability through REST-APIs/REST-CONF, Python scripting.		
		g) Switch should be supplied with Indian standard compatible IEC C13/C14 3pin power cord suitable for PDU.		
		h) Switch should be supplied with the necessary patch cord for HA.		
		i) posed solution should not be declared with End-of-Life, End-of-Sale, or End-of-Support by OEM on the date of final-acceptance by OCAC.		
3	IPv6	a) Switch shall be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		b) Switch should support the complete STACK of IPv4 and IPv6 services		
4	Hardware & interface	a) 1U 19" Rack Mountable with mounting kit included.		
		b) The switch should have dual, redundant, field replaceable, hot-swappable power supplies and field-replaceable, hot-swappable fans with airflow.		
		c) The switch should have at least 24 ports of 10G/25GbE (SFP+/SFP28) ports and 4x40/100G ports.		
		d) 25G (SR) Transceiver modules shall be offered on all 25G SFP28 ports and all 100G ports shall have 100G Bi-Directional (BiDi) Transceiver modules suitable for MMF cabling with LC interface. All the transceivers should be from the same OEM as the switch. The switch should have RJ-45 serial or USB-C console port, RJ-45 Ethernet Management port and USB Interface.		
		e) Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source.		
5	Performance	a) The proposed switch should have minimum 16GB DRAM, 64GB SSD/Flash and 32MB Packet buffer memory.		
		b) The switch should support minimum 90K IPv4 routes/30K		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		IPv6 Routes and 8K IPv4/IPv6 Multicast Routes.		
		c) The proposed switch should have switching performance of 1.6 Tbsp. Should be nonblocking capacity including the services such as: Switching, IP Routing (Static/Dynamic), IP Forwarding, Policy Based Routing, QoS, ACL, and Other IP Services including IPv6 routing.		
		d) Switch should support Graceful Restart for OSPF, BGP etc.		
		e) e) The switch should support switch virtualization or VPC or equivalent feature for combining dual switches into single logical unit/fabric with active-active control planes.		
		f) The switch should support minimum 90K IPv4 routes/30K IPv6 Routes and 7K IPv4/IPv6 Multicast Routes.		
		g) The switch should support Data Centre Bridging (DCB) capability supporting Priority Flow Control (PFC), Enhanced Transmission Service (ETS).		
		h) The Switch should support advanced telemetry and automation.		
		i) The switch should support powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
6	Layer 2 features	a) The switch should support Spanning Tree Protocol (STP/ RSTP/MSTP) for rapid protection and recovery.		
		b) The switch should support Link Aggregation Control Protocol (LACP).		
		c) The switch should support IEEE 802.1Q VLANs (4000 VLANs).		
		d) Switch should support Jumbo Frames up to 9K Bytes on Ports.		
		e) The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds.		
		f) Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures.		
		g) The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2).		
7	Layer 3 features	a) The switch should support IPv4 and IPv6 Static Routing.		
		b) The switch should support Open shortest path first (OSPF) for IPv4 and IPv6.		
		c) The switch should support Border Gateway Protocol 4 (BGP) for IPv4 and IPv6.		
		d) Switch should support basic routing features i.e. IP Classless, default routing and Inter VLAN routing.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		e) The switch should support Multicast Routing using PIM-SM, SSM and Multicast Service Delivery Protocol (MSDP).		
		f) The switch should support dynamic VXLAN with BGP-EVPN and VRF.		
		g) Switch should be capable of working as DHCP server or relay.		
		h) The switch should support Equal-Cost Multipath.		
8	High Availability	a) Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy.		
		b) Switch should provide gateway level of redundancy in IPV4 and IPV6 using HSRP/VRRP.		
		c) Switch should support BFD For Fast Failure Detection		
9	Quality of Service	a) Switch system should support 802.1P classification and marking of packet using: CoS (Class of Service), DSCP (Differentiated Services Code Point), Source/destination IP subnet, Protocol types (IP/TCP/UDP), and Source/destination TCP/UDP ports.		
		b) Switch should support diverse types of QoS features for real time traffic differential treatment using: Weighted Random Early Detection and WRR/DWRR, Strict Priority Queuing, Rate Limiting, Egress queue shaping.		
		c) Switch should support trust the QoS marking/priority settings of the end points as per the defined policy		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
10	Security	a) The switch should support Secure port access like 802.1x, Mac-auth, Port-Access Policy.		
		b) Switch should support an external database for AAA using: TACACS+ & RADIUS.		
		c) Switch should support DHCP Snooping.		
		d) Switch should support control plane i.e., processor and memory Protection from unnecessary or DoS traffic by control plane protection policy.		
		e) Switch should support Dynamic ARP/ equivalent Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.		
		f) Switch should support Spanning tree BPDU protection.		
		g) Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined.		
		h) Switch should support MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed.		
		i) Switch should support the IP Source Guard to prevent a malicious host 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.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
11	Management	a) Switch should support embedded RMON/RMON-II for central NMS management and monitoring.		
		b) The switch should support sFlow or equivalent for traffic analysis.		
		c) The switch should provide advanced telemetry and automation features for monitoring, troubleshooting, and improving network operations.		
		d) The switch should have Command Line Interface (CLI) with a hierarchical structure and SSH, Secure FTP/TFTP support.		
		e) Switch should support sending logs to multiple centralized syslog server for monitoring and audit trail.		
		f) Switch should provide remote login for administration using: Telnet or SSHv2.		
		g) The switch should support Port mirroring.		
		h) The switch should support Precision Time Protocol (PTP)/NTP.		
		i) Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding.		
		j) Switch should support basic administrative tools like: Ping & Traceroute.		
		k) Switch should support management and monitoring status using different type of Industry standard NMS using:		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		SNMP V2c/V3 & SNMP MIB support.		
12	Certifications	a) The Switch series/Switch OS should be Common Criteria Certified (EAL or NDPP).		
		b) The switch should have RoHS compliance.		
		c) The switch should have safety/emissions certifications including UL/CUL 62368, VCCI Class A, IEC 62368-1		
13	Warranty	a) All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1.		
		b) Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		

11.2.8. Network Switch (L2), Type 4

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
1	OEM Eligibility	a) OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on "Wired and Wireless" OR "DC Switching."		
		b) OEM must have India presence for last 5 years on both Sales and Support operation.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
2	Solution Requirement	a) The Switch should support non-blocking Layer 2 switching.		
		b) The Switch should function in line rate and should not have any port with over subscription ratio applied.		
		c) The switch OS should support programmability through REST-APIs/REST-CONF, Python scripting.		
		d) Switch should be supplied with Indian standard compatible IEC C13/C14 3pin power cord suitable for PDU.		
		e) Switch should be supplied with the necessary patch cord for HA.		
		f) posed solution should not be declared with End-of-Life, End-of-Sale, or End-of-Support by OEM on the date of final-acceptance by OCAC.		
3	IPv6	a) Switch shall be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		
		b) Switch should support the complete STACK of IPv4 and IPv6 services		
4	Hardware & interface	a) 1U 19" Rack Mountable with mounting kit included.		
		b) The switch should have at least 48 ports of 1G BaseT and 4 ports of 1/10G (SFP+) ports.		
		c) 10G (SR) Transceiver modules shall be offered on all 10G SFP+ ports. Transceiver modules suitable for MMF cabling with an LC		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		interface. All the transceivers should be from the same OEM as the switch. The switch should have RJ-45 serial or USB-C console port.		
		d) Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source.		
5	Performance	a) The proposed switch should have a minimum of 4GB DRAM, 16GB SSD/Flash and 12MB Packet buffer memory.		
		b) The proposed switch should have switch performance of 176 Gbps.		
		c) The switch should support powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses.		
6	Layer 2 features	a) The switch should support Spanning Tree Protocol (STP/ RSTP/MSTP) for rapid protection and recovery.		
		b) The switch should support Link Aggregation Control Protocol (LACP).		
		c) The switch should support IEEE 802.1Q VLANs (1000 VLANs).		
		d) Switch should support Jumbo Frames up to 9K Bytes on Ports.		
		e) The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		f) Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures.		
		g) The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2).		
7	Quality of Service	a) Switch system should support 802.1P classification and marking of packet using: CoS (Class of Service), DSCP (Differentiated Services Code Point), Source/destination IP subnet, Protocol types (IP/TCP/UDP), and Source/destination TCP/UDP ports.		
		b) Switch should support diverse types of QoS features for real time traffic differential treatment using: Weighted Random Early Detection and WRR/DWRR, Strict Priority Queuing, Rate Limiting, Egress queue shaping.		
		c) Switch should support trust the QoS marking/priority settings of the end points as per the defined policy		
8	Security	a) The switch should support Secure port access like 802.1x, Mac-auth, Port-Access Policy.		
		b) Switch should support an external database for AAA using: TACACS+ & RADIUS.		
		c) Switch should support DHCP Snooping.		
		d) Switch should support control plane i.e., processor and memory		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		Protection from unnecessary or DoS traffic by control plane protection policy.		
		e) Switch should support Dynamic ARP/ equivalent Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.		
		f) Switch should support Spanning tree BPDU protection.		
		g) Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.		
		h) Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed.		
11	Management	a) Switch should support for embedded RMON/RMON-II for central NMS management and monitoring.		
		b) The switch should support sFlow or equivalent for traffic analysis.		
		c) The switch should provide advanced telemetry and automation features for monitoring, troubleshooting, and improving network operations.		
		d) The switch should have Command Line Interface (CLI) with a hierarchical structure and SSH, Secure FTP/TFTP support.		
		e) Switch should support sending logs to multiple centralized syslog server for monitoring and audit trail.		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		f) Switch should provide remote login for administration using: Telnet or SSHv2.		
		g) The switch should support Port mirroring.		
		h) The switch should support Precision Time Protocol (PTP)/NTP.		
		i) Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding.		
		j) Switch should support basic administrative tools like: Ping & Traceroute.		
		k) Switch should support management and monitoring status using different type of Industry standard NMS using: SNMP V2c/V3 & SNMP MIB support.		
12	Certifications	a) The switch should have RoHS compliance.		
		b) The switch should have safety/emissions certifications including UL/CUL 62368, VCCI Class A, IEC 62368-1		
13	Warranty	a) All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1.		
		b) Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical		

Sl.	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		data about cases must be available in the same portal.		

11.2.9. Disk Backup Appliance

Sl.No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1.	Proposed Disk to disk backup device shall be Modular design to allow configuration, add capacity increase performance.		
2.	Proposed appliance shall be certified to work with at-least 3 Backup application vendor ISV like HPE Zerto, Veeam, Commvault etc.		
3.	Proposed appliance shall be offered with Minimum of 500TB of usable space		
4.	Proposed appliance shall also be scalable to at-least 1PB usable in native mode (Without de-duplication and compression)		
5.	Vendor shall not use any additional staging device in-between while moving the data from Disk based backup device to public cloud or object storage.		
6.	Proposed appliance should have separate dedicated drives for Operating System of appliance and shall not participate in data backup.		
7.	The vendor shall configure at-least 30TB space on SSD for data caching operation. This space shall be additional to the above raw capacity asked in the RFP.		
8.	Proposed appliance shall be protected with hardware RAID 6 from the factory so that no raid configuration is required in field for data drives.		
9.	Proposed appliance shall support emulation of both VTL and NAS target like NFS and CIFS.		
10.	Proposed appliance shall have capability to do complete copy of data sets from on premise disk backup storage to Cloud storage instead of data tiering.		
11.	Proposed appliance shall have the ability to configure at-least combination of 128 tape Libraries & NAS targets		

Sl.No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	along with 1,000,000 or more Cartridge slots in the single appliance.		
12.	Proposed appliance shall have capability to deliver selective restore from disk Library itself.		
13.	Proposed appliance shall have integrated de-duplication license, low bandwidth replication license so that only unique non duplicated block transfers to remote / DR location.		
14.	Proposed appliance shall have intelligence to understand both sources based, and target based de-duplication and shall be integrated with all well-known backup ISVs. At-least 3 ISVs shall be supported.		
15.	Proposed appliance shall have Minimum of 4 x 25 Gbps SFP IP ports & 4 x 32Gbps ports. License and SFP for all ports shall be offered and configured.		
16.	Proposed appliance Fiber channel ports shall support connectivity of servers either directly or via SAN switches while supporting both source and Target based de-duplication.		
17.	Proposed appliance shall also support encryption functionality.		
18.	Proposed appliance shall also support dual authorization for preventing disruptive operations so that hackers shall not be able to execute or complete all critical operations like deletion of backup store, changing system time etc.		
19.	Dual authorization shall be independent of Backup ISV being used in the environment.		
20.	Proposed appliance shall also support Secure erase feature for protecting against unauthorized recovery of deleted data		
21.	Proposed appliance shall support rated write performance of at-least 100TB per hour.		
22.	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for storage.		
23.	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to		

Sl.No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	log the case online and historical data about cases must be available in the same portal.		

11.2.10. Backup & Appliance and Software

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1.	Proposed Disk to disk backup device shall be Modular design to allow configuration, add capacity increase performance.		
2.	Proposed appliance shall be certified to work with at-least 3 Backup application vendor ISV like HPE Zerto, Veeam, Commvault etc.		
3.	Proposed appliance shall be offered with Minimum of 300TB of usable space		
4.	Proposed appliance shall also be scalable to at-least 1PB usable in native mode (Without de-duplication and compression)		
5.	Vendor shall not use any additional staging device in-between while moving the data from Disk based backup device to public cloud or object storage.		
6.	Proposed appliance shall have separate dedicated drives for Operating System of appliance and shall not participate in data backup.		
7.	Vendor shall configure at-least 30TB space on SSD for data caching operation. This space shall be additional to above raw capacity asked in the RFP.		
8.	Proposed appliance shall be protected with hardware RAID 6 from the factory so that no raid configuration is required in field for data drives.		
9.	Proposed appliance shall support emulation of both VTL and NAS target like NFS and CIFS.		
10.	Proposed appliance shall have capability to do complete copy of data sets from on premise disk backup storage to Cloud storage instead of data tiering.		
11.	Proposed appliance shall have the ability to configure at-least combination of 128 tape Libraries & NAS targets		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	along with 1,000,000 or more Cartridge slots in the single appliance.		
12.	Proposed appliance shall have capability to deliver selective restore from disk Library itself.		
13.	Proposed appliance shall have integrated de-duplication license, low bandwidth replication license so that only unique non duplicated block transfers to remote / DR location.		
14.	Proposed appliance shall have intelligence to understand both source based, and target based de-duplication and shall be integrated with all well-known backup ISVs. At-least 3 ISVs shall be supported.		
15.	Proposed appliance shall have Minimum of 4 x 25 Gbps SFP IP ports & 4 x 32Gbps ports. License and SFP for all ports shall be offered and configured.		
16.	Proposed appliance Fiber channel ports shall support connectivity of servers either directly or via SAN switches while supporting both source and Target based de-duplication.		
17.	Proposed appliance shall also support encryption functionality.		
18.	The proposed appliance shall also support dual authorization for preventing disruptive operations so that hackers shall not be able to execute or complete all critical operations like deleting backup store, changing system time etc.		
19.	Dual authorization shall be independent of Backup ISV being used in the environment.		
20.	Proposed appliances shall also support Secure erase feature for protecting against unauthorized recovery of deleted data		
21.	The proposed appliance shall support rated write performance of at-least 100TB per hour.		
22.	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for storage.		
23.	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		

