Request for Proposal (RFP) for selection of System Integrator (SI) for IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)

RFP ENQ No. – OCAC-NEGP-INFRA-008-2018-24037

Odisha Computer Application Centre (OCAC)

(Technical Directorate of E&IT Department, Government of Odisha)

OCAC Tower, Acharya Vihar, Bhubaneswar, Odisha.

1 Contents

1. Invitation for Bids

1.1. Important Dates

Sl. No.	Activity	Timeline
1	Release of RFP	01/03/2024 at 05:00 PM onwards
2	Last date & time for submission of pre-bid queries	11/03/2024 by 03: 00 PM
3	Date & time of pre-bid conference	12/03/2024 at 04: 30 PM
4	Date of Corrigendum, if any	15/03/2024 by 05: 00 PM
5	Last date for submission of Bids on e-Tender website	27/03/2024 by 03: 00 PM
6	Date of opening of pre-qualification bids	27/03/2024 at 04: 00 PM
7	Date of opening of Technical Bids	To be informed
8	Date of opening of Commercial Bids	To be informed

1.2. Disclaimer

The information contained in this RFP or subsequently provided to bidders, whether verbally or in documentary or any other form 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. This RFP is not an agreement and is neither an offer nor invitation by OCAC to the prospective bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their bid pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at byOCAC in relation to extension of OSDC. Such assumptions, assessments and statements do 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 readsor 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. 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 incurredor 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.OCAC may in its absolute discretion, but without being under any obligation to do so, update, amendor 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, as the case may be, 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 personincluding 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 arisefrom or be incurred or suffered on account of anything contained in this RFP or otherwise, includingthe 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 arisingin 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 remainwith 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.

2. General Instructions to Bidders

I. While every effort has been made to provide comprehensive and accurate background information, requirements, and specifications, Bidders must form their own conclusions about the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.

II. All information to be supplied by Bidders will be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

III. A bidder with solutions developed in an entity incorporated in a country sharing a land boundary with India cannot participate in this bid.

IV. Sub-contracting to be allowed as per State ICT Policy 2014 clause 5.5.2 where it is mandated that the successful bidder must associate a local enterprise, who has not been debarred / blacklisted by any State Government.

V. No commitment of any kind, contractual or otherwise, shall exist unless and until a formal written contract has been executed by or on behalf of OCAC with the bidder. OCAC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of OCAC.

VI. This RFP supersedes and replaces any previous public documentation & communications in this regard and bidders should place no reliance on such communications.

2.1. Bid Invitation

Odisha Computer Application Centre invites offer/proposal from interested bidders for “Installation, Commissioning, Integration and Operation & Maintenance of IT infrastructurefor Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar” for a period of five (5) years from date of acceptance of work order. This RFP document is being published on web Portal “https://www.ocac.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 ofits 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 witha 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. 25,000/- + 12% GST in the form of Demand Draft 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.

2.2. Factsheet

Proposal inviting agency	**Odisha Computer Application Centre**
Start date of Uploading document	01/03/2024 at 05:00 PM
Non Refundable RFP Cost	Rs. 25,000/- (Twenty Five Thousand only) exclusive of 12% GST in the form of DD/ Bankers Cheque in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India
The contact information	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, www.enivida.odisha.gov.in
Last date & time for submission of pre-bid queries	11/03/2024 by 03: 00 PM
Date & time of pre-bid conference	12/03/2024 at 04: 30 PM
Issue of Corrigendum (if Any)	15/03/2024 by 05: 00 PM
Earnest Money Deposit - (EMD)	Rs.2,00,00,000/- (Two Crore only) in form of Bank Guarantee in the prescribed format in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India.
Last Date and Time for Submission of Bid Document	27/03/2024 by 03: 00 PM
Opening of Pre-Qualification Bid	27/03/2024 at 04: 00 PM
Opening of General cum Technical Presentation by the qualified bidder.	Will be intimated later
Opening of Commercial Bids	Will be intimated later
Bid validity	Bid must remain valid up to 180 (One Hundred & Eighty) days from the actual date of submission of bid.
Language of the proposal	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.
Proposal currency	Bidder shall be quote prices in Indian Rupees (INR) and will receive payment is Indian Rupees only
Address for Correspondence and Clarifications	**General Manager, OCAC,** **Odisha Computer Application Centre**, **N1/ 7D, Acharya Vihar Square, Near Planetarium,** **P.O. – RRL, Bhubaneswar 751013Ph. - 0674-2582850/ 2588064 Website: www.ocac.in** **Project Manager, OSDC** **osdc@ocac.in & pm.osdc@odisha.gov.in**

Please visit web site "www.ocac.in, www.odisha.gov.in, www.enivida.odisha.gov.in" for complete detail. The Bidders are advised to submit the bids well in advance of the deadline as OCAC will not be responsible for non-submission of the bids because of any problems whatsoever.

2.3. Acronyms

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

Sr. No.	Abbreviations	Description/ Definitions
1	OCAC	Odisha Computer Application Centre
2	OSDC	Odisha State Data Centre
3	OSDC 2.0 /ODESSEY	Odisha State Data Centre 2.0
4	BOM	Bill of Material
5	BOQ	Bill of Quantity
6	BTA	Business Transaction Activity
7	CAPEX	Capital Expenditure
8	Cr.	Crores
9	DaaS	Database as a Service
10	DC	Data Centre
11	DOT	Department of Telecom
12	DPR	Detailed Project Report
13	EMS	Enterprise Management System
14	FAT	Final Acceptance Test
15	FTP	File Transfer Protocol
16	G2B	Government to Business
17	G2C	Government to Citizens
18	G2G	Government to Government
19	HLD	High Level Design
20	HPC	High Performance Computing
21	IaaS	Infrastructure as a Service
22	IP	Internet Protocol
23	IPS	Intrusion Prevention System
24	ISO	International Organization for Standardization
25	ISP	Internet Service Provider
26	IT	Information Technology
27	IOT	Internet over Things
28	ITSM	IT Service Management
29	LAN	Local Area Network
30	MeitY	Ministry of Electronics and Information Technology
31	MPLS	Multiprotocol Label Switching

Sr. No.	Abbreviations	Description/ Definitions
32	NGFW	Next Generation Firewall
33	NMS	Network Management Server
34	NOC	Network Operations Centre
35	O&M	Operations and Maintenance
36	OEM	Original Equipment Manufacturer
37	OPEX	Operational Expenditure
38	PaaS	Platform as a Service
39	POE	Power over Ethernet
40	POI	Point of Interconnect
41	QOS	Quality of Services
42	SAN	Storage Area Network
43	SaaS	Software as a Service
44	SDC	State Data Centre
45	SDN	Software Define Network
46	SIEM	Security Information and Event Management
47	SWAN	State Wide Area Network
48	STP	Spanning Tree Protocol
49	TCP	Transmission Control Protocol
50	TCV	Total Contract Value
51	GoO	Government Of Odisha
52	UPS	Uninterrupted Power Supply
53	VRF	Virtual Routing & Forwarding
54	WAN	Wide Area Network

3. Project Objective & Brief Scope of Work

3.1. About OCAC

The Odisha Computer Application Centre (OCAC), 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 center 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.

3.2. 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 the majority 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.

3.3. Project Objective

The State Data Centre (SDC) stands as a crucial pillar supporting e-Government initiatives, aiming to deliver citizen services with enhanced reliability, availability, and serviceability. It plays a pivotal role in providing improved operations and management control while minimizing the overall costs associated with Data Management, IT Management, Deployment, and related expenditures.

As outlined by the National eGovernance Plan (NeGP), State Data Centres form one of the three essential infrastructure pillars designed to enable web-enabled, anytime, anywhere access. The primary objective of State Data Centres is to furnish a common enabling infrastructure for states, addressing their e-governance application hosting requirements across the entire state government and its departments. Operational since October 2011, the SDC hosts services, applications, and infrastructure, facilitating the efficient electronic delivery of Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C) services.

The Ministry of Information Technology and Electronics (MeitY), along with the Government of Odisha (GoO), served as key stakeholders in implementing various Mission Mode Projects under NeGP. A dedicated Composite Team, comprising officers from the Odisha Computer Application Centre (OCAC) and the National Informatics Centre (NIC), has been established to provide techno-administrative support for the overall operations, management, and hosting of various departmental applications at the SDC.

In its commitment to extending the success of computerization, the Government of Odisha, in collaboration with its nodal agency, established the SDC to host departmental applications. The existing SDC, located at the OCAC building and built in 2011, spans approximately 4000 sq. ft., including a server farm area of around 1500 sq. ft. This infrastructure enables on-premises hosting of government applications. Currently, over 500 applications are hosted under a virtualized/cloud environment (Hyper-V/vCloud suite) within the SDC. Future Business Continuity Planning (BCP) and Disaster Recovery (DR) for applications hosted at the SDC are envisioned to be provisioned at an alternate site.

OCAC is extending and upgrading the existing State Data Centre (SDC) with the construction of a dedicated Tier III standard facility on the first floor of OCAC Towers. This new space, known as ODYSSEY (Odisha State Data Centre 2.0), within the same campus, is designed to address the evolving needs of the SDC, which has been operational for over eleven years.

The current technology infrastructure in the Data Centre requires refreshing to stay current with security standards and industry best practices. Proposals are invited from prospective bidders for the design, supply, installation, configuration, integration, operation and maintenance of the IT infrastructure of the proposed Tier-III ODYSSEY.