11.2.11. Virtualization Software with Cloud Management

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1.	Bidders shall propose direct back-to-back OEM support on a 24 x 7 x 365 coverage basis for the proposed solution with an unlimited number of incidents.		
2.	Bidders shall propose “Plan, Design and Implementation Services (Professional Services)” from the software OEM. Software OEM shall not subcontract such professional services to any third party. OEM engineers designing, deploying, and implementing the solution shall have to be on the payroll of the software OEM.		
3.	Bidders shall ensure that the resources required for management components are called out and are deployed on a separate dedicated infrastructure (management cluster) as per best practice.		
4.	The bidder shall ensure that all the proposed software components as part of the solution shall have the ability to run on any standard commodity server infrastructure and external FC storage without having any dependence on specific make/model of infrastructure components.		
5.	Bidders should propose Virtualization, Container runtime & cloud management solution from the same OEM for interoperability as well as single-window TAC support. Bidder shall submit an undertaking from their proposed cloud management software OEM for overall ownership of installation, commissioning, integration, and support during asked contract duration of 5-years post customer-acceptance date for all the three stacks – Virtualization, Container runtime and cloud management		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	along with cloud-management software supported codeless integrations with other IT-infra components.		
6.	Bidders shall ensure that offered solution is configured in multi-node high-availability and unavailability of any node shall not stop the services of the offered platform components.		
7.	Proposed multi-node highly available management cluster should be ready for cross-region distributed-HA so as to achieve a zero-downtime always-on availability of cloud management software across DC & DR wherein the DR site can be either on-premises or hosted with any public cloud such as AWS or Azure.		
	Virtualization		
8.	Proposed virtualization software shall be qualified for both Intel as well as AMD architecture and shall have capability to provide high availability.		
9.	Proposed virtualization software shall be supported with all leading Guest Operating Systems.		
10.	Proposed virtualization solution shall support migration of a running virtual machine from one host to another within the same cluster with zero downtime.		
11.	Proposed virtualization solution shall automatically restart virtual machines on another host in the same cluster in the event of an unexpected host failure within the cluster.		
12.	Proposed virtualization shall dynamically schedule the placement of virtual machines within a cluster based upon optimal workload distribution across the cluster.		
13.	Proposed virtualization should support container and OpenStack integration for cloud native application from day 1. must be a cloud native platform ready from day one		
14.	Proposed virtualization Management software should be available independent of failure of host/node, and OS.		
15.	Proposed virtualization shall support migration the virtual disk(s) of a running of virtual machine from one storage datastore to another with zero downtime.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
16.	Proposed virtualization shall include suitable data backup solution which shall be able to protect VM and Hosts to Target Storage provider. Offered backup engine shall be able to use at least CIFS, NFS, S3 from Storage providers as a backup target.		
17.	Proposed virtualization shall also have functionality to integrate with third party backup software like Veeam, Commvault, Rubrik, Zerto etc.		
18.	The offered backup engine shall have deep integration into the instances / VM provisioning so that all newly created instances / VMs are protected and backed up automatically.		
19.	The offered backup engine shall also support critical features like Scheduling of backup, backup retention counts, on-demand backup etc.		
20.	Proposed virtualization shall support and integrate with storage - Object Buckets which can be used for Backup, Archives, Deployment and Virtual Images storage targets.		
21.	It shall be possible to browse, upload, download, or delete files from Bucket and shall support all well-known object storage from AWS, Azure, Google, Dell-EMC ECS, OpenStack Swifts buckets etc.		
22.	Proposed virtualization shall also allow creation of file share based NFS and CIFS protocols which can be used for Backup, Archives, Deployment and Virtual Images storage targets. It shall be possible to browse, upload, download, or delete files from File share and shall support all various file share protocols like CIFS, NFS, Local Storage and all well-known industry leading file storage arrays.		
23.	Proposed virtualization shall support running virtual machines on external storage via iSCSI, NFS, and Fibre Channel.		
24.	Proposed virtualization management engine shall have a concept of grouping resources into a common identity, comprises of resources like Clouds, hosts, VMs,		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	network, resource pools, data stores etc. so that required users can be assigned to it.		
25.	Proposed virtualization management engine shall allow users to configure their photo, username, password, email, theme, 2FA, Linux and Windows VM login credentials from the console		
26.	Proposed virtualization management engine shall support additional private cloud provider and hypervisor, preferably VMware, from the common interface without any additional coding.		
27.	Proposed virtualization Management engine shall allow administrator to create service plan or t-shirt size based on CPU, Memory and Storage and shall be available to users while creating / provisioning the instance / VMs		
28.	Services plan shall also have the option to provide custom ranges and flexibility to provisioning users for providing predefined limit for number of additional volumes, customization of Volumes, number of cores etc.		
29.	Proposed virtualization shall have internal user management engine, integration with external directory-based providers – Active directory and LDAP, SAML based providers – Okta, OneLogin, Azure AD SAML etc. It shall be possible for mapping of External integration provider users with offered hypervisor roles.		
30.	Proposed virtualization shall have Integration with external IPAM providers like Infoblox, phpIPAM, BlueCat, SolarWinds etc. to automate the reservation of an IP address for the virtual machine during the provisioning process.		
31.	Proposed virtualization shall have Integrate with external DNS providers like Infoblox, Microsoft DNS, BlueCat, SolarWinds etc. to automate the creation of DNS records for a virtual machine during the provisioning process.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
32.	Proposed virtualization shall execute Bash or PowerShell scripts during virtual machine provisioning to automate system bootstrapping operations.		
33.	Proposed virtualization shall also support the execution of Bash and PowerShell scripts on provisioned and discovered virtual machines like an operational workflow.		
34.	Access to grouping of resources shall be controlled through appropriate roles while assigning to users. Roles shall provide access to resources using appropriate permissions. At-least, it shall be possible to configure following key permissions:		
	a) Access to Native data protection configuration.		
	b) Read or full access for creation of Service plans.		
	c) Access to API to executes scripts on Instances / VM.		
	d) Access for allowing users to use Dynamic workload schedular for VM placement and pinning of VM to a specific host.		
	e) Access for creating the automation scripts.		
	f) Permission for resizing the instance.		
	g) Access to instance / VM – Console, Adding or deleting an Instance / VM.		
35.	Proposed virtualization shall support below features for Virtual Machine Management:		
	a) Create / Delete / Restart / Start / Stop / Suspend and Discovery of Virtual machines.		
	b) Snapshot operations – Create / Delete / revert of Virtual machines		
	c) Tagging – Add / Delete / Edit tagging for Virtual Machines.		
	d) Live Migration of VM, VM HA and Pin virtual machine to a specific host.		
	e) Cloning of VM, Clone to VM Template.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	f) Virtual Hardware Management - Add and remove virtual hardware such as hard disks, network interfaces, CPU, and memory from a managed virtual machine.		
36.	Proposed virtualization shall support both expansion and shrinking of VM cluster.		
37.	Proposed virtualization shall support both internal and external Credential store for securely pulling in the username and password, access, and secret key along with key pair and SSH certificates.		
38.	Proposed virtualization software shall provide the flexibility to bring / upload OS images. While uploading the OS image, it shall be possible to define the location and provide the flexibility to use internal space within the hypervisor cluster or using appropriate available S3 bucket or file share.		
39.	Proposed virtualization shall provide global search to facilitate search of Instances, Users, cloud, group, hosts, and networks.		
40.	Proposed virtualization shall allow creation of Wiki, which shall be RBAC-controlled, auditable Wiki that allows easy access to information, notes, configurations, or any other data needed to be referenced or shared with others.		
41.	Consolidated dashboard for the offered Hypervisor shall highlight the overall environment status, System Status, Alarms, log history, Instance status, Instance status by configured clouds, cluster workloads etc.		
42.	Proposed virtualization management engine shall provide activity reports like provisioning tasks, Users related tasks etc. It shall be able to search the specific activity.		
	Cloud Automation & Management Platform (CMP)		
43.	Proposed CMP solution shall be a persona-based platform so that following minimum required functionalities can be performed from a common cloud management platform dashboard with appropriate RBAC controls.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	a) Security and Control - Governance		
	b) Cloud operations for VM, Bare-metal and Containers		
	c) Automation and Orchestration		
	d) Visualization and optimization		
44.	Proposed CMP shall be capable of creating a cloud with secure multitenancy where each tenant shall have capability to have own uses, roles, and integration with required authentication providers like Active directory, Okta, SAML, etc.		
45.	Proposed CMP shall be truly cloud native so that resources can be managed, provisioned, and controlled with required security and role-based access for achieving the true cloud experience and agility.		
46.	Proposed CMP shall be truly heterogenous and shall quickly integrate with below tools / Platforms / integrations:		
	a) Hypervisors: VMware, Nutanix, Microsoft, HPE etc.		
	b) Clouds: AWS, Azure, GCP, IBM, Oracle, OpenStack, Alibaba, Digital Ocean etc.		
	c) Identity: MS AD, Okta, SAML, LDAP, OneLogin etc.		
	d) Network: NSX, ACI, Infoblox, Bluecat, SolarWinds etc.		
	e) Backup: Veeam, Commvault, Zerto etc.		
	f) ITSM: ServiceNow, BMC-Remedy etc.		
	g) Containers: AKS, EKS, GKE, Kubernetes, OpenShift, KVM cluster etc.		
	h) Load Balancer: F5, A10, Citrix, ALB, Azure Load Balancer etc.		
	i) Automation: Chef, Puppet, Ansible, Ansible Tower, VMware Orchestrator etc.		
47.	Proposed CMP shall offer the consistent unified console for all above integrations for self-service provisioning and life-cycle management.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
48.	Proposed CMP shall quickly enable on-prem private clouds, centralize public cloud access, deploy Kubernetes clusters, and execute automation jobs from the unified console instead of opening the separate console of above-mentioned integrations.		
49.	Consolidated dashboard for the Proposed CMP shall highlight the overall environment status, System Status, Alarms, log history, Instance status, Instance status by configured clouds, Job executions, Task executions, Backup status, cluster workloads, Activity logs etc.		
50.	Proposed CMP Platform shall have at least one deployment of minimum 500 instances across DC & DR for any government data Centre in last 3 years.		
	Security & Control – Governance		
51.	Proposed CMP shall have truly secure multi-tenant isolated environment where each tenant shall have capability for unique users, role, and workloads.		
52.	Apart from Master tenant – it shall not be possible for sub-tenant to see the resource of other subtenants.		
53.	It shall be possible to white label the subtenant as per organization requirement.		
54.	Proposed CMP shall have a concept of grouping of resources into a common identity, comprises of resources like Clouds, hosts, VMs, network, load balancers, resource pools, security groups, data stores, polices etc. so that required tenants can be assigned to it.		
55.	Access to grouping of resources shall be controlled through appropriate roles. Roles shall provide the granularity level to define the control on Groups, Application blueprints, Automation tasks, Catalog item types, instance types etc.		
56.	For true governance – roles shall have unique feature of permission access across above mentioned integration and shall support more than 100+ permissions for a given role. Vendor shall provide the documentary proof or GUI screenshots.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
57.	Role access permissions shall be configurable, but not limited to, across Group of resources, Backup, Instance types, Application blueprints, Reporting, VDI pools, Workflows, Personas, reports, and automation tools etc.		
58.	Proposed CMP shall support different roles for Users and Tenant access management. Every tenant shall be able to create their own set of users.		
59.	The offered cloud management platform shall have internal user management engine integration with external directory-based providers – Active directory and LDAP, SAML based providers – Okta, OneLogin, Azure AD SAML etc.		
60.	It shall be possible for mapping of External integration provider users with offered cloud management platform roles.		
61.	Proposed CMP must ensure isolated identity domains and identity provider for each tenant, such that users and their resources are securely segregated.		
62.	Proposed CMP shall offer governance policies which can be scoped to specific entities of user, roles, groups, Cloud, tenant, network along with global policies. At least following policies shall be available:		
	a) Define access to resources based upon project/application.		
	b) Define Quota for user in terms of CPU, Memory, and number of VMs.		
	c) Define approval policy for creation and deletion of VM resources.		
	d) Define number of snapshots can be taken.		
	e) Define the number of VM that can be created across network segments.		
	f) Define expiry date for deletion of resources.		
	g) Define policy to power off/on VM at schedule time.		
	h) Restrict or provide access to VM console.		
63.	Proposed CMP shall allow admin users in the Master Tenant to		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	impersonate any user in the Subtenants to see the application and console.		
64.	The offered solution CMP shall allow users to configure their photo, username, password, email, theme, 2FA, Linux and Windows VM login credentials from the console.		
65.	Proposed CMP shall allow resources to be configured with private or public visibility.		
	Cloud Operations		
66.	Proposed CMP shall be truly-cloud agnostic so that all supported clouds can be provisioned from CMP console in a common repeatable and unified fashion.		
67.	Proposed CMP shall provide one common interface and method for all supported clouds as asked in the integration clause.		
68.	Proposed CMP shall support at least 20+ cloud integration from both public and private clouds from the common interface without any additional coding.		
69.	Proposed CMP shall support Bare metal environment as Private cloud to deploy KVM, Docker, Kubernetes and other virtualization technologies and shall also support major platform like HPE OneView and CISCO UCS.		
70.	Proposed CMP shall support following key features across Cloud vendors from the CMP platform:		
	a) Security Group and rule Creation and synchronization		
	b) Kubernetes cluster creation and synchronization		
	c) Network and load balancer creation and synchronization		
	d) Virtual machine provisioning, Management, and synchronization		
	e) Cloud formation like provisioning and resource synchronization		
	f) Terraform like provisioning and resource synchronization		
	g) RDS / MSSQL support for appropriate cloud		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	h) Network pools / Elastic IP / Availability set / Guidance recommendation etc.		
	i) Backup / Snapshots management		
	j) ARM blueprint, Spec, template, Git / GitHub integration.		
71.	Proposed CMP shall support both internal and external Credential store for securely pulling in the username and password, access, and secret key along with key pair and SSH certificates.		
72.	Proposed CMP shall have a concept of Instance provisioning or equivalent that can contain a set of Containers or Virtual machines or bare metal server that can correlate to a single application or a service suite like group of Web server, App server etc.		
73.	Proposed CMP shall have pre-configured and in-built configuration template or instance types for provisioning Virtual machines, containers & Bare-Metal environments.		
74.	Proposed CMP shall have at least 50+ in-built templates or instance types across technology Platform from different cloud providers of public cloud, private cloud, containerized and bare-metal environments.		
75.	Proposed CMP shall also provide the flexibility for creating the customized templates or instance types across technology platforms from different cloud providers of public cloud, private cloud, containerized and bare-metal environments.		
76.	Proposed CMP software shall have flexibility to bind the multiple versions of technology types, e.g. Application versions to a given instance type instead of creating multiple instance types so that user or administrator can choose the appropriate version while deploying the instance.		
77.	Proposed CMP software shall also support a vast array of providers and configurations with programmatic markup or Infrastructure as Code capabilities i.e.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Terraform, ARM (Azure), Kubernetes, CloudFormation (AWS) and Helm.		
78.	Proposed CMP shall have ability to deploy complete on private cloud application via template across VM, BM or K8S via UI or by IaaC scripts: Should support terraform provider to enable IaaC. Should support ARM and AWS cloud formation template for provisioning.		
79.	Proposed CMP software shall have in-built virtual images for well-known operating systems and hypervisors and shall also provide the flexibility to bring / download own images as well.		
80.	While deploying the instance – User or administrator shall be able to choose appropriate version of the given application as well as appropriate image as per organization requirement.		
81.	Proposed CMP shall also allow create vmdk, qcow2, vhd and raw Images from scratch.		
82.	Proposed CMP shall provide common multi-cloud blueprints for programmatic configuration through Infrastructure-as-code for deploying across on-premises and public cloud.		
83.	Blueprints shall allow to deploy the multi-tier App Architecture for one click provisioning and it shall be possible to define the booting sequence of tier while creating the tier.		
84.	It shall be able to build the blueprint either using the GUI based builder section or using the code and it shall be possible to export the blueprint as YAML or JSON.		
85.	Proposed CMP Shall have included data backup solution which shall be able to protect VM, Containers, Hosts, File, directory, Volume to Target Storage provider including backup of the management plane of CMP software.		
86.	Proposed CMP shall be able to use at least CIFS, NFS, S3 from Storage providers as a backup target.		
87.	Proposed CMP shall also have functionality to integrate with third party backup software like Veeam,		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Commvault, Rubrik, Zerto etc. Vendor shall provide either the GUI screenshot or supporting document in the technical bid.		
88.	The offered integrated backup software shall be deeply integrated into the instance provisioning window so that all newly created instances are protected and backed up automatically.		
89.	The offered backup engine shall support critical features like Scheduling of backup, backup retention counts, on-demand backup etc.		
90.	Proposed CMP shall support and integrate with storage - Object Buckets which can be used for Backup, Archives, Deployment and Virtual Images storage targets.		
91.	It shall be possible to browse, upload, download, or delete files from Bucket and shall support all well-known object storage from AWS, Azure, Google, Dell-EMC ECS, OpenStack Swifts buckets etc.		
92.	Proposed CMP shall also allow creation of file share based NFS and CIFS protocols which can be used for Backup, Archives, Deployment and Virtual Images storage targets.		
93.	It shall be possible to browse, upload, download, or delete files from File share and shall support all various file share protocols like CIFS, NFS, Local Storage used by CMP software as well as well-known industry leading file storage arrays.		
94.	Proposed CMP shall allow administrator to create service plan or t-shirt size based on CPU, Memory and Storage and shall be available to users while creating / provisioning the instances.		
95.	Services plan shall also have the option to provide custom ranges and flexibility to provisioning users for providing predefined limit for number of additional volumes, customization of Volumes, number of sockets and cores per socket. It shall be possible to create plans for a specific technology or cloud like AWS – Cloud		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	formation, VMware, Nutanix, KVM, OneView, Cisco UCS, Docker etc. It shall also be able to create service plans with or without pricing.		
96.	Service plans shall also allow attaching of Price sets and price unit where price set shall define the overall price bundling and price unit shall provide the actual price for a given bundle or a specific component.		
97.	Price unit granularity level shall be minimum configurable at 1 minute and shall have even have the option of 3 and 5 years for effective measurement of resource consumption. It shall be possible to create the price unit for a specific tenant.		
98.	Public cloud plans, when required cloud is being managed by CMP, shall be automatically synced in the CMP platform and it shall be possible to adjust prices either at fixed markup, at percentage markup or custom markup, if required by the organization / department.		
99.	Service plan shall also be available for Load Balancer (Both Synced in from public cloud and Physical / Virtual LB), Virtual image (Storage space being used for Virtual images) and Snapshots.		
100.	Proposed CMP shall allow provisioning of Instances, Apps, Catalog, execution of Jobs which consists of tasks and workflows and building of service integrations.		
101.	Proposed CMP shall support capabilities to integrating machine provisioning /management with configuration management databases (CMDBs), Ticketing systems, IP address management systems, or Domain Name System (DNS) servers.		
102.	Instance provisioning of Proposed CMP shall provide following functionalities from the Instance dashboard:		
	a) List of Instances which are already provisioned.		
	b) Status of provisioned instances along with overall CPU, Memory, and Storage utilization.		
	c) Number of Virtual Machines or containers within a given instance.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	d) Cumulative status of all instances along with overall CPU, Memory, and Storage utilization.		
	e) It shall be possible to Start or stop the container servers of the instances from the instance dashboard.		
	f) It shall be possible to start, stop or suspend the instance from the instance dashboard.		
	g) It shall be able to run a workflow against the given instance by selecting the appropriate phase like Provision phase, deploy phase, pre-provision phase, Teardown the instance etc.		
	h) Instance dashboard shall also display provisioning clouds under which instance is being consumed.		
103.	Instance provisioning of the Proposed CMP shall provide the following functionalities from the VM or Container dashboard of the given instance:		
	a) Shall display the overall health of given VM or container, CPU, Memory and Storage utilization, Availability level and response time along with protection level.		
	b) Shall display the resources associated with the VM or containers, Environment variables, Storage information, Networking information, Access to console etc.		
	c) Shall also display the data protection information of the given VM or container along with backup size and shall also allow to restore or delete the data protection, if required.		
	Shall also display the overall monitoring statistics for CPU, memory, and Storage utilization at the granularity level of as low as 15 minutes.		
	e) Shall also display the overall audit trail messages for carried out operations.		
104.	Instance provisioning of the Proposed CMP shall allow following functionality during the provisioning process:		
	a) Provisioning instance shall guide the provisioning user to the right selection of provisioning Instance type / template.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	b) Instance type / template selection shall provide both user created and CMP software in-built selection of Instance types.		
	c) The provisioning process shall allow you to choose the appropriate Cloud, as per assigned permissions. It shall also allow us to assign the appropriate labels, if required.		
	d) The provisioning process shall allow you to choose the appropriate version of technology type / version / layout, along the service plan, size of the volume, datastore (if applicable), appropriate network etc.		
	e) The provisioning process shall provide the options to use about creation of user within a given group, defining the environment variables and scaling factor so that multiple Containers or VMs can be created automatically.		
	f) The provisioning process shall allow you to select the appropriate workflow, Data protection, thresholds, power schedules etc.		
	g) Shall have the ability to allocate the storage to the VM from various storage containers or datastores as per user's requirement as and when required.		
105.	Proposed CMP shall extend Day 2 operations capabilities to the requestor of the service and shall provide the following functionalities:		
	a) Start/stop/suspend virtual machines.		
	b) Request additional resources like change of plan, additional resources like modifying the size of storage volumes, adding additional network etc.		
	c) Access the VM using RDP/SSH protocols through the self-service portal based on entitlement.		
	d) Clone, Snapshot, import as image, Clone to image, running task, workflow, backup, apply template, adding additional nodes etc. shall be supported.		
	e) Basic day-2 operations should be natively deployed in entire solution from day-1.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
106.	Proposed CMP shall support bulk Import of hypervisor virtual machines and multi-cloud VMs from existing infrastructure to CMP platform for management perspective.		
107.	Proposed CMP shall allow to create and manage lifecycle of K8s cluster and offered solution should allow integration with all major K8s distribution including public like EKS, AKS & GKE and private external k8s clusters.		
108.	Proposed CMP shall allow configuration of networks across all clouds and existing networks from Clouds added in the solution shall auto-populate in the Networks section.		
109.	Proposed CMP shall allow creation of IP Pools, which is an IP address range CMP can use to assign available static IP addresses to Instances.		
110.	Proposed CMP shall support floating IP addresses.		
111.	Proposed CMP shall allow setting FQDNs, joining Domains, and creating DNS records.		
112.	Proposed CMP shall provide out of the box support for proxy connectivity. Proxy authentication support should also be provided with both Basic Authentication capabilities as well as NTLM for Windows Proxy environments.		
113.	Proposed CMP shall support Security Group which acts as a virtual firewall that controls the traffic for one or more Instances.		
114.	Proposed CMP shall allow integration with various SDN solutions, IPAM tools, and DNS tools.		
115.	Proposed CMP shall support integration with various LB like Ha Proxy, AWS, & Azure as well as integrates with several external hardware Load Balancers.		
116.	Application and catalog provisioning of the Proposed CMP shall allow the following functionality:		
	Application dashboards display the running instance of the application along with CPU, Memory, and disk utilization.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	b) Application dashboard shall provide the option to export the application blueprint configuration as JSON.		
	c) Application provisioning shall allow to deploy the application either from the existing instance type / template or directly from the created blueprint.		
	d) In case, application is being deployed using the instance type then an application deployment wizard shall automatically ask the user to create an application blueprint.		
	e) Catalog dashboard shall present a simplified self-service view where users can select and deploy Instances, Blueprints or Workflows with pre-defined configuration in just a few clicks and without presenting an overwhelming list of options		
117.	Proposed CMP shall allow scheduled execution of tasks and workflows through Jobs.		
118.	Proposed CMP shall contain the execution status and history from Task and Operational Workflow Executions run based on time and day.		
119.	Proposed CMP shall allow users to create and schedule SCAP program scans for group of managed systems through security scan jobs.		
120.	Security Scan job shall call in existing SCAP packages and checklists, which shall be used to scan the targeted systems on-demand or on a scheduled basis.		
121.	Proposed CMP Provisioning engine shall allow Git and Github Repository Integrations, and Jenkins Build Service Integrations, which can be created and managed.		
122.	It shall be possible to onboard the GIT repository as import and export target for the CMP constructs like tasks, workflow etc. so that these can be backed up to repository as a code.		
123.	Proposed CMP shall have support to automate infra, app & service deployments with a release pipeline as a capability within the platform i.e. CI/CD pipelines.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
124.	It shall be possible to import the backed-up construct into a new CMP environment instead of creating the entire construct from scratch.		
125.	Repositories integrated with the Proposed CMP shall be allowing users to browse repository folders and files, view file contents from any branch, trigger a refresh, and create tasks, scripts, and templates directly from the repos.		
126.	Proposed CMP shall provide PaaS like capabilities when it comes to deploying applications into the newly provisioned environment, directly from the above repositories and via the APIs.		
127.	Proposed CMP shall provide global search to facilitate search of Instances, Users, cloud, group, hosts, Network, load balancers.		
	Automation & Orchestration		
128.	Proposed CMP should be able to provide automation capability to schedule tasks, workflow for provisioning or Operational workflow along with option to define retry upon failures.		
	a) Schedule Task based upon Shell script, power-cli, java scripts, ansible script, ansible tower, python, groovy script etc.		
	b) Integration with external automation and provisioning tools of Ansible, Chef, StaltStack and Puppet.		
	c) Support custom scripts.		
	d) Scheduled tasks like power up / power down at specific times.		
	e) Operational workflow based upon platform i.e. Linux, windows.		
	f) Operational Workflow to start/stop services.		
	g) Operational Workflow Start/stop/tear Instance.		
	h) Workflow to change configuration as per schedule.		
	i) Run pre/post schedule tasks inside guest machine.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	j) Support both operational and provisioning workflow.		
129.	Proposed CMP shall allow scheduled execution of Automation Tasks and Workflows. It shall be possible to create an independent single task, or multiple tasks shall be combined as a workflow where output of task can be treated as input to another task.		
130.	It shall be possible to assign the task to the complete lifecycle of an instance and automation through workflow. For example, workflow shall assign tasks during configure, pre-provision, provision, post-provision, pre-deploy of an app, shutdown, and startup schedule etc.		
131.	It shall be possible to attach the provisioning workflow to the instance type template or shall be able to select the required provisioning workflow while doing the instance provisioning.		
132.	It shall be possible to run the operational workflow on-demand on “Existing instance” or can be scheduled to run as a job.		
133.	Proposed CMP shall have user-defined custom inputs that are used throughout tasks, workflows, and service catalogues e.g. the user shall be able to provide the inputs like username, password, selection from a dropdown menu etc.		
134.	Proposed CMP shall support elasticity for scaling out additional virtual instances automatically based upon CPU, memory, and disks thresholds.		
135.	The Proposed CMP shall also be able to define the maximum number of elastic virtual instances to be scaled.		
136.	The Proposed CMP shall have Scale Thresholds as pre-configured settings for auto-scaling Instances.		
137.	The Proposed CMP shall be able to set weekly schedules for shutdown and startup times for Instances and VM’s.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
138.	It shall also be possible to apply power schedules to Instances pre- or post- provisioning and power schedule policies on Group or Clouds.		
139.	Proposed CMP shall also provide guidance to recommend and optimize power schedules.		
140.	Proposed CMP shall permit to create time schedules for Jobs, including Task, Workflow and Backup Jobs.		
141.	Proposed CMP shall present a simplified self-service view where users can select and deploy Instances, Blueprints or Workflows with pre-defined configuration in just a few clicks and without presenting an overwhelming list of options.		
142.	Proposed CMP shall 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.		
143.	Proposed CMP shall allow administrators to create easily deployable items like instances, blue-prints or workflows with predefined configuration for consumption by users operating under the “Service Catalog” Persona.		
144.	Proposed CMP shall support creation of services such as 'Single VM' and a 'multi-tier application infrastructure’ like service map across private and public cloud as catalogue within a group or project/applications.		
145.	Proposed CMP shall have a unified GUI for designing catalogues, software components and application stacks with the ability to extend or define external integrations as well as provide features such as Infrastructure as a code (IaaC), using required templates.		
146.	Proposed CMP shall also allow Templates for generating config files, such as my.cnf, elasticsearch.yml or any text file.		
147.	Proposed CMP shall have the capability to publish and share Catalogue (VM Types, Tasks, Workflows) across Projects / applications.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
148.	Proposed CMP shall be able to provide the audit trail or logs for all the catalogues to know which user has requested and shall also display all recent activities.		
149.	Proposed CMP should provide resources consumption as well as quota management for both users, business groups and projects across all the offered services.		
150.	Proposed CMP shall allow creation of Wiki, which is a tenant-wide, RBAC-controlled, auditable Wiki that allows easy UI, API and CLI access to information, notes, configurations, or any other data needed to be referenced or shared with others.		
	Visualization & Optimization		
151.	Proposed CMP shall be able to give complete cost governance across the private, as well as public clouds.		
152.	Proposed CMP shall allow customers to create budgets across Private and public clouds to provide insights into spending.		
153.	It shall be possible to assign the budget to account, tenant, user, groups and at tenant level.		
154.	It shall be possible to assign the budget to every quarter and each month of the year along with the option of customizing it as per organization need.		
155.	Vendor shall provide the live costing API to pull down the overall costing details from the public cloud provider like AWS, Azure, google etc. and shall also have in-built cost metering for private cloud like VMware.		
156.	It shall be possible to review the existing budget against the budgeted like cost to budget breakdown.		
157.	It shall be possible to generate highly granular costing data through invoices for both public and private clouds.		
158.	The invoice engine of the Proposed CMP shall allow customers to see detailed line item-wise breakup, if required and shall show the history of the given resource for both cost and pricing.		
159.	Proposed CMP shall have in-built analytics engine to provide administrators the tools to break down costs and usage across group, cloud and at tenant level.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
160.	Proposed CMP shall show recommendations or guidance for resource and cost optimization by analysing the CPU, RAM, and Storage activity.		
161.	Proposed CMP shall provide the recommendation or Guidance, if any, at a frequency of 30 minutes after establishing the baseline for at least 7 days.		
162.	Proposed CMP shall provide to setup at-least following threshold for the baseline of Guidance / recommendations:		
	a) Recommendation of power shutdown after defining the exceeding of defined threshold at Average CPU percentage, Max CPU percentage and Network bandwidth threshold.		
	b) Recommendation of CPU-Up size when exceeding the Average CPU percentage and Peak CPU percentage utilization.		
	c) Recommendation of Memory-Up size when minimum free memory percentage is going down below threshold.		
	d) Recommendation of Memory-down size when average free memory percentage and maximum free memory percentage is exceeding the threshold.		
163.	Proposed CMP shall ensure that any Guideline or recommendation shall not be executed automatically, and a decision shall be taken only after due diligence.		
	Dashboarding, Monitoring, & Reporting		
164.	Consolidated dashboard for the Proposed CMP shall highlight the overall environment status, System Status, Alarms, log history, Instance status, Instance status by configured clouds, Job executions, Task executions, Backup status, cluster workloads, Activity logs etc.		
165.	Proposed CMP shall offer different report types which are designed to slice up costing and usage across Clouds, Tenants etc.		
166.	It shall be possible to run reports on-demand as needed or can be scheduled to run at certain intervals.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
167.	Proposed CMP shall have at least 25+ in-built reports, and it shall be possible to develop the custom reports as well.		
168.	Proposed CMP shall support following common in-built reports:		
	a) Tenant Inventory summary		
	b) Cloud usage, Cloud usage Application summary, Cloud usage instance summary		
	c) Application, Cloud, Group, instance, tenant cost etc.		
	d) Cloud Inventory, Container Host inventory, Hypervisor inventory etc.		
	e) Tag Compliance, Workload Summary, Virtual machine inventory etc.		
169.	Proposed CMP shall facilitate the servicing of a large amount of Log data along with viewing and shall have in-built log engine like Elasticsearch.		
170.	It shall be able to define the retention period for logs data from few days to years for PCI Compliance along with defining the syslog forwarding rules for exporting purpose.		
171.	Proposed CMP shall also provide the activity logs to track system changes made by the users, e.g. creation and deletion of instances by respective set of users.		
172.	Proposed CMP shall also provide the creation of Application monitor checks to measure the high availability of application provisioned either through blueprint or manually added.		
173.	It shall be possible to define the number of days to calculate the availability level of application along with check interval which shall be possible to define as low as 1 minute.		
174.	Proposed CMP shall also be able to generate an incident based on Application monitor checks and shall be able to integrate the same with well-known support ticketing platform.		
	Licensing & Deployment Footprint		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
175.	Bidder shall provide the licenses on physical / virtual - CPU-core(s) across all servers. Offered licensing shall be scalable.		
176.	Offered licensing subscription shall be offered for at-least 5years from the date of customer-acceptance date. Bidders shall provide and supply all required software for CMP management platform.		