Given that many components of the existing SDC are currently in a state of extended support by the respective Original Equipment Manufacturers (OEM), immediate replacement of these devices is crucial for the smooth operation of OSDC. The State user departments are experiencing a significant demand for hosting their applications, necessitating the upgrade.

ODYSSEY (Odisha State Data Centre 2.0) aims to host applications from various user departments of the State and PSU's on a shared infrastructure. This approach promotes ease of integration and efficient management, ensuring optimal utilization of computing resources and the supporting connectivity infrastructure (OSWAN). ODYSSEY will have the capacity to host and co-locate systems such as Cloud, Web Servers, Application Servers, Database Servers, SAN, and NAS, utilizing centralized computing power. The IT infrastructure is designed to support multiple applications with high availability, scalability, reliability, portability, and a centralized authentication system for users to access their respective systems.

3.4. Brief Scope of Work

The expansion of the Odisha State Data Centre aims to meet the increasing demand from user departments for hosting their applications. Additionally, it strives to establish a highly secure, flexible, automated, and managed cloud service environment that deploys the latest industry computing infrastructure. This initiative is geared towards ensuring the security, scalability, and availability of user department applications.

There is a recognized need for strategic infrastructure that facilitates high availability, quick scalability, efficient management and optimized resource utilization. To address this, OCAC is proposing the establishment of ODYSSEY, a Tier-III data centre with high availability. This facility will grant government offices access to servers, storage, databases and a comprehensive set of application services over the Internet. The primary objectives include enhancing operations and management control and minimizing the overall costs associated with Data Management, IT Management, Deployment and related expenses.

ODYSSEY aims to unify virtual and physical infrastructure, incorporating cloud and legacy systems. It will possess the capability to support containers, bare metal, and virtualized workloads, treating compute, storage, and network devices as flexible resource pools. The goal is seamless integration, eliminating fragmented silos and ensuring that various technologies fit into a cohesive picture suitable for OCAC, the E & IT Department, and any user line department of the State.

Flexibility and programmability are central to ODYSSEY, allowing for the composition and re-composition of resources based on workload requirements or application needs. The infrastructure should support workload elasticity and agility, accommodating diverse requirements such as large storage, high network bandwidth or enhanced compute performance. Capacity planning and scalability are critical considerations in the overall systems engineering of ODYSSEY.

The transformation of ODYSSEY must be prepared for both composable and hyper-converged workloads, allowing incremental additions of hyper-converged solutions as needs arise. The bidder is expected to undertake the comprehensive scope of work for the Supply, Installation, Testing, Commissioning, Integration & Operations, and Maintenance of ODYSSEY IT Infra in Bhubaneswar. The selected bidder is required to ensure an uptime exceeding 99.982% quarterly for five years post-Go-Live.

The scope of work encompasses various schedules, including the supply and installation of IT infrastructure, migration of selected applications, acceptance tests, and ongoing operations and maintenance services for the complete IT infrastructure at ODYSSEY in OCAC Towers, Bhubaneswar. Bidders are encouraged to submit proposals for each phase or schedule in the technical bid for comprehensive evaluation purposes. Any additional requirements deemed essential for project completion may be brought to the notice of the authority during the pre-bid meeting.

The comprehensive Scope of Work (SoW) for the selected bidder through this RFP for the IT infrastructure encompasses, but is not limited to, the following:

3.4.1.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.

3.4.2.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 & SDN controller.

3.4.3.Storage Area Network (SAN):

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

3.4.4.Security Infrastructure:

- Supply, installation, configuration, testing, and commissioning of Security infrastructure, including D-DOS protection, Next Generation Firewalls, Anti-APT solution, WAF Solution and Network-based Intrusion Prevention Services (NIPS) solution.
- Create different PODs, as required by OSDC Team.

3.4.5.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-premise service implementation for the Orchestration layer.

3.4.6. Additional Security Measures:

Supply, installation, configuration, testing, and commissioning of Antivirus, Host Intrusion Prevention System (HIPS), On-Premise Virtual Machine (VM) based solutions and an Enterprise Management System. Implementation of single management portal for all IT security infrastructure to be deployed in ODESSEY. All the management of IT security infrastructure to be operated through this portal.

The proposed solution should have out of the box support for automatic baselining wherein the solution can automatically learn the behaviour of monitored applications and set baseline thresholds automatically for all the monitored metrics, including:

i. Application metrics
ii. Server metrics
iii. End User Metrics
iv. Custom Metrics
v. Business Metrics
vi. Database Metrics.

The solution must also provide an option of fixed as well as rolling time periods to calculate these thresholds.