11.2.12. Tape Library

Sl.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1.	Tape Library shall be offered with Minimum of 12 x LTO-9 FC tape drives. Tape Drive shall support encryption. Tape Library shall be offered with 160 Cartridge slots.		
2.	Proposed LTO-9 drive in the library shall conform to the Data rate matching technique for higher reliability. Tape Drive Architecture in the Library shall conform to the INCITS T10 standard ADI Protocols or newer standards.		
3.	Proposed LTO-9 drive shall support 300MB/sec in Native mode.		
4.	Tape Library shall be scalable to more than 500 slots and 40 LTO-9 Drives within the same Library.		
5.	Tape Library shall provide 8Gbps native FC connectivity to SAN switches.		
6.	Tape Library shall have partitioning support so that each drive can be configured in a separate partition. Offered Tape Library shall have support for at-least 20 partitions.		
7.	Tape Library shall provide web based remote management.		
8.	Proposed Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the encrypted keys in a redundant fashion.		
9.	Out of 160 slots, Tape library shall support Barcode reader and at-least 10 mail slots and shall be scalable to 30 mail slots when fully populated.		
10.	a) Tape Library shall have GUI Panel		

	b) Shall be rack mountable.		
	c) Shall have option for redundant power supply		
	d) Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.		
	e) Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved		
11.	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for storage.		
12.	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		

11.2.13. DR Automation

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
1	Key capabilities	Proposed software shall be based upon the foundation of Continuous Data Protection while supporting both local and remote data Protection.		
		Proposed software shall support both Backup and disaster recovery capabilities at on premise, at on premise DR location and public cloud like Azure and AWS.		
		Proposed software shall be an IT Resilience Orchestration and Automation software and shall be able to provide SLA reports and RPO monitoring at all the times.		
		Proposed software shall provide automated failover and failback		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		after initiating the DR execution as per defined policies.		
		Proposed software shall be able to generate automated alert if RPO level increases beyond the prescribed limit.		
		Proposed software shall be able to protect the even large critical VMs which are using more than 120+ vCPUs.		
		Proposed software shall be able to support more than 60TB RDM disks in both physical as well as Virtual mode.		
		Proposed software shall support vSphere API for IO filtering (VAIO).		
2	Ransomware Detection	Proposed software shall provide a native critical capability for ransomware resilience with real-time encryption anomaly detection, without bringing any additional add-on tools.		
3	Licensing	Proposed software licensing shall be based upon the number of protected VM instances. A bundled licensing for minimum 30 Protected VM instances shall be provided, and additional orders shall be placed in future during the contract duration based on this bundle commercials.		
		License shall be agnostic to Virtualization/cloud platform and same offered license shall be able to protect VMs at on premise		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		using VMware Virtualization, HVM, AWS and Azure VMs.		
		License must be able to cater for all asked/ mentioned functionalities across DC & DR.		
4	Always-On Replication	Proposed software shall have in-built native capability of always-on replication instead of using snapshot/clone technology for both local as well as DR data protection.		
		Proposed software shall not be dependent on any software agent within the given production virtual machines.		
		Proposed software shall have flexibility for delivering less than 10-second RPO for both local-data Protection as well as remote-data protection after excluding the link latency.		
		Proposed software shall be able to create thousands of checkpoints, separated out by less than 10 seconds, for minimal RPO and RTO using journal-based or equivalent technologies.		
5	Platform Independence	Proposed software shall be virtualization-platform agnostic so that protected -VM can be VMware vSphere-based and recover-VM can be either AWS or Azure VM or vis-à-vis or any cross-combination of listed platforms.		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
6	Application Consistency	Proposed software shall have capability for creating application-consistent group for multi-VM application for data consistency during backup and recovery.		
		Proposed software shall have capability for defining the boot order of the VMs within the application consistent group during the failover operation for reducing the overall RTO.		
		Proposed software shall not put any limitation on the number of application-consistent groups or vendor shall support at-least 256 number of application-consistent groups for data consistency.		
		Proposed software shall not put any limitation on the number of VMs within the application-consistent groups or vendor shall support at-least 2048 VMs within application-consistent groups for data consistency.		
		Proposed software must be able to replicate the VMs within the application-consistent group to multiple Application consistency groups for better data protection. It shall be possible for both Local data Protection as well as remote data protection.		
		Proposed software shall be able to prioritize the replication of VMs traffic within the application consistency group as per end-user needs at low, medium, and		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		high level and shall do automatic bandwidth usage.		
		Application-consistency group shall allow ad hoc-backup support (one time backup) either for entire consistency group or selected Virtual machines within the group.		
7	WAN Optimization	Proposed software shall also support WAN optimization technologies like compression when protecting the information at DR location.		
		Proposed software shall also have capability to switch ON / OFF the WAN optimization technology depending upon the type of VMs or application-consistent group.		
8	Extended copy	Proposed software shall support creation of extended copies, as per customer data retention and backup policies to various media.		
		It shall support High speed SSD / NVMe drives enabled datastore for short-term backups (Daily and weekly).		
		It shall support various retention repositories (Daily, weekly, and Monthly backups) based upon S3 interface, NFS, SMB, AWS Storage gateway, Amazon S3, Microsoft Azure storage and purpose-built backup appliance from heterogeneous storage vendors.		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		Proposed software shall provide the scheduling engine for Daily, weekly, and monthly backups.		
		Proposed software shall also be able to keep the retention copy at-least for a year on defined media in the policy.		
9	Immutability	Proposed software shall support immutability for retention when using S3 Compatible storage on-prem, Amazon S3 or Azure.		
		Proposed software shall support both S3 Bucket versioning and S3 Object lock for delivering write once read many functionalities in compliance retention mode.		
		Proposed software shall be able to define immutability for complete retention copies and shall also have flexibility to define for a given application-consistency group in the software.		
10	DR failover	Proposed software shall have capability for doing failover from primary location to DR location in automated mode so that there shall no need to create the VM manually at DR location.		
		Proposed software shall have capability for selecting the restore point or checkpoint, as per end-user requirement, while doing the failover from primary location to DR location.		
		Proposed software shall have capability for selecting the boot		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		order of VM at DR location during failover process for minimizing the overall RTO.		
		Proposed software shall have capability for configuring the reverse protection (DR to Primary location) after successful failover from Primary location to DR location.		
		Proposed software shall have flexible commit policy so that environment can be rolled back to Primary location if planned DR failover is not successful due to unforeseen event or any unknown reason.		
		Proposed software shall also have flexible commit policy in minutes to hours so that after failover operations can be thoroughly checked before announcing the successful failover.		
		For planned failover, failover policy shall provide the flexibility to end-user for shutting down the primary site virtualized environment for minimal RPO.		
11	DR drill	Proposed software shall have capability for doing DR Drill (Test Failover) from Primary location to DR location in automated mode so that there shall no need to create the VM manually at DR location.		
		Proposed software shall have capability for selecting the restore		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		point or checkpoint, as per end-user requirement, while doing the test failover from Primary location to DR location.		
		Proposed software shall have capability for selecting the boot order of VM at DR location during test failover process for minimizing the overall RTO		
		Proposed software shall have capability for selecting and configuring the separate test network at DR location for DR Drill operations.		
		Proposed software shall have capability for cleaning up the DR location after successful completing the DR Drill operations. There shall be no manual task at DR location for cleaning operations.		
		Proposed software shall provide the drop down to end-user for acknowledging the successful completion of DR drill.		
		End-user shall have flexibility for doing the DR Drill operations for an individual VM inside the application-consistency group instead of doing it for all VMs within the consistency group.		
12	Bandwidth management	Proposed software shall automatically adjust the bandwidth usage across sites for given application-consistency groups depending upon the defined prioritization level.		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		Proposed software shall be able to throttle the bandwidth between Primary and DR location from the overall available bandwidth.		
		Proposed software shall also be able to throttle the bandwidth for a specific period of time.		
		Proposed software shall also have bandwidth regulation mechanism for troubleshooting.		
13	Ransomware Protection	Proposed software shall have strong mechanism for ransomware protection and shall be achieved with minimum RPO.		
		Proposed software shall have capability for creating the checkpoint at every 5 second of data protection so that customer can select the required checkpoint while restoring the files during the ransomware attack and can achieve lowest RPO.		
		Proposed software shall have capability for storing the latest data information, at-least for a month, on the faster storage devices of NVMe or SSD and remaining day information on slowest media automatically. This is to ensure that recovery from ransomware attack is really quick.		
14	Cyber Vault	For a last line of defence against ransomware, proposed software shall have capability to support a cyber-resilient vault for providing		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		isolation, air-gapping, immutability in a zero-trust architecture.		
		Cyber-resilient vault shall be supported on enterprise-production grade hardware like using at least 99.9999% data-availability storage and silicon-root-of-trust enabled compute.		
		Cyber-resilient vault shall be completely isolated from the production network and data from the source storage shall be copied on periodic bases to the vault. Network ports shall be immediately closed after replication.		
		Data Replication to cyber-resilient vault shall be completely encrypted.		
		In an unforeseen event of ransomware attack, end-user shall be able to bring-up the production running from cyber-resilient vault, if needed and instead of copying back the data immediately to source Compute and Storage.		
15	Restoration management	Proposed software shall allow the restoration of selected files from the good known backups / checkpoints without restoring the full virtual machine.		
		Proposed software shall provide the flexibility to restore the files at original location and shall provide the flexibility to administrator for		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		downloading the selected files so that it can be restored at required location / system.		
		Proposed software shall provide the flexibility for restoring the selected VM and Deleted VMs.		
		While restoring the VMs / Deleted VMs, restore engine shall provide the flexibility for changing the IP address either using Static IP or DHCP IP scheme.		
		VM restoration engine shall provide the flexibility for changing the network setting during the restoration process.		
		Proposed software shall also provide the flexibility for restoring the complete application consistency group.		
		Proposed software shall have in-built search and index engine for restoration version control.		
		Search and index engine shall allow restoration of VM or application consistency group.		
		Search and index engine shall provide the flexibility to customer for complete version control so that customer can restore the appropriate version as per organization need.		
		Search and index engine shall also provide the flexibility for searching within a given data range for granular control.		
16	Reporting	Proposed software shall have in-built reporting engine and shall		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		provide at-least following reports. In case vendor doesn't support the below minimum report functionalities, then vendor shall ensure that appropriate commercialized IT Resilience Orchestration and Automation software is factored in their submission.		
		Application consistency group performance reports: It shall clearly show the over data protection SLA (RPO) being achieved by the Application throughout the day along with IOPS, Throughput and wan bandwidth consumption.		
		Recovery reports: It shall allow administrator to have recovery reports for Failover, failback, DR-drill, Successful backup and recovery, failed backups, and recovery.		
		Resources report: It shall provide the resource reports consumed by VMs within the application consistency group.		
		Data Protection Report: It shall provide the complete data protection report over a period of time.		
17	Management	Proposed software shall have GUI based management which shall shows critical parameters of Average RPO for the complete site, Number of VMs being protected, Number of Application		

Sl. No	Minimum Requirement Specification		Compliance (Yes/No)	Compliance Cross reference Page No.
		consistency groups along with their status and health, Site topology, IOPS, WAN traffic, Compression, events and running tasks etc.		
18	OEM Ranking	OEM must be rated as Leader's in the latest magic quadrants for Primary Storage / ITRO/DRA by Gartner OR OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for storage/DRA.		
19	Support	Five years OEM support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.		

11.2.14. NGFW Internal

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	Proposed Internal Firewall cannot be from same OEM of External Firewall. NGFW should have min 10 GBPS enterprise mix traffic throughput with IPS.		
2	Proposed OEM must be in Gartner Leader's magic quadrant for NGFW as per last five report before release of this RFP.		
3	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology.		
4	Firewall appliance must have 12 x 1GE RJ45 interface, 6 x 1GE SFP, 4 x 10GE SFP+ slots and 4 x 25G		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	SFP28 slots Populated with 04 Numbers of 1G Base SX Multimode, 04 Numbers of 10G Base SR Multimode, 04 nos. of 25G base SR Multimode transceiver from day one, all these interfaces should be available simultaneously. NGFW should have minimum 2 x 480 GB SSD local storage for Logging.		
5	Threat Prevention (including FW, IPS, Application Control, Sandbox & Antivirus with logging enable) throughput must be at least 20 Gbps with real- world / enterprise / app mix traffic.		
6	NGFW (including FW, IPS, Application Control) throughput must be at least 22 Gbps with real-world / enterprise MIX traffic		
7	NGFW should support 700 site-to-site VPN Tunnels.		
8	NGFW should support more than 600,000 new sessions per second on tcp or 250,000 new sessions per second on layer http		
9	NGFW should support at least 12 million concurrent sessions on tcp or 3 million concurrent sessions on http		
10	The NGFW solution should support NAT64 / NAT46 and DHCPv6.		
11	The proposed system should be able to operate in Transparent (Access) mode and NAT/ Route mode simultaneously		
12	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.		
13	The NGFW should support WAN links load balancing and fail- over for at least 4 links		
14	The proposed system should have integrated Traffic Shaping functionality for both inbound and outbound traffic.		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
15	The proposed firewall must support at least 10 Gbps of SSL Inspection throughput.		
16	Proposed NGFW must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.		
17	The NGFW shall be able to support various form of user Authentication methods simultaneously, including Local Database, LDAP, RADIUS/TACACS+, Windows AD.		
18	The NGFW should readily be available integration with SDN platforms - VMware ESXi / NSX / OpenStack, Cisco ACI / Nuage Networks / Nutanix.		
19	The IPS should be able to inspect SSL sessions by decrypting the traffic		
20	Should have more than 17,000+ pre-defined intrusion prevention signature (excluding custom signatures) to optimize security effectiveness.		
21	Should support Behavioural DoS (Behavioural Denial of Service) Protection to defend against zero-day network flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.		
	Network-flood protection should include:		
	• TCP floods—which include SYN Flood		
	• UDP flood		
	• ICMP flood		
	• IGMP flood		
22	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level:		
	high medium low)		
23	NGFW should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Body parameters in length to block advanced HTTP layer attacks.		
24	The appliance should have at least 3500 + application signatures database readily available and must create custom application signature.		
25	Should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services and their equivalent encrypted versions, wherever applicable: HTTP,		
	SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI		
26	NGFW must include Anti-bot capability using IP reputation DB, terminates botnet communication to C & C servers also. Vendor needs to add additional license if it is required.		
27	The solution must include Anti-Malware for defence against known and unknown file-based threats. Antimalware services should span both antivirus and file sandboxing to provide multi-layered protection in real-time with threat intelligence		
28	The NGFW should have web-based management tool and/or appliance-based management tool and also support SSH, Telnet to manage.		
29	Should have on device and capable of managed by centralized management with complete feature parity on firewall administration.		
30	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
31	Firewall and APT should be manageable from dashboard and/or Centralized Management. In case centralized management in not available/required, administrator should be able to configure firewall directly from Device GUI with complete feature parity.		
32	NGFW should integrate tightly with proposed sandbox to protect organization from Advance Persistence		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Threats to protect against Zero-day threat prevention entails OEM's AI-based inline malware prevention using sandbox. Solution should analyse and block unknown files in real-time, offering sub second protection against zero-day and sophisticated threats.		
33	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
34	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.		
35	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component		
36	The NGFW shall support stateful session maintenance in the event of a fail-over to a standby unit.		
37	High Availability feature must be supported for either NAT/Route, Transparent or Hybrid mode		
38	The NGFW must support both Active-Passive and Active - Active with High Availability options.		
39	The NGFW must provide Load sharing mode along with the redundancy in case multiple virtual firewalls are created on it.		
40	The NGFW shall support interface link monitoring failover		
41	The NGFW shall support external device ping probe failover		
42	The HA solutions should support salient / equivalent features for firmware upgrade process that ensures minimum downtime		
43	The NGFW must have provision of fail-over and generate alert in case of high memory utilization on primary appliance.		
44	The NGFW must have the capability to perform security inspection in networks where forward traffic and return traffic follow different paths.		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
45	The NGFW should have web-based management tool also support SSH, Telnet to manage.		
46	The NGFW should have a mechanism to alert administrator for any critical events if occurs through different channel like email/SMS etc.		
47	Solution should allow administrator to create multiple administrative profile based on the requirement.		
48	The solution should allow administrators to capture the packet using built-in capture tool to select a packet and view its header and payload information in real-time. Once captured it should give option to filter the packets by different fields or through the search bar. The capture can be saved as a PCAP file that you can use with a third-party application, such as Wireshark, for further analysis.		