The proposed solution should provide an option to drill down directly from any problematic transaction to:

i. the server instance which was executing that transaction and provide visibility into health of the server and other transactions getting executed in that node
ii. related DB instance in-context with the queries that are being executed
iii. in-context OS level metrics
iv. correlated application logs from available log files

The proposed solution should provide contextual monitoring of OS level metrics and provide auto correlation to the application performance. The server OS level monitoring should include general server visibility, process, volume and network metrics. There should be seamless correlation between server and application metrics through UI on the same screen without having to switch UIs.

The proposed solution must have a robust alert and respond engine that leverages multiple data inputs into analysis (app performance data, machine data, analytics data and user provided data), uses Boolean logic to combine multiple conditions through AND / OR logic, has capability to disable rule evaluation temporarily for predetermined maintenance windows, can trigger alerts or notifications when rules are violated (email, SMS or custom), can utilize complex logic to combine different metrics into one trigger/alert.

This SoW is designed to ensure the seamless integration and operation of the IT infrastructure, providing a robust foundation for the client's diverse needs. The selected bidder is expected to execute these tasks with precision, meeting industry standards and best practices throughout the supply, installation, testing, and commissioning phases of the project.

3.5. Capabilities of Software Defined Cloud-Enabled Data Centre:

- Software-defined compute, storage, network and security.
- Unified life cycle management for the entire cloud solution with enterprise-class support.
- Future-proof to embrace technology changes and innovation.
- Enterprise-grade OEM-supported, industry-leading Private Cloud Landscape with cross-platform virtualization management capabilities.
- Open Source-based framework for cloud deployment.
- Complete agent-less automation with life cycle management.
- Single and unified run-time environment.
- Scalability to IaaS, PaaS, and SaaS & DaaS.
- Capability to manage a hybrid cloud environment.
- Support for generic x86 environment and leading hardware OEMs.
- Data-driven and ready for the unpredictable.

3.6. 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.

3.7. Onsite Support for Data Centre 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.

3.8. Certifications:

- Current SDC is certified with ISO 27001 & ISO 20000.
- Bidder to obtain the following Data Centre Certifications within 6 months from Go-Live, with all related costs borne by the bidder:
  - ISO 9001
  - ISO 27001
  - ISO 20000
  - ISO 27017
- Cost of sustenance audit for the above certifications through third-party agencies is the responsibility of the bidder for the entire contract period.

3.9. Migration and Connectivity:

- Relocation of existing/new Internet connectivity from SDC to ODESSEY, with the successful bidder managing and facilitating the internet connectivity with respective ISPs.
- Consolidation and integration of network and security devices from existing SDC to ODESSEY, with an integrated design and plan included in the technical proposal.

3.10. Others critical requirement

- The selected bidder has to integrate the critical infrastructures like OSWAN, Sec-LAN, CSOC, Existing SDC with ODESSEY to avail all the features required by the same.
- Logical PODs to be created container wise for better security purpose.
- Data Plane & Control Plane to be done separately for uninterrupted traffic flow.

3.11. Operation and Maintenance:

- Annual Maintenance of products and services.
- Adherence to Service Level Agreements (SLA).
- Resource deployment for effective operation and maintenance.
- Implementation and adherence to Standard Operating Procedures (SOP).

4. Pre-Qualification Criteria

For a bidder to be considered eligible for participation in the procurement process, mandatory pre-qualification criteria must be met as outlined in the following table. The technical evaluation will only proceed for proposals from bidders who fulfil these mandatory pre-qualification criteria. Proposals failing to meet any of the pre-qualification criteria will be subject to rejection.

A bidder engaging in the procurement process is required to meet the following minimum pre-qualification and eligibility criteria.

Sr. No.	Parameter	Specific Requirements	Documents
1	Legal Entity	The bidder must be a State or Central Govt. PSU having presence in Odisha and must have GST registration. Note: - Consortium of any kind shall not be acceptable for this project. Any deviation would lead to disqualification or termination of the same.	• Copy of GST registration. • Copies of relevant Certificates of registration Income Tax / PAN Number from the respective Government Department.
2	Financial Turnover	Annual Turnover of the PSU during the last three financial years, as per the last published audited balance sheets), should be more than (INR) 1000 Crores each year as on 31st March 2023.	CA/CS Certificate for Net Worth with CA's/CS's Registration No or Seal and Copy of audited profit and loss account and balance sheet of the last three financial years ending 31st March 2023.
3	Net Worth	The net worth of the PSU should be Positive for last three Financial Years, as on 31st March 2023.	Copy of audited profit and loss account/ balance sheet of the last three financial years, highlighting the requisite figure related to positive net worth and profitability ending 31st March 2023.
4	Certifications	The PSU must have following Certificates 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	Copy of Valid Certificate during the bid validity period