11.2.15. NGFW External

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	NGFW Throughput (Application Visibility and Control/Application-Identification and Logging enabled considering 100% application/webmix traffic flows) - 18 Gbps or higher		
2	NGTP Throughput (Enabling Firewall, IPS, URL filtering / Web Security Essentials, Application Control, Anti-Virus, Anti-Bot, DNS Security, Basic File Blocking and Logging enabled considering 100% application/webmix flows) - 10 Gbps or higher		
3	Minimum Concurrent TCP Connections or Concurrent http sessions - 20 million tcp or 2 million on http		
4	Minimum New TCP Connection per second or http sessions per second - 600,000 tcp or 200,000 on http		
5	Ports: 10G RJ45 - 12 or higher 10G SFP+ - 10 or higher 25G SFP28 – 4 or higher Deliciated HA ports – 2		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Dual Power Supplies (Hot Swappable) – Must High Availability from day 1 - Active-Active, Active-Passive (All accessories required for deployment of the product in HA should be provided by the bidder.)		
6	NGIPS Signature supported - 18000 or higher		
7	All above asked specifications should be provided on a single appliance only.		
8	NGFW must support: NAT64 & DHCPv6 from day one for seamless transition between IPv4 and IPv6		
9	Individual NGFW appliances and the Centralized Management and Logging solution should have GUI and role-based management solution from the same OEM. The proposed firewall solution must support full-featured local policy creation, modification, and deployment directly from the firewall device without reliance on any external centralized management system.		
10	The solution proposed should support in-built Multiple Security Groups provided by the same OEM		
11	The solution proposed should be latest and should not reach end-of-life for next 7 years from the date of supply. An undertaking from OEM needs to be provided for the same		
12	Operating system of NGFW solution must support: USGv6 / IPv6, FIPS-140-2		
13	NGFW appliance should have at least 480 GB or more integrated SSD Storage and 32 GB RAM minimum		
14	NGFW solution support with 10 or higher Virtual Firewall instances		
15	The bidder will be responsible for installing and configuring the appliances in HA at the respective locations. The bidder should further ensure seamless transition of security and access policies from existing solutions to the new setup, through appropriate technical solution and implementation strategy.		
16	Appliances must be populated with maximum supported hardware configuration from day-one.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
17	The proposed firewall solution must support separation of management plane and data plane on firewall device with capability to allocate dedicated management resources (like CPU cores, interface) on gateway device and configure management domain, so that access to the firewall device management is guaranteed even in scenario of heavy traffic load on firewall device or threats like DoS attacks. Proposed Firewall should use not proprietary CPU & should be open architecture to protect & scale against dynamic latest security threats with minimum 12 cores CPU.		
18	Firewall must comprehensive IPv6 support with following features on Day1 - Management access on IPv6, IPv6 routing protocols like Static, OSPF & BGP IPv4 & IPv6 VPN. There should no degradation in Firewall performance on IPv6 traffic.		
19	Proposed firewall solution must provide Dual stack (IPv4 and IPv6) support for IPsec & SSL VPN.		
20	The proposed NGFW should support both Client and client less (Browser based) VPN on the same platform. The proposed solution must be able enforce policy based on endpoint profile such as Patch updates, AV status, disk encryption status, data loss prevention for compliance verification and should be able to provide access based on the compliance state, this feature should be available from day 1 for type 1 NGFW The proposed solution should be able to share the identity information such as IP address, username, device type, OS and software details with other solutions such as NAC for conditional access from day 1 for type 1 NGFW		
21	The firewall must support Deep SSL Inspection on latest SSL & SSH protocols versions including TLS1.3. It shall support the deep packet inspection of different SSL / TLS based Web /any other applications simultaneously		
22	Inter-cluster communication between Firewalls devices configured in high availability and communication with central management should be secure and encrypted. Firewall must offer a complete management interface		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	(policy management , monitoring etc ..) accessible via modern web browsers (Chrome, Edge, Firefox) with no dependency on proprietary Windows-based clients		
23	The Firewall Solution should support DNS security capabilities within the same appliance with an additional license without any additional Hardware to provide protection against DNS tunnelling-based attacks, Dynamic DNS, DoH, DoT and DGA based attacks		
24	Solution should support database maintenance containing a list of known botnet command and control (C&C) addresses which should be updated dynamically		
25	The proposed solution should support prevention against new malicious domains and enforce consistent protections for millions of emerging domains		
26	Proposed Management solution must have integrated security architecture with multi-tenancy, analytics, Logging, management, and automation capabilities to address and dramatically improve visibility. Bidder must provide all license to achieve the overall requirement of Management solution. Solution must support policy audit trails and change history available locally on each firewall device.		
27	Firewall Management solution must provide administration control by segmenting security management into multiple virtual domains based on geography, business unit, security functions to strengthen security and simplify management. Each admin of different geography, business unit must be able to change policy and configuration related to their tenant simultaneously on Firewall. The proposed Management platform solution must provide a mechanism to identify rules that are not being used or have not been hit by any traffic.		
28	Appliance must be capable of sending logs in syslog format and its raw log format should be supported by all leading SIEM solutions. The said appliances should integrated with CSOC to receive logs over site to site VPN / other form of connectivity.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
29	If an appliance in the appliance cluster malfunctions, hangs, or loses network connectivity due to hardware or software issues, the appliance cluster (either active-active or active-passive) must be able to automatically switch-over to the healthy appliance without any manual intervention.		
30	Firewall must support zero-downtime inline policy changes without re-installation or full policy push.		
31	The propose Firewall should be provided with license like AVC, Threat prevention, URL filtering, Anti-malware, Sandboxing, DNS security (non-proxy) from Day one		
32	The Firewall/Firewall OS of the appliance should be certified under Common Criteria program (gobal or the Indian Common Criteria Certification Scheme(IC3S) has been set up by the Ministry of Electronics and Information Technology (MeitY)) program for NDPP, Protection Profile for Stateful Traffic Firewall, IPS and PP for VPN Gateway		
33	The Firewall OEM should be SOC2 certified. Malware analysis service should be certified with SOC2 for customer data privacy protection. The data uploaded for unknown threat emulation and analysis, along with all associated services like sandboxing, must reside within India's judiciary boundaries.		
34	The firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or : CB IEC 62368-1 or UL62368-1 or equivalent Indian standards like IS-13252 (Part 1): 2010 for Safety requirements of Information Technology Equipment		
35	Proposed NGFW should have following feature from day 1. • Application visibility and control • IPS • Antivirus • Antispyware • Zero-day protection (anti-malware) • File blocking • DNS security		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
36	Proposed model should be certified under "Mandatory Testing & Certification Of Telecommunication Equipment as per Department of Telecommunications, Ministry of Communications - Necessary documents to be provided from day 1		
37	Proposed NGFW supplies must be class II or above MII content		
38	NGFW should be proposed in-line with CERT-IN guidelines and should have mechanism to dynamically import and enforce IP addresses, URLs, domains, and custom indicators of compromise (IoCs) from external sources including CERT-IN from external source without changing firewall rules / configuration.		
39	Solution to support on-prem management & Analysis to be provided to ensure all the data and logs are kept on-prem for proposed NGFW		
40	The proposed OEM must have "Recommended" rating with min 97% Evasion proof capability and min 97.5% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall comparative Test Report.		
41	Must be certified from Common Criteria certified for NDPP, Protection Profile for Stateful Traffic Firewall IPS, SSH and PP for VPN Gateway.		
42	The vendors/bidders are required to quote the cost of the Firewalls solutions along with OEM TAC & RMA Support for 5 years. Necessary policy and rules change should be in scope of the successful bidders throughout the project phase.		
43	The provided NGFW should continue to provide a) Upgrades and latest OS version in market b) Updates c) Patches and Fixes (Scheduled / Emergencies)		
44	Proposed OEM must be in Gartner Leader's magic quadrant for NGFW as per last five years' report before release of this RFP.		
45	The NGFW should support WAN links load balancing and fail-over for at least 4 links		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
46	Solution modules shall support authentication protocols like RADIUS/ TACACS+ etc.		

11.2.16. DDOS

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
Hardware			
1	Proposed DDOS Solution must not be part of any UTM or NGFW or any white-labelled or virtual solution running on third party hardware.		
2	The document/cross reference provided by the OEM for each clause asked in the RFP must be available on a GLOBAL public domain and the proposed solution must support all technical features specified in the RFP from day 1. OEM Simple undertaking without any test results/proofs claiming any performance number will not be accepted.		
3	The proposed appliance must provide: 1. Minimum Appliance Throughput- 50Gbps 2. Minimum SSL TPS of 60K with RSA 2K keys and 30K SSL TPS with ECC		
4	Should have a minimum of 8 x 10G SFP+ ports and 2x40G Fiber ports from day1. The 10G and 40G ports should be able to upgrade to 25G and 100G ports respectively with the change of transceivers in future		
5	Virtualization feature that virtualizes the device resources – including CPU, memory, network, operating system and acceleration resources. Each virtual instance contains a complete and separated environment of the following: i. Resources ii. Configurations iii. Management iv. Operating System		
6	The Appliance must use it's own Hypervisor which should be a specialized purpose build hypervisor and NOT a commercially available hypervisor like XEN, KVM etc. It should NOT use Open Source/3rd party Network		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Functions. The appliance must support at least 8 virtual instances from day 1		
7	Proposed OEM should have been deployed at least 5 State Data Caners/Government customers		
DDOS functionalities			
1	System should be able to support multiple segment protection.		
2	The proposed solution should be an Application Proxy for HTTP/S, DNS, SMTP, FTP & SIP.		
3	The proposed DDOS solution must be able to inspect all the SSL traffic but not just first packet		
4	System should have in In-Line, SPAN Port, Out-of-Path deployment modes.		
5	System Should detect and mitigate IPv6 and IPv4 Attacks.		
6	System should provide protection for volumetric and Protocol level DDoS attacks.		
7	Inspection and prevention are to be done in same hardware.		
8	The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioral DoS attacks without manual intervention and be able to create auto signatures for zero-day DDoS attacks and DNS DDOS attacks.		
9	The DDOS solution must be resilient enough to mitigate following types of attacks: DNS reflection, DNS Amplification, Floods attacks like TCP, UDP, ICMP, IGMP, ARP, Bad header floods, SMURF attack, tear drop attack, DNS caching poisoning, protocol anomalies-based attacks, DNS Tunneling attack, DNS based exploits.		
10	Solution should provide protection from L3-L4 DDOS. DDOS should prevent signature based and TPS based attacks at Network, DNS and SIP level		
11	The proposed solution should have at least 100 DOS Vectors in-built.		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
12	The proposed solution should detect and protect against SMURF attack and Teardrop attack		
13	The proposed solution should have the capability to dynamic connection reaping feature to close idle TCP connections.		
14	The proposed solution should have the capability to define the below TCP parameters at a global level and granularly per application level: a. TCP Close Wait b. TCP FIN Wait c. TCP Idle Timeout d. TCP Keep Alive Interval		
15	The proposed solution should have the capability to define a global DDOS policy for the entire network and a granular DDOS policy for an application.		
16	The proposed solution must support protocol inspection and must support routing protocol		
17	The proposed solution should have the capability to define connections and connections per second for each application.		
18	The proposed solution should have the capability to allow only specific DNS query type and must support rate limiting and DDOS protection on specific DNS record types like A, AAAA, CNAME, axfr, MX, NS, PTR, SOA, SRV, TXT, DNS Malformed etc.		
19	Proposed DDOS solution should provide Geolocation IP address database to identify the source of the attack origin and should support IP Reputation Mechanism to identify the Blacklisted TOR Networks or Proxy IP address to Block the request immediately.		
20	Proposed DDOS solution should detect any DDoS traffic and mitigate any DDoS attack without interrupting any legitimate traffic and customer services.		
High Availability and Redundancy			
1	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active mode		

Sl. No.	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
2	The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support transparent failovers between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check.		
Management & Reporting			
1	Should support SNMP v2 & v3 traps, email alerts and SNTP/ NTP. Device should be able to send SNMP traps to centralized server and should provide login/ logout, configuration changes, dumps information.		
2	Should support authentication, authorization and accounting (AAA) integration with external authentication support providers such as RADIUS and TACACS+ and support RBAC to help ensure security. Should support role-based access.		
3	Should Support integration with SIEM and other Monitoring and Reporting solution		
4	The proposed solution should be from single OEM for SLB+WAF & DDoS.		
5	Proposed DDoS solution must be of same OEM as of hardware vendor and not a 3rd party solution integrated with hardware and supplied.		
6	The proposed DDoS solution should have online diagnostic tool, where administrator can take snapshot of configuration to diagnose the DDoS vulnerability and the OS related issue on the fly and tool should provide the recommended or necessary steps to patch those DDoS vulnerabilities		
Product / OEM Evaluation Criteria			
1	DDOS Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions		

11.2.17. Observability

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	The proposed NMS/EMS solution should be an integrated, modular, and scalable solution to provide comprehensive fault management performance management, Traffic Analysis & SLA monitoring functionality/Observability Platform with Helpdesk (250 Agent, NW – 55, HD - 5)		
2	The system should be accessible via a Web based GUI console/ portal from intranet as well as from internet.		
3	It should have a secure single sign-on and unified console for all functions of components offered for seamless cross-functional navigation & launch for single pane of glass visibility across multiple areas of monitoring & management.		
4	The proposed NMS/EMS solution deployment must support the latest version of Windows and/or Linux Operating Systems and should be a 64-bit application to fully utilize the virtual machine resources on which it is installed.		
5	Any additional components except hardware		
	(software, database, licenses, accessories, etc.) if required for implementation and execution of project, for providing the total solution as mentioned in the RFP document should be provided by the bidder.		
6	The proposed solution should be an integrated, modular, and scalable solution, accessible from a single pane of glass for KPI insights across the entire IT environment. This dashboard will provide service status, performance view, response-time date etc. based on role-based access.		
7	OEM of the solution provider should ISO 27001:2013 / ISO 27034 certified from Global Leading Certified Agencies. Documentary proof must be provided.		
8	The Network Management function must monitor performance across heterogeneous networks.		
9	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; to keep the topology always up to date. This		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	discovery should run at a low overhead, incrementally discovering devices and interfaces.		
10	NMS should provide integrated fault, performance		
	Monitoring, Configuration & Compliance Management.		
11	All possible Switches and other Networking Devices should be SNMP capable and MIB should be available.		
12	The solution should provide network Trap Analytics out of the box.		
13	The solution should be capable to support out of the box monitoring of at least 500+ devices/services		
14	The solution should support Compliance Model Configuration, Software, Running State.		
15	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e., Router, Switches, Servers etc.) and map the connectivity between them with granular visibility up to individual ports level. The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices.		
16	The tool shall be able to discover IPv4 only, IPv6 only as well as devices in dual stack. In case of dual stack devices, the system shall be able to discover and show both IPv4andIPv6IP addresses.		
17	The tool shall be able to work on SNMP V-1, V-2c & V- 3 based on the SNMP version supported by the device. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP.		
18	The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “start-up” configurations and alert the administrators.		
19	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements:		
	a) Capture running configuration.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	b) Capture startup configuration		
	c) Upload configuration;		
	d) Write start-up configuration;		
	e) Upload firmware		
20	Reporting solution should be able to report on Service Level status of configured business service.		
21	Solution should be able to collect Key performance measurements and statistics from all network domains and store it. This data is to be used for evaluation of performance of the end-to-end network infrastructure/ services.		
22	The performance management system shall be able to collect and report data like:		
	a) Packet delay and packet loss		
	b) User bandwidth usage rate		
	c) Network availability rate		
	d) CPU usage rate		
	e) Input/output traffic through physical ports		
	f) Input/output traffic through logical ports		
23	Bidder should calculate license as per proposed Infrastructure required as per the RFP requirement.		
24	5 Years onsite warranty support including all other accessories related to smooth operation of NMS Software from the date of successfully installation, commissioning, integration, and final acceptance		

11.2.18. Server Load Balancer and Web Application Firewall

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
Server Load Balancer			
General			
1	Application Load Balancer and Web Application Firewall (WAF) on same hardware running on same OS version from same OEM		
2	The solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the solution and integration with automation and CI/CD tools including Ansible, Jenkins, and Terraform. The solution shall support overlay network like VxLAN/Geneve for integration with Kubernetes services		
3	The solution shall have integration with Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from same make as WAF. It should not be third party or opensource.		
4	The Controller/Container Plugin shall support orchestration to dynamically create and manage WAF objects and shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis		
5	The document/cross reference provided by the OEM for each clause asked in the RFP must be available on global public domain like product datasheets, product guides etc. and the proposed solution must support all technical features specified in the RFP from the date of issue of this RFP.		
Hardware			
1	The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 2 Million 2) Network interfaces: 8x10G SFP+ and 2x40G QSFP+ from day 1 with 10G and 40G ports to be upgradable to 25G and 100G ports respectively in future with change of transceivers only.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	3) SSL Throughput: 30 Gbps with 60K SSL TPS with RSA and 30K with ECC 4) Storage:1 TB 5) Memory: 128 GB		
2	The appliance must use it's own Hypervisor which should be a specialized purpose build hypervisor and NOT a commercially available hypervisor like VMWare, XEN, KVM etc. The Appliance should not support deployment of any third party software on its hardware. The appliance must support at least 8 virtual instances from day 1 scalable up to 20 instances in future with license upgrade as and when required.		
Load Balancing Features			
1	The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based keys		
2	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed LB should be capable to trigger a script based on an event		
3	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2		
4	The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum RTO, window size, Nagle Algorithm, delay window control, packet loss ignore rate, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
5	The Proposed solution should have application delivery features such as Layer-7 load balancing, Layer-7 content switching, caching & compression, hardware based SSL offload and server side compression.		
6	The Proposed solution should be able to monitor the applications using intelligent application monitors which can be either using system defined executable scripts. It should also provide mechanism to bind multiple health checks, support for application specific VIP health check and next gateway health checks		
7	Following Load Balancing Topologies should be supported: • Client Network Address Translation (Proxy IP) • Mapping Ports • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses		
WAF FEATURES			
1	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the Application Security Top 10 attacks and also provide suggestions/shortcuts to address the compliances and configure policies for it.		
2	The WAF solution must support Security Policy to be applied per application, rather than one single policy for an entire system. 1) Different WAF policy and signature set based on URI 2) Should redirect traffic to different pool members based on URI 3) Should be able to rate limit based on each URI		
3	A given user must be enforced to follow a sequence of pages while accessing without any script and should have provision to apply the restriction to the application or part of the application based on Geo-Location		
4	The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	(Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.		
5	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode. The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.		
6	The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings		
7	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema validation, common attacks mitigation, and XML parser denial-of-service prevention.		
8	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)		
9	System should support inbuilt ability to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.		
10	The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	CAPTCHA challenge to do device fingerprinting. The Solution should have inbuilt ability within the appliance (without accessing the internet/cloud service) to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCIDSS/ HIPAA, ISO 27001, TLS 1.2/1.3 support compliance requirements for web application servers. Necessary logs to be generated for audit and compliance.		
11	Solution should support the following Security Protections: i. BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats ii. POSITIVE and NEGATIVE SECURITY MODEL should have advanced behaviour-analysis technologies to separate malicious threats from legitimate traffic. The administrators should be able to see all the signatures and not just the signature categories. Admins can apply Specific signatures to specific policies iii. ZERO DAY ATTACK PROTECTION should be provided by behaviour-based protection with automatic signature creation against unknown, zero-day DDoS attacks.		
12	The solution must be able to block transactions with content matching known attack signatures while allowing everything else. The solution should also have an option to put a signature in staging mode. Meaning that the system applies the attack signatures to the web application traffic, but does not apply the blocking policy action to requests that trigger those attack signatures.		
13	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a Ability to drop requests and responses, b Block the TCP session, c Block the application user, or IP address d Should be able to generate unique identifier to track attack event		
14	Proposed WAF Solution should have capability to automatic learning should include Directories, URLs, Form Field Values,		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Whether the field values is numeric/alphanumeric/alphabets, length of the field etc. Solution should support different profiling like different values like Directories, URLs, Form Field Values, Metacharacters etc. for different applications.		
15	WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic		
16	The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks.		
17	The WAF must provide BOT mitigation functionality (including CAPTCHA) without having to go on internet for some cloud based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc .		
18	Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript, CAPTCHA Challenge and device fingerprinting.		
19	The solution should be able to perform profiling of JSON with dedicated JSON parser to inspect all JSON messages and apply security policies to embedded object pairs and binary payloads. Solution should enforces JSON security policy parameters, such as restricting URL wildcards and parameters, malformed data, and JSON payloads, methods and objects.		
20	The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation • Backend application parser protection against XML DOS • XML Encryption and XML Signatures • Granular WSDL methods selection		
21	The proposed solution must support SSL VPN and Single Sign On functionality on same hardware solution running on same OS version from same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based application access instead of session-based application access and deny access for non-compliance		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups: • Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. • The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and same should be configurable. • Able to perform Operating System, Windows Registry, File or Process checks. • Able to check if mobile devices have been jailbroken		
22	The Web Application Firewall Solution shall have the Geo-location based IPv4 & IPv6 database. So, Geo-location based traffic filtering shall be done on the Web Application Firewall.		
23	The device should support following health check types: • Link Health Checks • TCP Health Checks • UDP Health Checks • ICMP Health Checks • HTTP/S Health Checks • TCP and UDP-based DNS Health Checks • TFTP Health Check • SNMP Health Check • FTP Server Health Checks • POP3 Server Health Checks • SMTP Server Health Checks • IMAP Server Health Checks • NNTP Server Health Checks • RADIUS Server Health Checks • SSL HELLO Health Checks • WAP Gateway Health Checks • ARP Health Checks • SIP Health Checks • Virtual Wire Health Checks • DSSP Health Checks • Script-Based Health Checks • Cluster-based Health Checks		
24	The proposed appliance should support the below metrics: 1. Hash 2. Persistent Hash 3. Weighted Hash 4. Least Connections 5. Round-Robin 6. Response Time, 7. Bandwidth, etc		
25	Solution should provide:		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	• Application Dashboard • Per Application Analytics • SLA Breakdown (Network, per server) • SSL Statistics (handshake and cypher breakdown, rejected handshake) • SSL CPS • System Dashboard • Network Dashboard • L4 Events • Per transaction type events (delay, user agent, response, headers) • SSL Events (type of handshake, cypher, TLS version)		
26	The WAF should support the following escalation modes: a) Active, b) Bypass, c) Passive		
API SECURITY			
1	WAF must provide inbuilt capability of API security including support for uploading swagger file and protect leakage of user credentials accessing the web applications using HTML field Obfuscation to protect against malware-based attacks and the solution should have capability to protect Credential Attacks that can steal credentials from the user's browser to avoid cyber exploits. It should be able to authenticate users based on browser type and version, operating system type and version. Necessary logs to be generated for audit and compliance.		
2	Solution should be able to Imported OpenAPI file automatically and configures policy with all API specific parameters as a list of allowed URLs, parameters, methods, and so on. Solution should have API security template which pre-configures WAF policy with all necessary violations and signatures to protect API backend.		
3	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
HIGH AVAILABILITY			
1	The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to achieve horizontal scaling		
MONITORING, LOGGING AND REPORTING			
1	The proposed solution should have the capability to create a granular logging policy per application. The system shall have ability to customize logging. The proposed solution should have the capability to define a customized log format for each application.		
2	The proposed solution should have the capability to define multiple log destinations for each application		
EASY ADMINSTRATION			
1	Proposed Solution should have Role-based management & Access Control with user authentication. There should be web application security administrator whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor(similar) whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor d. Operator e. SSL Certificate Manager f. Guest		
2	The solution must support the following password management capabilities without relying on any external system:		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	a) Password validity period in days b) Password length (minimum required number of characters in the password.) c) Whether a password must be significantly different from the last password used d) Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password Complexity)		
3	The solution must be able to support the configuration of the following lockout settings from the solution management UI: a) Login failed attempts period (in minutes) in which entering an incorrect password multiple times locks an account b) Number of failed login attempts which result an account to be locked c) Lock duration in minutes		
4	Should have diagnostics capability support (e.g. logs, core dumps, Syslogs, configurations etc.) which can be used to share with Technical support team in case of any malfunctioning by the devices. Should have online vulnerability and configuration diagnosing tool.		
Product / OEM Evaluation Criteria			
1	WAF / WAF's Operating System should be tested and certified for NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions		
2	The WAF solution should be in the Gartner's/ Kpingercole/ SecureIQ Magic Quadrant of Latest published Report Web Application and API Protection/WAF.		