Sr. No.	Parameter	Specific Requirements	Documents
5	Project Experience	During the last Seven years(PO/Work order Date should be with in last seven years ending last date of bid submission), the PSU should have implemented, commissioned and operated Data Centre projects/ large projects having Datacentre for Central / State Governments, PSUs, PSE, Banking & Financial Institutions, Telecom and IT companies in India that meets the below mentioned requirement: a. Single order of value 80 Crore or more; OR b. Two orders each having minimum value of 60 Crores or more; OR c. Three orders each having minimum value of 40 Crores or more **Note:-** (i) The orders should be include any DC/ DR/ NOC/ SOC/ CCC consisting of IT components like (Server, Storage, Backup system, Cloud solution, Network & Cyber security equipment etc) (ii) Operation & Maintenance including FMS of the DC/ DR/ NOC/ SOC/ CCC as on last date of Bid submission	Copy of work order(s) / Purchase Order/ Completion Certificate/ contract agreement. Supported with relevant documentary evidences for the design parameters and the completion or Go Live or FAT certificates by the customer. The work orders/agreement/completion certificate of projects having Datacentre as part of scope should have value mentioned and easily identifiable for evaluation purpose.
6	Technical Manpower	The PSU must have 100 technically qualified professionals in the IT/ICT domains i.e. systems, , networking, system software, systems integration, storage, Backup solution, cloud solution, Cyber security who have prior experience in providing the Data Centre Infrastructure maintenance services as on bid submission date.	Certificate from bidder's Head of HR Department for the 100 number of Technically Qualified professionals employed by the company in the following format. HR certificate on company's letterhead stating the points with employee Name, Qualification, Certification to be submitted along with copy of the relevant certificate.
7	Mandatory Undertaking	The Bidder shall: - a) Not be insolvent, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons;	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.

Sr. No.	Parameter	Specific Requirements	Documents
		b) Not have, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of five years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings; c) Not blacklisted with any of the State/Central Government or any government agency as on the date of submission of the bid.	
8	Bid Document Fee	₹25,000/- + 12% GST	In the form of Demand Draft from a scheduled bank of India in favor of Odisha Computer Application Centre, payable at Bhubaneswar.
9	Earnest Money Deposit (EMD	₹2,00,00,000.00 (Rupees Two Crore only).	In the form of a bank guarantee issued by any nationalized/scheduled commercial bank in favour of Odisha Computer Application Centre, payable at Bhubaneswar.

4.1. Submission of the Proposal

4.1.1.Instruction to Bidders for Online Bid Submission

e-Nivida is a complete process of e-Tendering, from publishing of Tenders online, inviting online bids, evaluation and award of contract using the system. 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.

4.1.2.Guidelines for Registration

a. 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.5,600/- inclusive of Applicable GST.

b. As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

c. 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.

d. 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.

e. Only valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.

f. 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.

g. The scanned copies of all original documents should be uploaded in pdf format on e-Tender portal.

h. 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.

4.1.3.Searching for Tender Documents

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

b. 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 fee 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.

4.1.4.Preparation of Bids

a. Bidder should take into account any corrigendum published on the Tender document before submitting their bids.

b. Please go through the Tender advertisement and the Tender document carefully to understand the documents required to be submitted as part of the bid.

c. 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.

d. 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.

e. 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 submission process. Already uploaded documents in this section will be displayed. Click "New" to upload new documents.

4.1.5. 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 has to 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 Department.

c. Bidder has to 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 case of BG bidder 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 time 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 has to 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.

4.1.6. 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 the Helpdesk Support. Please feel free to contact e-Nivida Helpdesk (as given below) for any query related to e-Tendering.
Phone No.: 011-49606060
Mail id: odishaenivida@gmail.com

4.2. Late Proposals

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

4.3. Proposal Prices

1. The prices outlined in the price schedule should be entered as follows:
   a) The total quoted price must encompass the cost of IT supply, installation, commissioning, and provision of hardware, licenses, software, services for installation, 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.
   b) The cost of operation and maintenance of IT systems for a period of FIVE (5) years after the date of Go Live.
2. The Bidder is not permitted to quote for the project in parts.
3. Before bidding, the Bidder may conduct site visits to all proposed sites/locations, which will be part of OSDC 2.0 at Bhubaneswar, to assess the actual physical and technical requirements. Site visits may be facilitated upon mail request to the Contact Officer, as mentioned in the Invitation of Bid section.
4. The bidder must submit a detailed Bill of Material, including Make & Model, and Bill of Quantity with prices for each component.
5. OCAC reserves the discretion to increase or decrease the quantity and items if the need arises.

4.4. Earnest Money Deposit

Bidders are required to submit an Earnest Money Deposit (EMD) of Rs. 2,00,00,000.00 (Two Crore only), in the form of a bank guarantee issued by any nationalized/scheduled commercial bank in favour of OCAC.

1. 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.
2. 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, as per the format provided in Proforma-22.
3. 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.
4. The EMD may be forfeited:

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

4.2. 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.