11.2.19. Extended Detection and Response (XDR)

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	Bidder should provide hardware and software and support license for broker/proxy if applicable. The bidder can provide a connection to the management server from air-gapped devices via an on-premise proxy server. Bidder to consider necessary license for broker/proxy from day 1.		
2	The proposed solution should continue to function and provide all technical functionalities irrespective of whether the Anti-virus solution/Endpoint Protection solution is available to the customer or not.		
3	AI/ML-based detection, behavioural analytics, signature-based detection, threat intelligence integration		
4	The proposed solution must deliver wide range of detection and response capabilities across multiple layers (e.g. Endpoint, Servers, network etc.) to provide enhanced, efficient and effective visibility to identify low and slow attacks.		
5	The proposed solution should not ask for a reboot for a minor version, hotfix upgrade, or post-installation of an agent.		
6	The proposed solution should ingest logs from different channels of the customer including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.		
7	The proposed solution should have advanced AI and ML capabilities to detect cyber threats in real-time and take immediate remedial action as a response to block the cyber-threat / cyber-attack.		
8	Proposed solution must be compliant with guidelines of MeitY for all their scoped services such as Data Lake, Management console, sandbox, logs and analytic services. Solution should be SOC-II type2+ and ISO/IEC 27001 compliant.		
9	All the necessary license to be quoted and supported for 5 years. Proposed solution and its associated services like management, sandboxing etc. must reside with in India (as per MeiTY guidelines) judiciary boundary.		
10	The proposed XDR solution, along with EDR component should be from a single OEM.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
11	The OEM must deploy such solution in a customer environment in India (10,000 end points or higher) & must be operational for last 2 years & more. The deployment has to be for Indian customer hosted within India cloud region having a resilient architecture (DC-DR sites).		
12	The proposed solution must be deployed in at least 5 customer environments in India, running successfully in a production environment.		
13	The proposed solution must be deployed in at least 5 customer environments in abroad, running successfully in a production environment to understand global threat patterns.		
14	The offered OEM should not be debarred or blacklisted by any organizations of Govt/State Government/PSU/Public Sector Banks as on last date of bid submission.		
15	The proposing solution OEM should have Development and Engineering centre based in India.		
16	The proposed solution should have on-premises server hosted at customer's DC and DR to bridge the connections between customer's intranet (endpoints, server and network) and the cloud. No endpoint, server or network device of the customer's intranet should directly connect to the cloud.		
17	The proposed solution should provide complete threat visibility i.e. End-to-end details of threats such as compromised IT assets, malware, IOCs / IOAs, tools, tactics and procedures.		
18	OEM should provide dedicated SaaS management instance with dedicated URL for the customer.		
19	The proposed solution must allow administrators to manage and control temporary exceptions for trusted devices if needed.		
20	The proposed solution must provide a dedicated tenant, ensuring complete isolation and data segregation, and not share with any other customer.		
21	The proposed solution should identify and protect customers' assets from known and unknown threats, including but not limited to zero-day, malware, ransomware, file always based and file-less attacks. Further, response action should be available to remediate the threats in real-time.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
22	The proposed solution should provide a unified console to view the entire chain of events linked to the threat across multiple channels like endpoint, server, cloud, network, etc.		
23	The proposed solution should provide details of tactics, techniques and procedures used by the attacker and provide mapping of threat / alerts to MITRE ATT&CK framework.		
24	OEM must be in the Gartner Market Guide / SPARK Matrix / equivalent industry analysis for Digital Forensics and Incident Response Retainer Services (DFIR) in 2024 / 2025.		
25	The proposed solution should provide detailed information of system and network level activities to rapidly assess the nature and extent of an attack and subsequently initiate response activities in real-time.		
26	The proposed solution should provide a unified console for threat analysis, forensic analysis, threat hunting, investigation and threat response functionality.		
27	The proposed solution should have a single console for policy management of all the EPP, EDR, Exploit Protection, Anti-APT, Host Firewall, Identity Analytics, Device Control etc		
28	The proposed solution should provide RCA of the Incident in a stitched way, i.e. Endpoint and Firewall alerts which are related to same attack chain should be visualized in a single incident tree.		
29	Proposed solution must have a unified management console for all action, policy, troubleshooting, threat hunting, Integration etc.		
30	The proposed solution must support all endpoint related task from unified management console for following, but not limited to: Generation of troubleshooting file, Agent Proxy configuration, Uninstallation of agent, Agent status etc..		
31	The proposed solution must provide detailed data about the hardware, software, and operating system of each endpoint. This must include information such as: 1. CPU and memory specifications 2. Installed software and versions 3. Operating system details 4. Network interfaces and configurations		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	5. Disk usage and partitions		
32	The proposed solution must provide the capability to set specified agent proxy settings from the management console, allowing agents to communicate with the cloud via proxy. There must be no dependency on agent-level proxy settings.		
33	The proposed solution should have single console for below features : - NGAV & EDR - Threat Hunting - Forensic - Network Traffic Analytics - Historical Queries - Identity Analytics - Cloud Workloads & Container Security		
34	The proposed solution should be able to prioritize incidents/alerts by identifying and highlighting the alerts/threat that pose greater risk to the customer.		
35	The proposed solution should support detection of advanced malware, zero-day attacks and exploits without requiring signatures at endpoint, server, network and cloud.		
36	The provided solution should support static, dynamic, bare metal, network analysis & recursive analysis etc.		
37	Proposed solution should able to consume threat intelligence from third party in form of CSV or JSON, and should able to distribute crowdsourced threat intel from cloud based malware analysis service to firewall, endpoint agents.		
39	The proposed solution should provide remediation suggestions to assist security teams for remediation/containment of the threat identified in the customer's environment.		
40	The proposed solution should provide multi-factor authentication for logging in to the console.		
41	The proposed solution should be able to send alerts/notifications over email.		
42	The proposed solution should support the creation and configuration of role-based access control (RBAC) through the GUI console		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
43	The proposed solution shall provide feature to generate, schedule, and view reports based on various parameters captured / stored. Out of the box reports should also be available.		
44	The proposed solution should provide minimum 30 day online raw log / telemetry data retention and minimum 180 days retention for alerts and incident related data (including applicable forensic data). Log retention (as mentioned) is applicable to all the components of the proposed solution.		
45	Proposed solution should have minimum 100 GB per day cloud-based storage capacity to ingest and store logs from 3rd party data sources like endpoints, servers, networks for correlation, stitching, analysis and present in single pane of visibility. Cloud based storage should be scalable to 1 TB per day or more by adding only license in future. The cloud storage should be in India.		
46	Proposed solution should have identity analytics to detect user/identity-based threats such as lateral movement, and it should have supervised and unsupervised learning capabilities.		
47	Proposed solution must have analytical capability but not to be limited to process, user/identity, device, Network, File, Registry, and Security alerts and should notify/alert as and when any anomaly is identified based on profiling, modelling, or benchmarking.		
48	The proposed solution is capable of Detection & Prevention Capabilities Against Identity Theft Attacks Such Below: • SSO & AD Session Hijacking • Data Exfiltration • Compromised Credentials • Compromised Devices • Privileged User Monitoring • Unconstrained Delegation • Enumeration (User, SMB, NetBIOS, DNS etc.) • The Printer Bug • Protection against Mimikatz to Extract the TGT • Pass the Ticket		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	• Pass the Token • Pass the Hash • DCSync to Domain Compromise • Impossible traveller		
49	Proposed solution should have timeline view and 360 degree identity view with its user risk score.		
50	The proposed solution should support demonstration Of Impersonation, Risky User Activities, Credential Misuse, Impossible Travel etc.		
51	Solution should allow to query either behaviour or IOC or any telemetry which is expected from agents, and it should not be dependent on agent status.		
52	The proposed solution should use machine learning to provide user / system risk score to assist security analysts in making informed decisions to remediate / block the threats.		
53	The proposed solution should provide querying mechanism in the console to enable threat hunting across different channels like endpoint, servers, network, cloud, etc.		
54	The proposed solution should detect malicious user activities including but not limited to stolen or misused credentials, credential harvesting, exfiltration, or brute-force attacks by applying AI/ML techniques		
55	The proposed solution should be scalable to incorporate customer's future requirements.		
56	The proposed solution should provide incident management functionality like adding comments on the incident, change status of incidents like Open, Closed and should support assigning of incidents to different team members within customer team		
57	The proposed solution must provide the ability to automatically capture record and analyse wide array of endpoint parameters, behaviour, execution, and subsequent events in order to assess system operations and enable threat hunting and incident forensic activities. Below is the minimum features from the proposed solution shall be capable of capture out of box		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	i. Registry - Record full registry strings and modified registry string ii. User Activity - Any user activities like threats on endpoint, process that tried to enumerate/query, set or change detailed information on endpoint system, like-PowerShell activities, scripted communication, encoded traffic etc. iii. Activity - Investigation of threat's activities which helps administrators re-construct the events of the security incident from start to end without relying on any 3rd party component iv. Processes and Services - Record process that launch any process or target to escalate privileges for specific programs and target to inject specific process through the allocation of memory or creation of remote threads on it. It must provide a linking of networking processes with their parent processes including the recent historical listing of processes for acquisition and analysis during the incident response. v. Software Changes – Forensics metadata related to changes pertaining to Operating System, driver and program installation, uninstall, patching and modification information must be captured and available vi. In-memory Activities - In-memory activities associated with potentially malicious activity associated with processes and In-memory detailed assessment/Investigation using search in-memory using Yara files, IOC's etc vii. Logon Activity - System, Application Experience, Security, AppLocker, PowerShell, Application, Windows Defender, Task Scheduler, Print Service, and Terminal Services event logs viii. Process tracking and protection - recognize unique file executions and validate malicious process, alert and generate triage on such malicious processes detections		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
58	Proposed solution must support Windows 7, 8, 10, and 11, windows Server 2008 to 2022 or latest. Supports Linux OS - Alma Linux, Amazon Linux/ Amazon Linux 2/ Amazon Linux 2023, CentOS, Debian, Oracle Linux, RedHat, Rocky Linux, SUSE, Talos Linux, Ubuntu.		
59	Also the proposed solution must support Ventura MacOS, Sonoma MacOS, Monterey MacOS, BigSur MacOS, Sequoia MacOS, latest and last two major builds, Android and IOS latest and last major release, Kubernetes (containers), and should have VDI support.		
60	The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below: -File hash Information collection -Termination of the service -Download of binary -Addition of hash value to block list -Delete the file -Send the hash to get the verdict (TI integration) -Execute a python script -Execute a powershell script		
61	Proposed solution must allow administrator to allow USB/Removable device access based on time like minutes, hours, day without modifying any policy.		
62	Proposed solution must allow administrator to allow USB/Removable device access based on time like minutes, hours, day without modifying any policy.		
XDR - Endpoint and Server Security Component			
63	The proposed solution must provide all capabilities (as per technical requirements of the customer) for threat detection and response in a single lightweight agent with minimal /no impact on performance of the endpoints and servers as well as minimal bandwidth requirements for communication with the on-premise server at DC/DR.		
64	The proposed solution should support collection of logs from third party security solutions like Active Directory, Firewall,		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Proxy, DNS, DHCP, O365 etc with any additional licenses included as part of proposed solution from Day 1		
65	The proposed solution must be able to detect and respond to cyber-threats on the endpoints and servers with artificial intelligence and machine learning capabilities that may be missed by traditional security solutions.		
66	The proposed solution must provide behavioural based cyber threat detection and prevention capabilities.		
67	It should support advanced querying language with support for wildcards, regular expressions, JSON, data aggregating, field, and value manipulation, merging of data from disparate sources, and visualization of data with ability for an analyst to easily pivot between views. In addition, it should support granular filtering and sorting capabilities.		
68	The proposed solution should provide insightful investigative capabilities, a rapid response for suspicious objects/activities and a centralized visibility across the all the endpoints and servers of the customer.		
69	The proposed solution should be able to monitor and protect endpoints and servers from threats regardless of their location like on-premise, cloud and roaming / remote.		
70	The proposed solution should provide endpoint agent self-protection to ensure no tampering / unauthorized modifications and should have password protection to disable configuration changes / uninstallation in an unauthorized manner.		
71	The proposed solution should have advanced machine learning capabilities and behaviour-based anomaly detection mechanism to detect cyber threats. It should be independent of signatures.		
72	The Proposed solution must comprise of below minimum functionalities & deliverables: a) Incident data search and investigations: Search historic and live systems for indicators b) Alert triage or suspicious activity validation: Workflow & orchestrated Integration to and from EDR and external file/indicator validation services		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	c) Suspicious activity detection: Automated threat-intelligence- based match and malicious behaviour detection d) Threat hunting or data exploration: Link entities investigated across different systems and additional visualizations e) Stopping malicious activity: Centrally Monitor processes, UAC Logs, detect malicious artefacts and help remove files, prevent execution, conduct network isolation, Manual & script based Remediation f) Stopping malicious activity: Centrally Monitor processes, UAC Logs, detect malicious artefacts and help remove files, prevent execution, conduct network isolation, Manual & script based Remediation g) Incident Live Forensics: Root cause Analysis, Forensic Acquisition, Incident Investigation at scale h) h. Stacking data & finding the unknown threats: Data Streaming, Data Analytics, Custom IOC sweeps, API access		
73	The proposed solution must have no dependency on signature based solution with typical use cases covered as below -IOC Detection (Malware & Methodology TTP's), -Intelligence feed integration, -Custom IOC creation, -Triaging an alert, -Containment/Isolation of a threat/machine, -Tracking compromised user activity , -Command-line visibility, -Investigating lateral movement, -Data staging and exfiltration, -Suspected anti-forensics activity -Investigating suspected rootkits & backdoors -Data Acquisition - Live Forensics -Hunting exercise like Stacking data & finding the unknown threats based on endpoint and server activity anomalies.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
74	The proposed solution should have 350+ Analytics based IOAs out of the box and also should not charge for any additional IOA rules that needs to be created		
75	The solution should have a remote Host Remediation shell access/CLI session feature available from the EDR console.		
76	The solution should be able to mitigate the impact of a compromised system with network isolation using workflow-driven containment to prevent lateral spread.		
77	The proposed solution must provide functionality for collection of forensics artifacts from the endpoints and servers on Windows and Mac OS systems.		
78	The proposed solution shall support the collection of forensic data using the same EDR agent without making any changes in the system (Endpoint Machine) configuration.		
79	The proposed solution shall have the capability to do enterprise-wide search and destroy across multiple endpoints with single search.		
80	The proposed solution should be able to detect and respond to exploit processes that are more complex than a simple signature or pattern.		
81	The proposed solution shall provide protection against exploits including MacOS, Windows, Linux (Ubuntu & Centos Flavours) and processes running in Linux Containers		
82	The proposed solution should have strong anti-evasion capabilities to ensure that no cyber-threat / attack in its pre-execution and execution stage goes undetected.		
83	The agent of the proposed solution must co-exist with any other software, application and Anti-Virus / Endpoint Protection solution on the endpoints and servers of the customer and provide seamless operation to provide extended detection and response functionality without any process crash, system crash or performance issue.		
84	The proposed solution should perform threat analysis of endpoints and servers to trace and block file-less malware, advanced persistent threats, browser-based attacks, zero-day attacks and any known or unknown attack / threat in the customer's environment.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
85	The proposed solution must provide threat hunting and response capability across all the endpoints and servers of the customer.		
86	The proposed solution must continuously collect, analyse and correlate data from the endpoints and servers with activities including file interactions, process execution, network traffic, registry change, user login, installed software, commands executed to identify and block malicious activities.		
87	The Proposed solution should support the forensic artifact collection from the start of Windows installation.		
88	The proposed solution should have feature to quarantine the endpoint and block all network communication (except with central management console) from/to the endpoint directly from the central console and allow investigation activities to be performed on the endpoint remotely. It should also provide option in central console to restore the network connectivity which was previously isolated / quarantined by the proposed solution.		
89	The proposed solution should support data acquisition from the unified console to conduct detailed in-depth analysis of the endpoint over a specified time-frame.		
90	The proposed solution should have capabilities for real-time detection and response to quickly detect, investigate, and remediate the threat on the endpoint and servers.		
91	The proposed solution should provide investigation and threat containment by complete and continuous incident logging with all relevant fields required for investigation.		
92	The proposed solution should be able to identify and terminate malware process and threads in memory, repairing the registry, delete any dropped malware files, remove any services created by malware, restore files damaged by malware.		
93	The proposed solution should be able to identify all the endpoints and servers that are infected with the same threat and display the entire threat attack lifecycle in a single view.		
94	The proposed solution should have the capability to detect threats using AI and ML, prioritize incidents and provide		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	immediate remediation of the threat at the endpoints and servers.		
95	The proposed solution should have advanced response options at the endpoints and servers including but not limited to isolation, network restoration, terminate process, delete file, block (IP, hash) & block specific ports.		
96	Behaviour monitoring must have thorough inspection capability to detect, and block compromised / malicious files. It should monitor for newly encountered program downloaded from various channels like web / email/ removable media.		
97	The proposed solution should provide real-time anti-exploit capabilities to protect customer's assets from exploit attacks including but not limited to memory corruption, logic flaw, malicious code injection/execution, application exploits prevention, DLL Hijacking, etc.		
98	The proposed solution should protect against exploits of unpatched OS and third-party application vulnerabilities and prevent execution of all unauthorized /malicious software, scripts, and dynamic-link libraries (DLLs).		
99	The proposed solution must identify and block privilege escalation attacks like rootkit, boot kit or any other such malwares and provide process monitoring mechanism.		
100	The proposed solution shall automatically submit unknown files to sandbox without the need of administrator intervention and it should support up to 1,000,000 sample uploads per day and up to 1,000,000 verdict queries per day and sandboxing should support static, dynamic, bare metal, network analysis & recursive analysis etc.		
101	The proposed solution must be able to detect attacks & alert using methodology indicators such as understanding attacks loaded into memory to steal passwords, PowerShell commands usage with arguments run by an attacker for stealing credentials, lateral movement, privilege escalation, etc.		
102	The proposed solution should provide protection and recovery from threats like ransomware, malware, browser exploits, Advanced persistent threats or any new or anticipated threats.		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	Ransomware protection must not be limited to specific ransomware behaviour /variants.		
103	The proposed solution should support restoration of the endpoints and servers in case the endpoints / servers are infected by ransomware or by any other cyber-threat / attack.		
104	The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file		
105	The proposed solution should have application blacklisting functionality to control execution of unauthorized or malicious applications in the customer's environment.		
106	The proposed solution should provide Pre and post compromise attack visibility (Root Cause Analysis). The root cause analysis methodology should have an interactive GUI with easy-to-use options.		
107	The Solution support Network Detection & Response (NDR) capability with necessary license in future : • Malicious Encrypted Traffic (Header Analysis) • North & South Malicious Traffic Monitoring Using AI (Data Exfiltration, C2C, DNS Tunnelling etc.) • East & West Malicious Traffic Monitoring using AI (Lateral Movement) • Protocol Monitoring (DNS, NTLM, MSRPC, Kerberos, SSL/TLS, LDAP, IMAP etc.) • Identify Data Exfiltration Via Legitimate Protocols (DNS Tunnelling, ICMP Tunnelling). • Identify And Block Usage Of Common Attack Tools (Metasploit, Empire, Cobalt Etc.) • Suspicious Network Activity within Cloud		
108	The Proposed solution should support backward and forward matching of IOCs and Custom Behavioural Indicators.		
109	The proposed solution should have the capability to inspect and block attacks which occur in encrypted manner.		
110	The proposed solution should provide chronological events that happened on the endpoint which includes system as well as user activities.		
111	The proposed solution should be able to detect and respond to the advanced threats which come through client-side		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	executable files, PDF files, Flash files, MS Office files, Images, Archives (zip, rar, 7zip), RTF files and/or other objects or file types.		
112	The agent of the proposed solution should continue to enforce the policies whether the management server is available or not i.e. the agent should work in offline mode as well.		
113	The proposed solution should allow to perform all configurations from the central management console including but not limited enabling/disabling agents, selecting and applying new policies, creating custom policies, reports.		
114	The proposed solution should have the capability for sandbox analysis of suspicious and malicious files along with AI/ML based malware and threat detection techniques.		
115	The proposed solution should automatically perform sandbox analysis of suspicious files without manual intervention.		
116	The proposed solution should provide secured remote connection on target endpoints / servers for investigation and execute commands / scripts centrally without requiring physical access to the endpoint / server.		
117	The proposed solution should be able to terminate an active malicious process on a specific endpoint / server or on all affected endpoints / servers.		
118	The proposed solution should support response actions on a target endpoint / server or on all affected endpoints / servers.		
119	The proposed solution should support discovery of rogue devices present in the network where current EDR agent is not installed		
120	The proposed solution must provide live query to the endpoints and servers to assist forensics investigations.		
121	Solution must support automated stitching of telemetry from endpoint, server, network etc., which is require for analysis and present it in single pane of visibility, and it should support noise cancellation (removing unwanted binaries, dll from visualization chain).		
122	Proposed solution should able to visualized client relational database directly to log repository for query using open		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	database connectivity for MySQL, PostgreSQL, MSSQL, and Oracle etc.		
123	The proposed solution must collect host firewall logs to provide comprehensive visibility into network traffic and security events on endpoints. These logs must be used to monitor and analyse firewall activity, such as blocked or allowed connections, and help in identifying potential security threats.		
124	The proposed solution must allow security teams to combine related incidents into a single incident. This must help in reducing the number of alerts and provide a more comprehensive view of an attack or threat.		
125	The proposed solution must incorporate automated XDR threat correlation and log stitching capabilities, aggregating data from third-party security solutions (e.g., firewalls, email security) to facilitate incident response, thereby eliminating manual queries and data ingestion into the data lake.		
126	Scheduled Queries - The proposed solution must allow administrators to set up queries that run at specified intervals. These queries must be used to automate the collection and analysis of data, helping security teams stay on top of potential threats without manual intervention.		
127	The solution must have the capability to protect systems within an air-gapped network, utilizing in-built broker components from the same OEM. Additionally, the solution should not rely on third-party protection extensions, ensuring a self-sufficient and secure architecture.		
128	The proposed solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the threat and respond to the threat to protect customer's assets at all times.		
129	The proposed solution should allow investigative work to continue on the isolated / quarantined device without allowing malicious activity to spread.		
130	The proposed solution should support adhoc and scheduled scanning of endpoints and servers, apart from real- time threat detection and protection functionality. There must not be any dependency on third-party systems or APIs to run the scans. If		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	scheduled scans require a third-party device with API configuration, this must be clearly specified.		
131	The proposed solution should collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner and eliminate the need of manual configuration of rules or policies.		
132	All binaries / updates from the OEM that are downloaded and distributed must be signed and signature verified during runtime for enhanced security.		
133	The proposed solution should reverse destructive data event including but not limited to ransomware. It should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state.		
134	The proposed solution should have the functionality for endpoint and server agent updates directly from the central management console.		
135	The proposed solution should inspect the network connections from / to the endpoint for any suspicious / malicious activity and block any such connection to prevent the customer IT infrastructure at all times.		

11.2.20. Link Load Balancer

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
Link Load Balancer			
1	**Solution Overview** High-performance LLB appliance in HA mode for ISP link failover, bandwidth optimization, and traffic steering across DC and DR		
2	The proposed appliance should be a dedicated appliance, it should not be part of any Firewall or UTM.		
3	Traffic Port Support: 8 × 10GE Fiber ports (10G SR populated) + 8 × 1GE Base-T ports; optional 2 × 40GE QSFP+ ports. Device L4 Throughput: 30 Gbps and scalable up to 75 Gbps Layer 4 connections per second: 1 Million Layer 7 requests per second: 2 Million		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	RSA CPS(2K Key): 50,000 ECC CPS (EC-P256): 25,000 with TLS1.3 Support RAM: 32GB and scalable up to 256GB Concurrent Connections: 80 Million The appliance should have dedicated 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port		
4	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1		
5	The proposed appliance should support the below metrics: — Hash/Equivalent, — Persistent Hash/Equivalent, — Weighted Hash/Equivalent, — Round-Robin, — Response Time, — Bandwidth, etc		
6	Following Server Load Balancing Topologies should be supported: • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses		
7	The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature, that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Each Virtual Instance contains a complete and separated environment of the Following: a) Resources b) Configurations c) Management d) Operating System		

Sl. No	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
	The proposed device should support 8 Virtual Instance from Day 1.		
8	Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications		
9	The Proposed Appliance should support Standalone as well as Virtualized Mode. The proposed Hardware must have Bandwidth Management feature from Day 1		
10	DNSSEC based Global Load Balancing should be supported in the proposed device from Day 1		
11	The proposed device should support standard VRRP (RFC - 2338) or equivalent for High Availability purpose.		
12	The device should support for IPv4 and IPv6 traffic		
13	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend		
14	The solution should have support for multiple VLANs with tagging capability		
15	The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure		
16	Device should be accessed through the below: • Using the CLI • Using SNMP • REST API • Using the Web Based Management		
17	The proposed appliance/software should be EAL2 / NDPP certified.		
18	Five years Comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support.		
19	Dashboard: Centralized GUI with real-time traffic analytics and link health Alerts & Logs: SNMP, Syslog, and email-based alerts; audit logs for link events License Audit: OEM must provide periodic license usage audit reports		

11.2.21. Workstation

Sl. No.	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
1	Processor	X86 latest Processor with minimum 24 MB cache, 12 cores and support for processor speeds up to at least 4.80 GHz or higher. (Processor TDP minimum 65W and Processor Launch date should not be older than 1 year from Bid publishing date).		
2	Chipset	Compatible Chipset with the above processor.		
3	Motherboard	Motherboard make from the same Desktop OEM (Desktop OEM logo must be embossed in the motherboard)		
4	Memory	Minimum 16 GB memory with support for memory expandability up to 64 GB or higher		
5	RAM Type	DDR5 with 4400 MHz or higher.		
6	DIMMs &Expansion Slots	2 DIMM slots or more, minimum 3 x M.2 slots.		
7	Hard Disk Capacity (SSD PCIe NVMe M.2)	Minimum 1 TB or more, support up to 2 TB PCIe M.2 NVMe SSD or more		
8	Graphics	Integrated / Dedicated Graphics (support 4K resolution).		
9	Ports: USB / HDMI / Display Port (Integrated in the motherboard)	Integrated USB Port: Minimum 5 no's (Min 4 nos. of USB 3.2 Gen-1 and 1 x USB 3.2 Type C), 1 x Secure Digital card reader slot.		
		Integrated HDMI Port (1.4) or better: Minimum 1 no.		
		Integrated Display Port: Minimum 1 no should be easily accessible.		
		Network: 10/100/1000 on-board integrated Network Port.		

Sl. No.	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		Audio: 1 x Audio Line-out port /1 Combo Audio jack		
10	Audio and Camera	Integrated Audio controller with Internal speaker (minimum 2 x 2W), Minimum full HD camera with microphone and physical privacy option		
11	Cabinet	All in One		
12	SMPS	Minimum 150 Watt (Internal integrated Power supply without any external power adaptor)		
13	Wireless	Integrated Dual band ax wireless with Bluetooth 5.2 or higher		
14	Operating system support	Windows, ubuntu or Redhat (certification must be available in the public domain against the quoted model name)		
15	Manageability	System Serial No, OEM Name, HDD, RAM, Processor Information, to be available into the BIOS (CMOS)		
16	Security	Discreet TPM 2.0, chassis Intrusion switch / Intrusion Sensor with chassis physical security cable lock slot.		
17	Monitor / Display	Narrow bezel, 23.8" or higher FHD (1920 x 1080) display. Panel Type: Antiglare, IPS / VA / TN, and LED backlight technology with AIO stand.		
18	Keyboard	Standard full size USB keyboard (Same AIO OEM make)		
19	Mouse	Standard USB Optical scroll mouse (Same AIO OEM make)		
20	Production Unit, Certification and Compliance	EPEAT India for the quoted AIO model (not for the series). Proof of certification to be submitted.		
		FCC, CE, UL or equivalent, ROHS for the quoted desktop model (not for the		

Sl. No.	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Compliance Cross reference Page No.
		series). Proof of certification to be submitted.		
		Minimum Energy Star 8.0, TCO Certification for the AIO model (minimum TCO 8). Proof of certification to be submitted.		
		OEM ISO 9001 and 14001 Certified India Unit (Proof of Certification of India unit to be submitted). Proof of certification to be submitted.		
21	Warranty	5 years onsite comprehensive OEM warranty (OEM supplied model warranty must be visible in the OEM website in respect to each product serial number)		
22	Manufacturer Criteria (OEM)	Minimum 10 Years presence in India. OEM letter confirming that Operating system pre- loaded / pre-installed from OEM factory and service request would be placed directly with the Desktop AIO OEM for the duration of warranty. OEM Toll free service phone no, Email ID/WhatsApp chat and online chat option must require along with the bid offering.		
23	Factory Preloaded /Preinstall Operating System	Factory Preloaded / Preinstall Operating System: Windows 11 Professional. OEM letter confirming that Operating system is pre-loaded / pre-installed from OEM factory and is genuine. Such declaration should be signed by a person having power of attorney/board resolution in OEM.		
24	Microsoft Office	Microsoft Office 2021 with minimum MS Word, Power point, Excel and with		
		Original Serial Key		

12. Service Level Agreement

This SLA outlines the minimum service levels required based on contractual obligations, including performance indicators and measurements for State DR-DC. The Bidder is obligated to ensure the provision of all necessary services, monitoring their performance to comply effectively with the specified standards, ensuring quality services. The Bidder must meet service level objectives and corresponding parameters to ensure timely delivery and quality services in accordance with the document's standards. Service level indicators and target performance levels are to be maintained by the Bidder throughout the contract period. Strict enforcement of SLA is ensured, and an agency will report Bidder's performance against the target metrics.

- The benefits of this SLA are:
- Triggering a process to draw attention to performance aspects falling below agreed-upon thresholds.
- Explicitly stating Customer expectations for performance.
- Empowering Customer to control service levels and Bidder service performance.
- The Bidder must submit a quarterly report to monitor service performance and the effectiveness of this SLA.

12.1. Brief Description of the Services

The Bidder will provide the following services for Supply, Installation, and Maintenance of basic Infrastructure for the establishment of the State Disaster Recovery Centre at Keonjhar , as detailed in the RFP's Scope of Work:

12.2. SLA Definitions

For this Service Level Agreement, the following terms are defined:

- **Availability:** The time services and facilities offered by the Bidders are available for conducting operations from the equipment hosted in the Data Centre.
- **Downtime:** The time services and facilities are not available to Customer, excluding scheduled outages for the Data Centre.
- **Helpdesk Support:** The Bidder's 24x7x365 Helpdesk Support Centre for fault reporting, trouble handling, ticketing, and related enquiries.
- **Incident:** Any event/abnormalities in the functioning of the Data Centre Equipment/Services that may lead to a disruption in normal operations.
- **Critical/Medium/Low Incidents:** Categories based on the impact on overall functioning, resolution requirements, and interruptions.
- **Resolution Time:** The time taken by the Bidder staff to troubleshoot and fix the problem from the time the call has been logged at the Helpdesk.

12.3. Implementation SLAs & Penalties

12.3.1. Mobilization of the Project:

#	Services	Parameter	Penalty
1	Mobilization of the resources	Go live of the DR + 7 days	1% of Quarterly Payment of the Payment Milestone P5

12.3.2. IT & Non-IT Infrastructure

The T is the date of Kick-off/signing of the contract will be treated as the project start date. The total time for the completion of the project, DR-DC, will be 6 months, including the certification of the DR-DC. If the Installation, Commissioning, Testing, FAT, and Go-Live are not executed within the specified time, Liquidated Damages (LD) will be imposed on the successful bidder as per the LD Table mentioned below.

Sl. No	Milestone	Deliverables	Timeline	LD
1	Inception Report	• Complete project plan. • Risk assessment report. • Initial project schedule	T + 1 Month	0.5% per week of the payment milestone P0 (Max 10% of P0)
2	Solution Design	• Detailed design documents. • Engineering blueprints. • Approval of designs from stakeholders	T + 2 Months	0.5% per week of the payment milestone P0 (Max 10% of P0)
3	Delivery of IT & Non-IT Infrastructure components	• Purchase orders placed for all required equipment. • Confirmation of delivery schedules. • Delivery of all the IT Infrastructure components	T + 3 Months	0.5% per week of the payment milestone P1 (Max 10% of P1)
4	Installation & Commissioning of IT & Non-Infrastructure components	• Successful installation of all IT and Non-IT components including power infrastructure. • Successful installation of Fiber optic cabling. • Integration with existing systems.	T + 5 Months	0.5% per week of the payment milestone P2 (Max 10% of P2)

Sl. No	Milestone	Deliverables	Timeline	LD
5	Final Acceptance Test & Go-Live of DC. Engagement of Operation & Maintenance team	• Perform the Test cases. • FAT completion	T + 6 Months	0.5% per week of the payment milestone P3 (Max 10% of P3)
6	Certifications	• Completion of the certification as mentioned in the section 8 of this RFP	T + 6 Months	0.5% per week of the payment milestone P3 (Max 10% of P3)

Note:

- Monthly Progress Reports: SI must submit detailed progress reports at the end of each month, outlining the completion status of each milestone, any issues encountered, and steps taken to address them.
- Regular Review Meetings: Monthly review meetings shall be conducted with all the stakeholders to discuss progress, address concerns, and ensure alignment with project timelines.

12.4. Operational SLA

12.4.1. IT Infrastructure related Level

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	Individual Server Availability (including the OS, database and the application running on it)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value
			>= 99.96% to < 99.97%	0.25% of the QGR value
			>= 99.93% to < 99.96%	0.5% of the QGR value
			< 99.93%	1.0 % of the QGR value for O&M [Record as Event of Default] Letter of warning may be issued to the bidder.

Sl. No.	Definition	Measurement Interval	Target	Penalty
2	Storage Availability	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value
			>= 99.96% to < 99.97%	0.25% of the QGR value
			>= 99.93% to < 99.96%	0.5% of the QGR value
			< 99.93%	1.0 % of the QGR value [Record as Event of Default] Letter of warning may be issued to the bidder.
3	Managed Backup Service Availability (with agreed retention period) Managed Backup Service provides automatic scheduled backup of Customer Data to the designated storage vault 'as is where is' and also restore it back in the same format as backed-up. Data backup Success Ratio must be calculated.	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value
			>= 99.96% to < 99.97%	0.25% of the QGR value
			>= 99.93% to < 99.96%	0.5% of the QGR value
			< 99.93%	1.0 % of the QGR value for O&M [Record as Event of Default] Letter of warning may be issued to the bidder.
4	LAN availability (Active and passive components)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to<99.98%	0.1% of the QGR value
			>= 99.96% to < 99.97%	0.25% of the QGR value
			>= 99.93% to < 99.96%	0.5% of the QGR value

Sl. No.	Definition	Measurement Interval	Target	Penalty
			< 99.93%	1.0 % of the QGR value [Record as Event of Default] Letter of warning may be issued to the bidder.
5	Preventive Maintenance (PM) plan /Schedule	Quarterly Reporting	100% Carried Out. PM Plan should be approved by Project Manager, DR-DC/OCAC prior to be carried out in that quarter. The approval should be within 1 Hour after the approval of the request by the Customer/ User	2% of the QGR value for delay in PM activity. 0.1% of the QGR value for non- adherence to PM plan or without approval. If PM of any equipment missed in a quarter, the same should be carried out within next two weeks. Else penalty of Rs. 5000/- per day per equipment for delays will be deducted. 0.5% of the QGR value for more 1 hours of delay beyond the target time. To the maximum capping of 5 Hrs.

12.4.2. Virtual/cloud Infrastructure Related Service Level

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	Provisioning and De-Provisioning of Virtual Machines	Quarterly		1.0 % of the QGR value for more 5 hours of delay on an incremental basis
2	Overall Cloud Solution Availability (includes cloud network, cloud virtualization layer,	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value

	cloud storage, virtual OS, cloud orchestration layer, cloud security layer and any other requisite component and services)		>= 99.96% to < 99.97%	0.25% of the QGR value
			>= 99.93% to < 99.96%	0.5% of the QGR value
			< 99.93%	1.0 % of the QGR value [Record as Event of Default] Letter of warning may be issued to the bidder.
3	Production Cloud or Cloud Dashboard is down; business operations severely impacted with no workaround; or a security issue	Every instance in the Quarter	Up to 25 Minutes	No Penalty
			>25 min to <= 1hr in case of peak hour (8 am to 8 pm on weekdays) and > 1hr at any other time	0.5% of the QGR value for 1st time and 0.1 % of QGR value for every subsequent lapse.

12.4.3. Security and Incident Management

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	For every Virus attack reported and not resolved within 36 hrs from the time of attack.	Every instance in the Quarter	Beyond 36 hrs	Rs.20,000.00 for delay of every 24 hours or its part. If more than three virus attacks are reported in a quarter, then 10% of the QGR would be deducted as penalty.
2	For every instance of Denial of Service (DoS) attack and not resolved	Every instance in the Quarter	Beyond 2 hrs	Rs.5, 00,000.00 per instance.

Sl. No.	Definition	Measurement Interval	Target	Penalty
	within 2 hrs from the time of attack.			
3	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ DR-DC data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	Every instance in the Quarter	At every instance	Rs.5, 00,000.00 per instance.
4	For every Intrusion reported by firewall or IPS and not resolved within 2 hours from the time of report	Every instance in the Quarter	Beyond 2 hrs	Rs.2,00,000.00
5	Patch Management (including rules updation in Firewall, IPS and updation of any SPAM control policy)	Every instance in the Quarter	Within 2 hrs time from the approved Request	No Penalty
			> 2hrs and <=3hrs	Rs.1,00,000.00
			> 3hrs and <=4hrs	Rs.2,00,000.00
			> 4hrs and <=5hrs	Rs.3,00,000.00
			Beyond 5hrs for every 3 hrs	Rs.5,00,000.00

12.4.4. Non-IT Infrastructure

Sl. No	Services	Parameter /Target	Penalty	Remarks
1	Power Availability (DG, UPS etc.)	99.98%	For each 0.25 SLA slab (lower) a penalty 0.75 % on QGR shall be charged for each instance.	For each component 99.98-99.73 - 0.75% of QGR value 99.72-99.48 - 1.5% of QGR value and so on If the SLA goes below 99%, this will be record as Event of Default and Letter of warning may be issued to the bidder.
2	CCTV Availability	99.98%	For each 0.25 SLA slab (lower) a penalty 0.25 % on QGR shall be charged for each instance.	99.98-99.73 - 0.25% of QGR value 99.72-99.48 - 0.5% of QGR value and so on If the SLA goes below 99%, this will be record as Event of Default and Letter of warning may be issued to the bidder.
3	Cooling System and its associated components Availability.	99.98%	For each 0.25 SLA slab (lower) a penalty 1 % on QGR shall be charged for each instance.	99.98-99.73 – 1 % of QGR value 99.72-99.48 – 2 % of QGR value and so on If the SLA goes below 99%, this will be record as Event of Default and Letter of warning may be issued to the bidder.
4	Rack Temperature (PAC etc.…) Temperature to be maintained between 18 - 22°C at all times	99.98%	For Lower Performance (temp more than 22°C or less than 18°C) a penalty of 0.25% on QGR shall be charged for the variance of 1 C.	23°C-24°C - 0.50% of QGR value 22°C-23°C - 0.25% of QGR value 18°C-17°C - 0.25% of QGR value 17°C-16°C - 0.50% of QGR value and so on If the temperature goes above 27°C or below 15°C, this will be record as Event of Default and Letter of warning may be issued to the bidder.

Sl. No	Services	Parameter /Target	Penalty	Remarks
5	Relative humidity to be maintained between 50 – 60%	99.98%	For Lower Performance (relative humidity more than 60% or less than 50%) a penalty of 0.25% on QGR shall be charged for the variance of 5%.	40% - 45% - 0.50% of QGR value 45% - 50% - 0.25% of QGR value 60% - 65% - 0.25% of QGR value 65% - 70% - 0.50% of QGR value and so on If the relative humidity goes above 80% or below 20%, this will be record as Event of Default and Letter of warning may be issued to the bidder.
6	Fire Suppression and Detection System, and all other NON-IT components availability	99.98%	For each component and for each 0.25 SLA slab (lower) a penalty 0.25 % on QGR shall be charged for each instance.	99.98-99.73 - 0.25% of QGR value 99.72-99.48 - 0.5% of QGR value and so on If the SLA goes below 99%, this will be record as Event of Default and Letter of warning may be issued to the bidder

Note: If the bidder receives three or more letter of warning as mentioned above in a quarter, no payment will be process for that respective quarter. Any further letter of warning may result in termination of the contract.

12.5. Targets of Service Level Agreement

The SLA clause establishes minimum service levels based on performance indicators, with the Bidder ensuring provision while monitoring performance. Periodic reviews by the OCAC appointed Consultant/PMU and OCAC will include checking Bidder performance, discussing escalated problems, reviewing statistics, and obtaining suggestions for improvements. Interim reviews may be initiated, and procedures will be followed in case of disputes between OCAC and Bidder on performance targets.