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

4.4. Any material breach of contract

4.5. Performance Bank Guarantee

4.5.1. 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 as mentioned in this RFP in favor of the Odisha Computer Application Centre shall be submitted by the successful bidder within 15 days of issue of Purchase Order.

4.5.2. Failure of submission PBG within the specified time period may lead to cancel the Purchase Order.

4.5.3. The Bank guarantee shall be valid till 5 years and 6 Months (66 Months) beyond completion of all installation of the necessary Hardware/components/Licenses at OCAC.

4.5.4. 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.

4.6. Bid Validity Period

1. The Earnest Money Deposit (EMD) submitted with the bid will remain valid for the entire duration specified in the fact sheet.
2. 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.
3. 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.

4.7. Compliance and Completeness of Response

1. 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.
2. The RFP offer may be out-rightly 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.
3. 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.

4.8. Clarification on Revised RFP

Bidders may raise clarifications on the revised RFP and all such queries/clarifications should reach OCAC in the above-mentioned mails in fact sheet on Dt. 11/03/2024 by 03: 00 PM. 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 below not later than date and time indicated above. OEM queries shall not be taken into consideration.

Name of the OEM/PSU -						
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 – http://www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in/

- Queries received, other than PSUs and OEMs, will not be entertained.
- **Queries should be given in MS-Excel only**. **Queries received beyond the given format will not be accepted.**
- OCAC at its discretion may extend the last date for the receipt of proposals.
- Once the similar queries shall be answered, same queries will not be entertained further.
- It is expected that the bidder shall do their own due-diligence on the question they may ask. Any changes sought must be with proper justification. Any statements such as 'specification/requirement is not vendor neutral' OR 'it implies to single OEM' or any such statement similar to this, must be asked with adequate and credible proof and justification, else such queries will not be accepted.

4.8.1. Responses to pre-bid queries and issue of corrigendum

1. Bidder may seek clarification on this RFP document not later than the date specified. OCAC reserves the right to not to entertain any queries post that date and time. The bidder are requested to submit their queries in MS-Excel editable format.
2. At any time prior to the last date for receipt of bids, OCAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the RFP document through a corrigendum.
3. Any modifications of the RFP Documents, which may become necessary as a result of the Pre-Bid queries, shall be made by OCAC exclusively through a corrigendum. Any such corrigendum shall be deemed to be part of this RFP and incorporated into this RFP. However, in case of any such amendment, the bid submission date may be extended at the discretion of OCAC.
4. The corrigendum or clarifications (if any) to the queries from any bidder will be published on the website, http://www.ocac.in, www.odisha.gov.in & https://enivida.odisha.gov.in/ in form of modified RFP/corrigendum etc.

5. In order to provide prospective bidders reasonable time for taking the corrigendum/modifications into account, OCAC may, at its discretion, extend the last date for the receipt of Bids.
6. It is the responsibility of the bidder to check the above websites time to time for updates.

4.9. Amendment of Proposals

i. 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.

ii. 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.

4.10. 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.

4.11. Evaluation Procedure

1. OCAC reserves the right to form an Evaluation Committee for scrutinizing bidder responses.
2. The Evaluation Committee, appointed by OCAC, will thoroughly assess RFP responses and accompanying documents. Failure to submit essential supporting documentation may result in rejection.
3. 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.
4. The Evaluation Committee may arrange meetings with bidders to seek clarifications on their submissions.
5. OCAC holds the authority to reject bids based on any identified deviations.
6. Each response will be evaluated according to the criteria outlined in the RFP.

7. 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.

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

    - The Evaluation Committee will assess the completeness of bids, identifying computational errors, and verifying overall orderliness.
    - Reasonableness of Prices: Bidders are required to quote reasonable prices aligned with market rates. Abnormally High Rates (AHR) and Abnormally Low Rates (ALR) will not be accepted.
    - OCAC may consider the price of an item as zero if not quoted but essential for project implementation.
    - Detailed Bill of Quantity (BOQ) and Bill of Material (BOM) must be submitted as an unpriced bid in the technical section.
    - Arithmetical errors will be corrected, with precedence given to unit prices in case of discrepancies.
    - Clarification meetings may be conducted, and results will be published on the specified website.
    - The Evaluation Committee's responsibilities extend to decisions related to the RFP Document and project execution.
    - The proposal opening will occur in the presence of bidder representatives who sign a register as evidence of attendance.
    - The proposal document will undergo the following steps:
        - Preliminary Examination: Ensures eligibility criteria compliance and overall completeness.
        - Technical Evaluation: Comprehensive assessment of technical aspects for responsiveness to RFP requirements.
        - Technically qualified bidders proceed to the opening of commercial bids for further evaluation.