The IT Infrastructure service level applies to devices specified in the Bill of Materials (BOM)

12.5.1. Help Desk Support Services Level

Response Time: The duration from the receipt of the incident (helpdesk call/alarm generated by the management system) to the initiation of work by a support team member.

Resolution Time: The total time from the receipt of the incident (helpdesk call/alarm generated by the management system) to the resolution of the incident.

12.5.2. Setting Priority Levels

The DR-DC Helpdesk is committed to resolving issues promptly during service calls, which is the initial approach before assigning a priority level. In cases where resolution does not occur during the service call, the Helpdesk will log and assign priorities to all outstanding requests.

Incident priority is primarily determined by its Impact and Urgency. The Helpdesk will maintain a matrix, as per the deployed EMS, which will automatically calculate incident severity based on the simple value of Impact x Urgency.

- Impact measures how critical an incident is to business operations.
- Urgency signifies the necessary speed of incident resolution.

Priority = Impact x Urgency Priority for Critical Components:

Priority Level 1

Standard compliance due to the total breakdown/failure of any equipment or component installed in the DR-DC. Users, equipment, and services covered under this Priority level include:

- Access Control Server Failure
- Anti-Virus Server Failure
- Active Directory Failure
- BMS Service Failure... (and more)

Priority Level 2:

Standard compliance due to partial breakdown/failure of any one of the equipment/components installed in the DR-DC. Indicative incidents/requests include:

- Agent – Installation, Configuration, Modification, Uninstallation
- Backup – New Backup Request, New Policy, Change in Policy, etc.
- Failure of physical infrastructure components related to humidity control and comfort air conditioning other than Server Farm Area... (and more)

Priority Level 3:

Partial/breakdown of any equipment/component installed in the Disaster Recovery Counter thought disrupting any services and failure/delay in undertaking and completing activities such as:

- Adding new device to Fabric.
- OS – Installation, Uninstallation
- Patch – Update, Remove,
- User Issues, Minor Bugs, Software Installation

This is an indicative list and not exhaustive.

12.5.3. Manpower Replacement Policy

The replacement of manpower by the bidder after deployment will be permitted (without penalty) under the following circumstances:

1. When the resource voluntarily leaves the organization by submitting a resignation to their current employer, and a copy of the resignation is marked to OCAC.
2. When the bidder withdraws the resource in accordance with its organizational policy due to non-performance or non-cooperation, aligning with DR-DC guidelines.
3. Verification of the resource profile, educational qualifications, and certifications concerning skills

and competence levels should be conducted jointly by the Consultant and OCAC before deployment.

4. No resource is allowed to be absent without prior permission from the designated authority.
5. Background verification may be carried out for selected resources to ensure the absence of any criminal history.

Note:

The manpower requirement provided in the RFP serves as an indicative minimum requirement for DR-DC. Bidders are expected to have a clear perspective on the necessary manpower to sustain the project and meet the required SLA.

Bidders are required to maintain additional resources to effectively address challenges related to leave, replacement, and any necessary changes, ensuring the seamless delivery of services.

12.5.4. Operations and Maintenance Management

The awarded bidder will be responsible for providing continuous operating and maintenance services, 24x7x365, for a duration of 5 years from the final acceptance test date. The service scope, aligned with the ITIL framework, should encompasses round-the-clock monitoring, maintenance, and management of the complete Disaster Recovery Centre infrastructure. This includes the provision of Helpdesk services, ensuring a minimum uptime efficiency of 99.982% for Odisha State DR-DC (DR-DC) and other managed facilities. The objective is to assure the operations team, System Integrators, and end-users meet the criteria for continuous 24x7 service. The focus is on realizing the full uptime potential, optimizing installed infrastructure, enhancing operational efficiency, and identifying opportunities for energy efficiency. This section provides guidance and a framework to drive best practices in the effective management and operations of the Odisha State ODR-DC (DR-DC).

Key Areas of Focus:

- Human Resource and Planning
- Policies and Procedures
- Maintenance Management
- Operations Monitoring
- Access Management
- Training and Development
- Reports
- Documentation
- Certification
- Automation of Services

Commissioning of System

i. The bidder should define the tests and processes to demonstrate the correct functionality of the supplied equipment, both individually and as an integrated system.

ii. System testing schedules, testing, and commissioning report formats, and the mechanism for report dissemination should be collaboratively developed by the Bidder and OCAC.

iii. Commissioning of the solution is deemed complete only after meeting the following conditions to the satisfaction of the OCAC:

1. Successful completion of Factory Acceptance Tests with the submission of necessary reports and certificates.
2. Delivery of all items under the proposed bill of materials at designated installation locations; short shipments will not be acceptable.
3. Installation and configuration of all solution components, including hardware, software, devices, accessories, etc., to the satisfaction of OCAC.
4. Certification of successful commissioning by OCAC; operations shall commence only after OCAC's approval.

Human Resource and Planning

Adequate staffing, with the right qualifications, is crucial for DR-DC to achieve long-term performance goals. In-house staff or vendor support must possess the necessary qualifications and experience to conduct maintenance activities and operate the Disaster Recovery Centre without impacting its functionality.

Requirements:

- **Organizational Structure:** Clearly outlines the DR-DC department structure and defines team responsibilities related to DR-DC operations.
- **DR-DC Team Escalation Matrix:** Specifies multiple user contacts to be notified in the event of critical issues or emergencies.

  Staff Qualifications: Ensures that the team assigned to handle the DR-DC is qualified, trained.

Policies and Procedures

An effective DR-DC management strategy necessitates documented and enforced policies and procedures. These guidelines prevent inconsistencies, reducing the risk of service interruptions or downtime.

Requirements:

- Disaster Recovery Centre User Manual
- Disaster Recovery Centre Instructions
- Emergency/Crisis Management Plan
- SOPs (Standard Operating Procedures)
- Health & Safety Procedures
- Change Management Procedures
- Access Procedures
- Maintenance Procedures

Maintenance Management

An effective maintenance program ensures optimal equipment condition, minimizing failures and preventing downtime. The program should include preventive and predictive maintenance, vendor support, failure analysis, life cycle tracking, and documentation.

Requirements:

- List of Equipment

- Specialized Vendor Details
- Service Level Agreements
- Planned Preventive Maintenance (PPM)
- Sequence of Operation
- Escalation Matrix or Emergency Call-out Matrix
- Service Evaluation
- Methodology and Risk Assessment
- Housekeeping Schedule
- Critical Spare Parts
- End-of-life study.
- Life Cycle study
- Predictive Maintenance
- Anticipation and Forecasting

Operations & Maintenance Monitoring

Continuous monitoring of network assets, both physical and virtual, is crucial for identifying vulnerabilities. Monitoring should cover missing patches, application changes, or configuration changes that may introduce exploitable vulnerabilities.

Requirements:

- Physical or Visual Inspection
- Online/Remote Monitoring
- Critical Alerts

Access Management

This guideline outlines the criteria for granting access to DR-DC, specifying different levels of access for individuals or groups. It includes Permit to Access, Permit to Work, Permit to Modify Equipment, No Objection Certificates, and Change Request Forms.

Training and Development

Proper training ensures the team understands policies, procedures, and unique requirements. Induction, ongoing training, and necessary knowledge transfer are essential for avoiding unplanned outages and responding effectively to events.

Requirements:

- DR-DC Induction
- DR-DC Trainings

Bidder shall provide all necessary training to OCAC officials and authorized team members for the successful functioning of the DR-DC operation and management.

Documentation

Documentation serves as a reference for operational knowledge and processes. It should be up to date, protected, and easily accessible.

Requirements:

- Asset List
- Licenses

- Operation Manuals
- Procedure Manuals
- Data Sheets
- Equipment Set Points
- Testing and Commissioning
- Warranty Certification

Reporting

Accurate, objective, and complete reporting is crucial for referencing. Reports include DR-DC Activity, Preventive Maintenance, Incident, KPI, and Service-related metrics.

Monthly Reports

Consolidated monthly reports include ICT infrastructure availability, SLA/non-conformance, issues/complaints, systems rebooted, backup and restoration log, changes in the DR-DC, uptime summary, maintenance logs, staff attendance, and spare parts inventory. Reports will be submitted in hard and soft copies to all stakeholders involved in the project.

Quarterly Reports

Consolidated and detailed component-wise reports on ICT infrastructure availability, bandwidth utilization resource utilization, and manpower availability must be submitted quarterly in hard and soft copies to all project stakeholders.

1. Component-wise IT infrastructure availability and resource utilization.
2. Consolidated SLA/(non)-conformance report.
3. Summary of component-wise DR-DC uptime.
4. Summary of changes in the DR-DC.
5. Log of preventive/scheduled maintenance undertaken.
6. Log of break-fix maintenance undertaken.
7. Details of manpower availability at the DR-DC.

Half-Yearly Reports

Consolidated component-wise reports on ICT infrastructure availability and resource utilization should be submitted in softcopy. Additionally, a DR-DC Security Audit Report, IT infrastructure Upgrade/Obsolescence Report, and another consolidated component-wise ICT infrastructure availability and resource utilization report should be submitted in hard Copy.

MIS Reports and Deliverables

The bidder is obligated to submit specified MIS reports regularly in a format determined by OCAC. The indicative list aligns with the reporting features outlined in the RFP. Reports should be provided to all project stakeholders, and hard Copy may be required upon OCAC's request.

Incident Reporting

Software License Violations:

OCAC will annually audit the IT infrastructure solution by a third-party, ensuring proper software versions and compliance.

1. The audit report will offer recommendations on infrastructure issues and obsolescence.
2. The audit covers IT infrastructure obsolescence, providing recommendations for upgrades and disposal plans.
3. A half-yearly security audit will assess security practices and vulnerability, rating them as Satisfactory, Requires Improvement, or Unsatisfactory.
4. Bidder support and cooperation are essential for these audits.
5. The bidder must implement audit recommendations within defined service levels.

Documentation:

1. The bidder shall submit documentation per OCAC's decision regarding format, media, and copies.
2. Documentation must follow ITIL standards and include project plans, OEM manuals, training materials, process documentation, installation and commissioning procedures, security practices report, and more.
3. All documents will be owned by OCAC.

Training – Information Security & BCP:

1. Technical training before Go-Live and operational training after Go-Live are essential. The contents should be documented and available to all attendees.
2. Training includes security awareness, practices, and operations for information security and BCP components.

Performance - Monitoring, Management, and Reporting

The proposed performance management system should integrate network, server, and database performance information and alarms, providing a unified reporting interface.

Constitution of the Team

1. The bidder shall provide adequate onsite support, administrators, and critical (L2 & above) onsite resources on its payroll.
2. Onsite resources for Network, Security, and technical support will work in shifts for 24x7x365 onsite operations.
3. Bidder shall maintain an attendance database and submit records as per OCAC's schedule.
4. Due diligence to ensure personnel trustworthiness is crucial.
5. A full-time Project In-charge with specified qualifications and experience will be appointed to oversee the overall project.

O & M Roles and Responsibilities

Responsibilities of the Bidder:

1. The Bidder shall prepare IT infrastructure solution architecture, diagrams, and plans, seeking approval from OCAC before installation.
2. Adherence to Change Management Procedures and OCAC's Information Security Policies is mandatory.
3. Ensure proper handover/takeover of documents and materials during personnel changes.
4. Proactively engage with vendors, third parties, and OEMs for equipment upgrades and maintenance.
5. Manage all aspects of Vendor Management.

Responsibilities of OCAC:

1. Provide timely approvals and signoffs for deliverables.
2. Direct and monitor Bidder activities as per RFP and validate service levels as per SLA.

Certification

Various operational standards must be followed, and the DR-DC should adhere to international standards provided by ISO. The following certifications are required:

- ISO/IEC 9001
- ISO/IEC 20000
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 22301

Automation of Services

DR-DC services should be automated through the building management system and incident management system for requesting and approving:

- Permit to Access
- Permit to Work
- Permit to Modify Equipment
- NOC
- Change Request
- Recording and alerting all DR-DC alerts related to critical equipment through SMS or Email to all concerned.

Handing Over Taking Over (HOTO) Plan

The selected SI will conduct a comprehensive analysis of the existing SDR-DC (AS-IS basis) in collaboration with the current DR-DCO, Project Consultants, Composite Team, OCAC, and other stakeholders. The HOTO plan involves a seamless transition of SDR-DC from the current DR-DCO to the selected bidder.

Key Points:

1. The transition period is a maximum of 90 days, with joint activities identified by the selected SI, current SDR-DC, and OCAC.
2. The SI will submit a site survey report, verifying inventory details and highlighting discrepancies.
3. The SI will undertake the takeover of equipment and operations from the current SDR-DC with due diligence.
4. OCAC will provide necessary documentation, communication matrices, entitlements, and other information for a smooth transition.
5. The selected SI will be provided with a detailed exit management plan submitted by the existing SI.
6. The existing SDR-DC will provide shadow support for 20 working days during the operational takeover.
7. The deliverable for this phase is the sign-off of the HOTO Report from OCAC and the submission of AMC documents to OCAC.

13. Annexures

13.1. Annexure 1: Proposal Covering Letter

To

The General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Sub: Request for Proposal (RFP) for Selection of System Integrator for " Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha"

Ref: <RFP Tender No>

Sir/Madam,

Having thoroughly reviewed the RFP, of which we duly acknowledge the receipt, we, the undersigned, express our commitment to delivering the highest quality goods and professional services in accordance with the requirements outlined in the RFP.

Enclosed herewith is our technical response, fulfilling the RFP requirements, constituting our comprehensive proposal. We assure that, upon acceptance, we will strictly adhere to the Project Timeline and Service Levels specified in the RFP for various activities.

Upon acceptance of our proposal, we commit to securing a performance bank guarantee, as per the format provided in the RFP document, from a Scheduled Commercial Bank in India, acceptable to OCAC. This guarantee will amount to 10% of the total price quoted in our financial proposal, ensuring the due performance of the contract.

We unconditionally accept all the terms and conditions set out in the RFP document and pledge to abide by this RFP response for a period of 180 days from the bid opening date. This commitment will remain binding until a formal contract is prepared and executed. This RFP response, along with your written acceptance in the notification of award, shall constitute a binding contract between us and OCAC.

We affirm that all information in this proposal, including exhibits, schedules, and other documents, is true, accurate, and complete. It encompasses all details necessary to ensure that the statements therein do not mislead OCAC in any aspect.

We acknowledge that OCAC is not obligated to accept the lowest or any RFP response received. We respect your absolute right to reject any or all products/services specified in the RFP response.

We hereby confirm our entitlement to act on behalf of our corporation/company/firm/organization and have the authority to sign this document, and any relevant documents required in this connection.

(Signature) (In the capacity of)

Having the Power of Attorney & duly authorized to sign the RFP Response for and on behalf of:
(Name and Address of Company) Seal/Stamp of Bidder Witness Signature:
Witness Name:
Witness Address:

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am …… of the ……, and that …… who signed the above Bid is authorized to bind the corporation by authority of its governing body.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)
Name
Designation
Place
Date

13.2. Annexure 2: Declaration of Acceptance of Terms & Conditions of RFP

To

The General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Sub - Declaration of Acceptance of Terms & Conditions of RFP of <Tender No>

Sir/Madam,

I have meticulously reviewed the Terms & Conditions stipulated in the RFP Document [OCAC/ /] concerning the RFP for the "Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha".

I affirm that all the provisions outlined in this RFP document, when read in conjunction with the proposal submitted by my Company, have been duly understood and accepted. I certify that I am an authorized signatory of my company and, therefore, have the competence to make this declaration. I further acknowledge that any interpretation made by the OCAC technical committee is considered final and binding on me.

Further, we <Bidder's Name> hereby declare that we have visited & surveyed the site and understood the entire requirement of the project. We have submitted our bid with all the knowledge and if any further requirement will arise during the SITC phase of this project, we will do the needful without any additional financial implications to OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name

Designation

Place

Date

13.3. Annexure 3: Format of Technical Proposal Document

RFP Ref. No.: OCAC/ Date:

To

The General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Subject: Submission of Technical Proposal for " Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha"

Ref: <RFP Tender No>

Dear Sir/Madam,

We, the undersigned, express our commitment to provide Systems Implementation solutions to OCAC Ltd in response to your Request for Proposal dated [insert date] and our Proposal. Our submission comprises this Technical Bid and the Financial Bid, submitted separately.

We affirm that all information and statements in this Technical Bid are accurate, and we acknowledge that any misrepresentation may result in our disqualification.

If our Proposal is accepted, we commit to initiating the Implementation services related to the assignment no later than the date indicated in the Data sheet.

We agree to adhere to all the terms and conditions outlined in the RFP document and confirm that the validity of our bid extends for 180 days, as specified in the RFP document.

Furthermore, we declare that we are not insolvent, in receivership, bankrupt, or undergoing winding up. Our affairs are not administered by a court or a judicial officer, our business activities have not been suspended, and we are not subject to legal proceedings for any of the reasons.

We acknowledge that OCAC is not obligated to accept any Proposal received.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name

Designation

Place

Date

13.4. Annexure 4: Forwarding Letter for Earnest Money Deposit

To

The General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Dear Sir/Madam,

Subject: **EMD submission for the RFP for** "**Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha**".

We, M/s <Bidder's Name>, having carefully read and examined in detail the RFP document for " **Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha",** published by OCAC, hereby submit EMD of Rs. <Amount>/- (Rupees <Amount in Words> Only) in the form of Bank Guarantee. The details are as under:

Name of Issuing Bank:

Bank Guarantee Number:

Amount:

Dated:

We, M/s <Bidder's Name>, have read and understood the clauses of the RFP document towards forfeiture of EMD.

Thank you,

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name:

Place:

Designation:

Date:

Encl: - Copy of Earnest Money Deposit

13.5. Annexure 5: Format for Furnishing Earnest Money Deposit

Whereas (hereinafter called the "tenderer") has submitted their offer dated for Selection of System Integrator for "Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha "hereinafter called the "RFP") against the purchaser's RFP enquiry No. OCAC/ /.

KNOW ALL MEN by these presents that *We* <Bank Name> of having our registered office at are bound unto (hereinafter called the "Purchaser) in the sum of for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this day of ,2021.

THE CONDITIONS OF THIS OBLIGATION ARE:

1. If the tenderer withdraws or amends, impairs, or derogates from the RFP in any respect within the period of validity of this RFP.
2. If the tenderer, having been notified of the acceptance of his RFP by the purchaser during the period of its validity:
    a. If the tender fails to furnish the Performance Security for the due performance of the contract.
    b. Fails or refuses to accept/execute the contract.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 180 days including the last date of RFP submission date/ RFP validity date, and any demand in respect thereof should reach the Bank no later than the above date.

(Signature of the authorized officer of the Bank)

Name and designation of the officer.

Seal, name & address of the Bank and address of the Branch.

13.6. Annexure 6: Company Profile of Bidder

Requirements	Details	Remarks
Name of the Company/Firm		
Date of Incorporation (Registration Number & Registering Authority)		
GST and PAN No.		
Legal Status of the Company in India & Nature of Business in India	Public Ltd Company/ Private / Partnership Firm	
Address of the Registered Head Office in India		
Date of Commencement of Business		
Address of the office in Odisha (if any)		
Active ISO/ SEI CMMI Level status (Enclosed Certificate)		
Details of the Contact Person	Name: Designation: E-mail id: Phone & Fax number:	
Details of the Contact Person to whom all references shall be made regarding this RFP	Name: Designation: E-mail id: Phone & Fax number:	
Website & -mail ID for any grievance		

(Seal & Signature of the Authorized signatory of the bidder)

Name:

Place:

Designation:

Date:

13.7. Annexure 7: Undertaking on Not Being Blacklisted

Undertaking on Not Being Blacklisted

This is to certify that to the best of my knowledge and based on the documents available << COMPANY NAME >> is not under a declaration of ineligibility for corrupt or fraudulent practices on the date of bid submission by any State Government, Central Government, Central Public Sector Undertaking (PSU), or autonomous body in India.

Company Secretary / Authorized Signatory Name of Signatory:

(Seal & Signature of the Authorized signatory of the bidder)
Name:
Place:
Designation:
Date:

13.8. Annexure 8: Undertaking of Service Level Compliance

To
The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Sub: Undertaking on Service Level Compliance < Bid Name>

Dear Sir/Madam,

1. I/We as Implementing Agency do hereby undertake that we shall monitor, maintain, and comply with the service levels stated in the RFP to provide quality service to OCAC.
2. However, if the proposed resources, Infrastructure, and ICT components are found to be insufficient in meeting the RFP and/or the service level requirements given by OCAC, then we will augment the same without any additional cost to OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)
Name:
Place:
Designation:
Date:

13.9. Annexure 9: Authorization Letters from all OEMs

List of components for which OEM MAF is required

S. No	Components
1	Diesel Generator with associated components
2	Modular UPS with associated components
3	Rack & PDU (all the racks)
4	Servers (Type I & II)
5	Storage solution
6	SAN Switches
7	Network Switches (Type I, II, III & IV)
8	Backup solution (Hardware and Software)
9	Virtualization Solution
10	DRM Tool
11	Tape Library
12	Endpoint Detection and Response
13	Next Gen Firewalls
14	DDoS
15	Link Load Balancer
16	Server Load Balancer with WAF
17	Observability Tool
18	Workstation

1. The Bidder must submit the bid specific MAF against the above components otherwise, the bid will not be considered for evaluation.
2. The specifications of the products and solutions proposed by the Bidder must comply with the specifications prescribed in the RFP.

Manufacturer Authorization Form (MAF) (On OEM's Letterhead)

To,
The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Reference: Supply of equipment/software/License for the project "" Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha", with ref no _____

Sir/Madam,

We, (name and address of the manufacturer) who are established and reputed manufacturers of _____having factories at_____(addresses of manufacturing locations) do hereby authorize M/s_____(name and address of the Bidder) to bid, negotiate and conclude the contract with you against the above-mentioned RFP for the above equipment manufactured by us.

Yours faithfully,

For and on behalf of M/s_____(Name of the manufacturer)

Signature
Name :
Designation:
Address :
Date:
Seal:

13.10. Annexure 10: OEM's Support Form

To,
The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Subject: RFP for Supply of equipment/software/License for the project "" Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha", with Ref No _____

Sir/Madam,

We__, (name and address of the manufacturer) who are established and reputed manufacturers of _____having factories at _____(addresses of manufacturing locations) do hereby assure that we would support our equipment/software/license and provide free software upgrade for a period of Five years during Operations and Maintenance, from the date of go-live of the project, through M/s _____(name and address of the Bidder) for the project **"" Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha",** or his successor. We would also adhere to the timelines as indicated in this RFP by closely working with the Bidder or his successor for a period of five years from the date of Go-Live. We abide by the commercials quoted by the Bidder towards AMC charges for five years from the date of supply and successful commissioning of equipment(s) i.e. Go-Live.

We confirm that the products quoted will not be end of life for the next seven years from the last date of submission of bids.

Yours faithfully,

For and on behalf of M/s_____(Name of the manufacturer)

Signature
Name :
Designation:
Address :
Date:
Seal:

13.11. Annexure 11: Declaration by OEM

To
The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Subject: RFP for Supply of equipment/software/License for the project "Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha", with Ref. No _____

Madam/Sir,

This is to certify that, we <OEM Name>, have issued the Manufacturing Authorization Form (MAF) to the bidder <Bidder's Name>, against the RFP No. XXXXXXXXXXXX, Date XX/XX/2024.
We hereby declare that the MAF is binding with the bidder and cannot be revoked by <OEM Name> at any point of time during the Bid Process and entire contract period.

<OEM Name>
<Authorised Signatory>
Name:
Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer.

13.12. Annexure 12: Technical specification compliance by OEM.

Minimum Criteria and Condition for OEM for Technical Specifications

The OEM for all the above-mentioned equipment's should be able to support the Warranty and Replacement services efficiently.

Please fill up compliance statement as per below format with Technical Proposal for all items as per technical specification mentioned in this RFP.

<< OEM Name >> << Table need to modify as per specification table>>

Device Name				
Make				
Model				
S No.	**System**	**Description**	**Compliance (Y/N)**	**Remarks**

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)
Name:
Place:
Designation:
Date:

13.13. Annexure 13: Statement of No Deviation from Specifications

To
General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Sir,

There are no technical deviations (null deviations) from the requirement specifications of tendered items and schedule of requirements. The entire work shall be performed as per your specifications and documents.

This is to certify that our proposed solution meets all the requirements of the RFP including but not limited to Scope of Work, stated Project Outcomes (including SLAs), Business Requirements and Functional Specifications/ Requirements.

We further certify that our proposed solution meets, is equivalent or better than the minimum technical specifications as given in the RFP.

We understand that the Bill of Quantity provided in the RFP is indicative, we confirm that we have undertaken our own assessment to finalize the components and quantity.

In case any item of hardware or software is found non-compliant at any stage during project implementation, it would be replaced with a fully compliant product/solution at no additional cost to OCAC. In case of non-adherence of this activity, OCAC reserves the right to cancel the contract, in case the said Contract is awarded to us by OCAC.

We further confirm that our commercial proposal is for the entire scope of work, comprising all required components and our obligations, for meeting the scope of work.

Thank you,

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)
Name:
Place:
Designation:
Date:

13.14. Annexure 14: Warranty Certificate Undertaking

To

The General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Subject: Supply of equipment/software/License for the project **"Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha"**.

Sir/Madam,

We warrant that the equipment(s) supplied under the contract would be newly manufactured, free from all encumbrances, defects and faults in material or workmanship or manufacture, shall be of the highest grade and quality, shall be consistent with the established and generally accepted standards for materials of the type ordered, shall be in full conformity with the specifications, drawings of samples, if any, and shall operate as designed. We shall be fully responsible for its efficient and effective operation. We also warrant that the services provided under the contract shall be as per the Service Level Agreement (SLA) with GoO/OCAC.

The obligations under the warranty expressed above shall include all costs relating to labour, spares, maintenance (preventive as well as unscheduled), and transport charges from site to manufacturer's works / service facilities and back for repair or modification or replacement at site of the equipment or any part of the equipment, which under normal care and proper use and maintenance proves defective in design, material or workmanship or fails to operate effectively and efficiently or conform to the specifications and for which notice is promptly given by OCAC to us (Bidder). We shall provide on- site support for all the equipment and services supplied hereunder during the period of this warranty (5 years after acceptance for equipment (5 years for the date of go-live) and entire service period for services).
Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name:
Place:
Designation:
Date:

13.15. Annexure 15: Bidder's Annual Turnover

Date:

This is to certify that we M/s---------- are the statutory Auditors of M/s---------- and that the below mentioned calculations are true as per the Audited Financial Statements of M/s- -for the below mentioned years.

S No.	Annual Sales Turnover Calculation	2022-23	2023-24	2024-25
1	Total Sales as per the P/L A/c (A)			
2	Less: Custom and/or Excise Duty if included In total Sales as per P/L in Total Sales as per P/L A/C (B)			
3	Less: Sales Tax if included in Total Sales as per P/L A/c (C)			
4	Less: Any other statutory taxes if included in total Sales as per P/L A/C (D)			
5	Less: Any other income from sources other than the normal business source if included in Total Sales as per P/L A/c (E)			
6	Annual Turnover (F) ==(A)-(B)-(C)-(D)-(E)			

The Bidder is required to enclose the audit financial statements for these three years.

Company Secretary / Statutory Auditor /CA Name of Signatory:
Bidder Company Name:
Date:
Place:

13.16. Annexure 16: Format for Unpriced Bill of Material

S. No.	Product Detail (Parent & it's Child)	Part Code (Parent and Child)	Make & model	UoM	Qty.	Remarks (If Any)
1.						
2.						
3.						
…						

Attach detailed specifications and provide reference number in remarks column.

Thanking you, Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name:

Place

Designation:

Date:

13.17. Annexure 17: Format for Performance for Bank Guarantee (PBG)

To,
The General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Whereas << name of the agency and address >> (hereinafter called “the Bidder”) has undertaken, in pursuance of contract no. << insert contract no. >> dated. <<Insert date >> to provide Implementation services for << name of the assignment >> to OCAC (hereinafter called “the beneficiary”)
And whereas it has been stipulated by in the said contract that the Bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract.
And whereas we, << name of the bank >> a banking company incorporated and having its head /Registered office at << address of the registered office >> and having one of its offices at << address of the local office >>have agreed to give the supplier such a bank guarantee.
Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Rs.<< insert value >> (Rupees << insert value in words >> only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs.<< insert value >> (Rupees << insert value in words >> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein. We hereby waive the necessity of your demanding the said debt from the Bidder before presenting us with the demand. We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you, and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition, or modification.
This Guarantee shall be valid until << Insert Date >>) Not withstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs<< insert value >> (rupees << insert value in words >> only).
II. This bank guarantee shall be valid up to << insert expiry date >>)
III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before << insert expiry date >>) failing which our liability under the guarantee will automatically cease.

Authorized Signatory of the Bank) Seal
Date

13.18. Annexure 18: Format for providing CV of Key Personnel

To

The General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Subject: CV format Of Key personnels

RFP Ref. No.: OCAC/ /

The bidder shall provide the summary table of details of the manpower that will be deployed on this project during the implementation.

Table A

S No	Type of Resource	Name of Resource	Key Responsibilities	Highest Academic Qualifications and Certifications (e.g. PMP/CDCP /ATD/CCNA/ITIL)	Years of Relevant Experience
1	Project Manager				
2	---				
3	---				
4	---				
5	---				
6	Others				
…					

Table B

Sl. No.	Particulars	Details	Supporting document
1.	Key resource / non-key resource		
2.	Name of the Personal		
3.	Current Designation/Job title		
4.	Current job responsibilities		
5.	Proposed Role in this project		
6.	Total experience and relevant experience (in years)		
7.	Number of years with the organization and date of joining the firm		
8.	Whether resource is engaged by the firm in its own payrolls	YES/NO	
9.	Summary of Professional / Domain Experience		
10.	Date of Birth		
11.	Academic Qualifications: • Degree • Academic institution graduated from • Year of graduation Specialization (if any)		Attach certificate of highest qualification
	• Key achievements and other relevant information (if any)		
12.	Professional Certifications/ Training		Attach relevant certificates
13.	Membership of Professional Associations		
14.	Employment Record*		
15.	• Details of similar project handled & the role assigned • Prior project experience • Project name • Customer • Key project features in brief • Location of the project • Designation • Role • Responsibilities and activities Duration of the project		
16.	Detailed tasks Proposed to be assigned	Work already undertaken that best illustrates capability to handle the tasks assigned**	
17.	Signature of the representative		

I hereby declare that the above-mentioned resource would be available during the project phase of this RFP

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name:

Place:

Designation:

Date

Note: Table B should be furnished for all the proposed resources

13.19. Annexure 19: Format of Commercial Proposal Document

(Not to be provided in the Pre-Qualification & Technical Bid Document)

RFP Ref. No.: OCAC/ / Date:

Format for reporting commercials and mandatory letters that needs to be part of the commercial proposal document. Breakdown of cost mentioned, cost of each component, operating cost, employee cost, cost of operations and management, any other cost which the Bidder feels.

To
General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square,
Near Planetarium, P.O. – RRL,
Bhubaneswar, Odisha, Pin-751013

Subject: Submission of Commercial proposal for "**"Selection of System Integrator (SI) for Setting up and Managing the Disaster Recovery Centre cum Data Centre Infrastructure at Keonjhar, Odisha"**

We, the undersigned Bidder, having read and examined in detail the RFP documents for "selection of System Integrator (SI) for Selection of System Integrator for Setting the Disaster Recovery Centre at Keonjhar **"**. I / we do hereby propose to provide services as specified in the RFP documents number **OCAC/__/__ Dated _/_/**

1. PRICE PROPOSAL AND VALIDITY

All the prices mentioned in our RFP are in accordance with the terms specified in the RFP documents. All the prices and other terms and conditions of this RFP are valid for a period of 180 days as desired in the RFP

We hereby confirm that our RFP prices include all taxes. However, all the taxes are quoted separately under relevant sections.

We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax in altercated under the law, we shall pay the same.

2. UNIT RATES

We have indicated in the relevant schedules enclosed the unit rates for the purpose of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. DEVIATIONS

We declare that all the services should be performed strictly in accordance with the RFP documents except for the variations and deviations, all of which have been detailed out exhaustively in the following statement, irrespective of whatever has been stated to the contrary anywhere else in our proposal.

Further, we agree that additional conditions, if any, found in the RFP documents, other than those stated in the deviation schedule, shall not be given effect to.

4. RFP PRICING

We further confirm that the prices stated in our proposal are in accordance with your Instruction to Bidders included in RFP documents.

5. QUALIFYING DATA

We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our RFP, we agree to furnish the same in time to your satisfaction.

6. PROPOSAL PRICE

We declare that our Proposal Price is for the entire scope of the work as specified in the Schedule of Requirements and RFP documents.

(A) Non - IT Infrastructure							
S. No	**Components**	**UOM (a)**	**Qty (b)**	**Unit Price in INR (c)**	**Applicable GST in Percentage (d)**	**Total Unit Price exclusive of GST (e)= (b)*(c)**	**Total Unit Cost in INR with GST (f)=(e)+((e)*(d))**
1	Interior Works	Lot	1				
2	Structural Works	Lot	1				
3	Transformer with associated components (750kVA)	Nos	2				
4	Diesel Generator with associated components (500kVA)	Nos	3				
5	Electrical Works - Electrical Panels, DG Sync Panel, Incomer / Outgoing cabling, PDUs, Earth Pits, Sockets, HSD Tanks, HSD Electrical panel, and wiring	Lot	1				
6	Modular UPS – IT with associated components (400kVA)	Nos	2				
7	UPS non-IT with associated components (40kVA)	Nos	2				
8	Precision Air Conditioner (40 TR)	Nos	3				
10	VRV	Lot	1				
11	Fire Detection	Lot	1				
12	Fire Suppression	Lot	1				

13	Security & Surveillance	Lot	1				
14	Rodent Repellent	Lot	1				
15	Access Control System	Lot	1				
16	Water Leak Detection System	Lot	1				
17	Building Management System	Lot	1				
18	Rack & PDU (all the racks)	Lot	1				
19	Structural Cabling (all the racks)	Lot	1				
20	Passive items (Cat6 cables, Patch panels, IO, Patch Cord etc.,)	Lot	1				
21	Civil Work if required	Lot	1				
22	Any other items	Lot	1				
TOTAL COST (A)							

(B) IT Infrastructure

S. No	Components	UOM (a)	Qty (b)	Unit Price in INR (c)	Applicable GST in Percentage (d)	Total Unit Price exclusive of GST (e)= (b)*(c)	Total Unit Cost in INR with GST (f)=(e)+((e)*(d))
1	Server Type-A	Nos	12				
2	Server Type-B	Nos	2				
3	STORAGE (2 PiB Usable)	Nos	1				
4	SAN SWITCH	Nos	2				
5	SWITCH TYPE 1	Nos	2				
6	SWITCH TYPE 2	Nos	4				
7	SWITCH TYPE 3	Nos	4				
8	SWITCH TYPE 4	Nos	2				
9	BACKUP APPLIANCE	Nos	1				
10	BACKUP SOFTWARE	Nos	1				
11	SERVER - BACKUP & UTILITY	Nos	1				
12	VIRTUALIZATION	Nos	1				
13	DB -MS-SQL – (4C Lic.)	Nos	4				
14	OS - Windows	Lot	1				
15	DRM Tool (30 VM's)	Lot	1				
16	Tape Library	No	1				
17	OS-Linux	Lot	1				

18	Endpoint Detection and Response	Nos	250				
19	NGFW - Internal	Nos	2				
20	NGFW - External	Nos	2				
21	DDoS	Nos	2				
22	Link Load Balancer	Nos	2				
23	Server Load Balancer with WAP	Nos	2				
24	Observability Tool	Nos	1				
25	Workstation	Nos	6				
26	IP KVM Switch with Display (48 - Ports)	Lot	1				
27	Printer	Nos	2				
28	Any other items	Lot	1				
TOTAL COST (B)							
C) OTHER COST							
1	One Time Implementation (IT & Non-IT)	Lot	1				
TOTAL COST (C)							

D) SUPPORT SERVICES								
1. SUPPORT SERVICES				Y1	Y2	Y3	Y4	Y5
1.1	AMC Support (Non-IT)	Lot	1					
1.2	AMC Support (IT)	Lot	1					
TOTAL COST (D)								
E) RESOURCE REQUIREMENTS								
1	Project Manager	Nos	1					
2	Storage Administrator	Nos	2					
3	Network Administrator	Nos	2					
4	Cloud Administrator	Nos	2					
5	Security Administrator	Nos	1					
6	Database Administrator	Nos	1					
7	System Administrator	Nos	2					
8	Helpdesk Support	Nos	2					
9	Datacentre facility engineer	Nos	3					
TOTAL COST (E)								

Implementation and Maintenance cost (F = A+B+C+D)	
GRAND TOTAL G = E + F	

Thank you,

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name:

Place:

Designation:

Date:

13.20. Annexure 20: Undertaking on Exit Management and Transition

To

General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Sub: Undertaking on Exit Management and Transition

Ref: <RFP No>

Dear Sir/Madam,

I/We hereby undertake that at the time of completion of our engagement with OCAC, either at the End of Contract or termination of Contract before planned Contract Period for any reason, we shall successfully carry out the exit management and transition of this Project to OCAC or to an agency identified by OCAC to the satisfaction of OCAC. I/We further undertake to complete the following as part of the Exit management and transition:

a. We undertake to complete the updating of all Project documents and other artefacts and handover the same to OCAC before transition.

b. We undertake to design standard operating procedures to manage the system (including application and IT systems), document the same and train OCAC personnel on the same.

c. If OCAC decides to take over the operations and maintenance of the Project on its own or identifies or selects any other agency for providing operations & maintenance services on this Project, then we shall provide necessary handholding and transition support, which shall include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the ICT components , conducting Training sessions etc.

I/We also understand that Exit management and transition will be considered complete based on approval from OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Name:

Place:

Designation:

Date

13.21. Annexure 21: Undertaking on Technical Resource in the organization

To

The General Manager, OCAC,
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar 751013

Subject: HR Declaration on number of technical employees in India
Ref: <RFP No>

Dear Sir/Madam,

We hereby declare that <Company Name>has <No. of Technical Resource> technical employees on its payroll in India as on <date of signature>.

SL. No	Name of the Resource	Highest Qualification and certification (Certificate copy to enclosed)

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)
Name:
Place:
Designation:
Date

13.22. Annexure 22: Integrity Pact

INTEGRITY PACT

This pre-contract agreement (hereinafter called the "Integrity Pact" or "Pact") is made on <<day>> of <<month, year>>, between, on one hand, the President of India acting through <designation and department> Purchaser (hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part

AND

M/s <<bidder's legal entity >> represented by <<name and designation>> (hereinafter called the "BIDDER/Seller", which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to engage the Managed Service Provider (MSP) for implementation and operations management of the Project and the BIDDER is willing to offer/has offered the services and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Ministry/Department of the Government of India performing its functions on behalf of the President of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent, and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:-

Enabling the BUYER to obtain the desired services at a competitive price in conformity with the defined specification by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organisation or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will, during the pre-contract stage, treat all the BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

Commitments of the BIDDER

3 The BIDDER commits itself to take all the measures necessary to prevent corrupt practices, unfair means, and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following: -

3.1. The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour or any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any advantage the bidding, evaluation, contracting and implementation of the contract.

3.2. The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or dis-favour to any person in relation to the contract or any other contract with the Government.

3.3. BIDDER shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.4. The BIDDER further confirms and declares to the BUYER that the BIDDER has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.5. The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to, or intends to

make to officials of the BUYER or their family members, agents, brokers, or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

3.6. The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness, and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.7. The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means, and illegal activities.

3.8. The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals, and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.9. The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.10. The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.11. If the BIDDER who is involved in the bid process or any employee of such BIDDER or any person acting on behalf of such BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of BUYER who is involved in the bid process has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender.

3.12. The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

For the purposes of clauses 3.11 & 3.12, the listed words shall have the ascribed meanings as follows:

i) "Employee of such BIDDER or any person acting on behalf of such BIDDER" means only those persons acting on behalf of such Bidder who are involved in the bid process / Project.

ii) "officers/employee of the BUYER", means only those persons who are involved in the bid process / Project.

iii) "Financial interest/stake in the BIDDER's firm" excludes investment in securities of listed companies".

4. <u>Previous Transgression</u>

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5. <u>Earnest Money (EMD)</u>

5.1 The Bidder's EMD of Rs. 4 Cr. deposited along with the bid shall remain valid till the submission of performance guarantee by the BIDDER.

5.2 In case of the successful BIDDER, a clause would also be incorporated in the Performance Bank Guarantee that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.3 Within 15 days of the receipt of notification of award from the employer, the successful Bidder shall furnish the performance security equal to <10 per cent> of the value of contract from a commercial bank in accordance with the conditions of the Agreement.

5.4 Performance security should remain valid from date of execution of Contract to the expiry of 60 days after the date of completion of all contractual obligations including warranty obligations.

5.5 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/ Performance Security for the period of its currency.

6. <u>Sanctions for Violations</u>

6.1 Any breach of the aforesaid provisions by the BIDDER or anyone employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle BUYER to take all or any one of the following actions, wherever required:

i) To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

ii) The Earnest Money Deposit (in pre-contract stage) and/or Performa Security (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be require assigning any reason, therefore.

iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing prime lending rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding payment could also be utilised to recover the aforesaid sum and interest

v) To encase the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments already made by the BUYER, along with interest.

vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money (s) due to the BIDDER.

vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the BUYER.

viii) To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.

x) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1 to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fall Clause

7.1 The BIDDER undertakes that under similar buying conditions, it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or subsystems was so supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 Shri <Name> has been appointed as Independent External Monitor (hereinafter referred to as Monitor) for overseeing and implementation of the Pre-Contract Integrity Pact for procurement of services in the <Purchaser's entity>. His contact details are as under:

<Name>

<Address>

<Contact details>

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, the Model will inform the Authority designated by the BUYER.

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request, and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

8.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is New Delhi.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend up to <X years> or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER, including warranty period, whichever is later. In case Bidder is unsuccessful, this Integrity Pact shall expire after six months from the date of signing of the contract.

12.2 Should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The parties hereby sign this Integrity Pact at _____ on _____

Buyer	Bidder
Name of The Officer:	Name Of the Officer:
Designation:	Designation:
Department:	Department:

WITNESS	WITNESS
1.	1.
2.	2.

* Provisions of these clauses would need to be amended / deleted in line with the policy of the BUYER in regard to involvement of Indian agents for foreign suppliers.

Company Secretary / Authorized Signatory Name of Signatory:

(Seal & Signature of the Authorized signatory of the bidder)
Name:
Place:
Designation:
Date:

13.23. Annexure-23: Project Citation

1.	Project Name	
2.	Value of Contract/Work order (In INR)	
3.	Name Of the Client	
4.	Contact Person of the client with Address, phone, and email	
5.	Project Duration	
6.	Start Date and Completion date	
7.	Status of the project (completed / ongoing)	
8.	Narrative description of the project with scope	
9.	List of Services provided by your company	
10	Document attached (Contract document / FAT/ MSA etc.)	

Note:

1) Project Citation should be provided for all the projects
2) OCAC reserves the right to do a background check of the cited projects during evaluation phase.