5. Technical Bid Evaluation Scoring Matrix

5.1. Tender Evaluation Methodologies

The assessment process is structured into three primary categories: (a) Organizational Strength and Project Experience Evaluation (b) Technical Evaluation (c) Technical Presentation

The bid will be evaluated based on the following criteria:

Sr. No.	Criteria	Scores
1	Organizational strength and Project Experience	80
2	Technical Presentation	20
	Total	**100**

5.1.1. Organizational Strength and Project Experience – 80 Marks

Sl.	Criteria	Description	Max. Score	Scoring Mechanism	Credential Required
1	**Turn over:**	Annual Turn Over per annum of PSU for last 3 years as mentioned in eligibility criteria, minimum 1000 Crores.	30	Scoring Mechanism >= 1000 Crores- <2000 = 10 Marks >=2000 Crores and <3000 Crores = 20 Marks >= 3000 Crores = 30 Marks	Copy of audited Balance Sheets and Profit and Loss (P/L) statement/ CA Certificate for last 3 FY 2023-22, 2022-21, 2021-20
2	**Project Experience:**	During the last Seven years(PO/Work order Date should be with in last five years ending last date of bid submission), the PSU should have implemented, commissioned and operated Data Centre projects/ large projects having Datacentre for Central / State Governments, PSUs, PSE, Banking & Financial Institutions, Telecom and IT companies in India that meets the below mentioned requirement: a. Single order of value 80 Crore or more; OR . Two orders each having minimum value of 60 Crores or	20	>=80 crore - 1 order OR >=60 crore - 2 orders OR >=40 crores -3 orders = 10Marks >=80 crore -2 orders OR >=60 crore- 4 orders OR >=40 crores -6 orders = 20 Marks	Copy of Work Order / Agreement / Work Completion/ In progress Certificate

Sl.	Criteria	Description	Max. Score	Scoring Mechanism	Credential Required
		more; OR c. Three orders each having minimum value of 40 Crores or more (i) The orders should be include any DC/ DR/ NOC/ SOC/ CCC consisting of IT components like (Server, Storage, Backup system, Cloud solution, Network & Cyber security equipment etc) (ii) Operation & Maintenance including FMS of the DC/ DR/ NOC/ SOC/ CCC as on last date of Bid submission			
3	Technical Manpower	The PSU must have at least 100 technically qualified professionals in the IT/ICT domains i.e. systems, networking, system software, systems integration, storage, Backup solution, cloud solution, Cyber security who have prior experience in providing the Data Centre Infrastructure maintenance services as on bid submission date.	20	100 Technical Manpower = 5Mark >100 & <300 Technical Manpower = 15Mark >= 300 Technical Manpower = 20Mark	Certificate from bidder's Head of HR Department for the 100 number of Technically Qualified professionals employed by the company in the following format. HR certificate on company's letterhead stating the points with employee Name, Qualification, Certification to be submitted along with copy of the relevant certificate.
4	SDC/NDC Management	Experience in managing IT Infrastructure of any SDC/NDC	10	One SDC/NDC management experience = 4Mark Two SDC/NDC management experience = 7 Mark >Two SDC/NDC management experience = 10 Mark	PO/Work Order of the project.
Total			**80**		

Technical Presentation - 20 Marks

The technical presentation must exhibit a high level of professionalism and should encompass, but not be limited to, the following aspects:

- **Bidder's Understanding of the Project & Scope of Work** – 5 Marks
- **Solution Architecture & Design (IT)** – 5 Marks
- **Approach & Methodology** – 3 Marks
- **Project Plan & Project Team's Experience** – 3 Marks
- **Operation and Maintenance Plan** – 4 Marks

Note:

1. This information is for the vendor's internal reference and need not be submitted with the Bid.
2. Vendors must furnish relevant credentials for each of the above points for scoring.
3. 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.
4. The solution demonstrated will be evaluated using a pre-set questionnaire.
5. The vendor must provide supporting documentation such as product technical architecture, describing various technical parameters.
6. The overall proposal, implementation methodology, and adherence to the project plan will be assessed.
7. Bidder's experience in building their own in-house Data Centre or captive Data Centre for commercial use will not be considered.

6. Evaluation of Bids and Award of Contract

6.1. 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 80 marks in Technical Score for eligibility to open the financial proposal.

6.2. Financial Evaluation Methodology (LCBS):

a) The financial bids/ cover of the bidders who qualify in pre-qualification/eligibility criteria shall be opened at the notified time, date and place by the members of the designated Procurement 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 appropriate format as per **Proforma 24** followed by financial bid details**.**

c) The process of opening of 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 price for all the deliverables and services 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 levies and 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 of 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 the ascending order as L1, L2, and L3 etc.

6.2.1.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.

6.3. Deviations and Exclusions

Bids must strictly adhere to RFP requirements. A No Deviation Certificate (Proforma 15) is required. Deviations may result in rejection.

6.4. 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 makes/models for a unique item.

6.5. 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.

7. General Conditions of Contract

7.1. 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. **Approvals:** 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. **Data Centre 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 4.18.

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 30 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.

7.2. Right to Terminate the Process

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

7.3. 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).

7.4. OCAC's Right to Accept and Reject Proposals

- Notwithstanding anything else contained to contrary in this RFP Document, OCAC reserves the right to accept or reject any Bid or to annul the bidding process fully or partially or modifying 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 and without assigning any reason. OCAC makes no commitments, express or implied, 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

7.5. 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 similar to the original Proposal.
- Subsequent to 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, telegraphic or telephonic proposals modifications will be acceptable..

7.6. 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.

7.7. 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.

7.8. 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 allowed for opportunity to mutually discuss its terms and conditions. The final decision in such an occurrence lies with OCAC.

7.9. Governing Law & Jurisdiction

- The Contract shall be governed by and interpreted in accordance with the laws of the India. The High Court of Judicature at Cuttack and Courts subordinate 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.

7.10. 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 that 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.

1. 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 60 days' notice. The decision of OCAC as to such breach shall be final and binding on the system integrator
2. In the event of the breach of any of the major and significant terms and conditions of this agreement by the system integrator, OCAC will give 60 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 60 days. In case the breach will continue till/after expiry of such cure period, OCAC will terminate the agreement.

3. Effects of Termination
4. Upon expiration or termination of this Agreement:
   a. The System integrator shall:
      i. Notify forthwith the particulars of all project assets.
      ii. 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 State Data Centre
      iii. Deliver relevant records and reports pertaining to the State Data Centre 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
      iv. Shall expeditiously settle the accounts.
   b. 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.
   c. 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
   d. 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.
   e. Any and 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
   f. SI immediately upon termination, discontinue providing any or all of the services contemplated hereunder.
   g. 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 of this agreement; and

h. Upon the termination or expiration this agreement , in case before complete delivery of materials, then the title and ownership of all materials, plans, ideas, services or information (developed by System Integrator for OCAC) shall be transferred by SI to OCAC. Thereafter, OCAC, shall have no liability to SI's service arising from OCAC's use of any material was approved ,used, published or presented by or on behalf of OCAC. SI shall transfer such property, and documentation related thereto, to OCAC immediately after termination in case termination happens before complete delivery of materials.

i. SI shall return all the property which belongs to OCAC including any data, information, files of completed or unfinished work. SI shall have no lien over the property of OCAC.

5. **Termination due to bankruptcy of the System Integrator –** OCAC shall serve a written notice on the System Integrator at any time to terminate this Agreement with immediate effect in the event that the System Integrator reporting an apprehension of bankruptcy to OCAC or its nominated agencies. No Charges to the system integrator shall be payable in case of termination under this clause except for the equipment satisfactorily delivered and approved by OCAC as per the terms of this Agreement and services performed by the System Integrator up to the date of termination

7.11. Statutory Compliances

- 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.

7.12. Consequences of Termination

- In the event of termination of the Contract due to any cause whatsoever, whether consequent to the stipulated term of the Contract or otherwise, OCAC shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/material breach, and further allow the next successor Vendor to take over the obligations of the erstwhile

- Vendor in relation to the execution/continued execution of the scope of the Contract.
- Nothing herein shall restrict the right of OCAC to invoke the Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available OCAC under law or otherwise.
- The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.
- Upon Termination of the Contract, the System Integrator shall:
- Prepare and present a detailed exit plan within five calendar days of termination notice receipt to the customer.
- The customer and along with designated team will review the Exit plan. If approved, SI shall start working on the same immediately. If the plan is rejected, SI shall prepare alternate plan within two calendar days. If the second plan is also rejected, the customer or the authorized person will provide a plan for SI and it should be adhered by in totality

7.13. Indemnification

- Successful System Integrator hereby indemnifies, hold harmless & undertakes to defend OCAC, its affiliates and their respective employees, officers and directors against any claim by a third party including but not limited to damages, costs, expenses as a result of such claim with regards to:
- the extent that the System Integrator provided to OCAC by System Integrator under this Agreement infringes any third party’s intellectual property rights;
- taxes/charges/cess/levies (and interest or penalties assessed thereon) against OCAC that are obligations of System Integrator pursuant to this Agreement;
- any damages for bodily injury (including death) and damage to real property and tangible personal property caused by the System Integrator;
- any claim or action by or on behalf of the System Integrator personnel based on his or her employment with the System Integrator, including claims arising under occupational health and safety, worker’s compensation, provident fund or other applicable laws or regulations;
- claims by government regulators or agencies for fines, penalties, sanctions or other remedies arising from or in connection with the System Integrator failure to comply with its regulatory/legal requirements and compliances;

- any claim on account of an alleged breach of confidentiality and security of data occurring as a result of acts of omissions or commission of the System Integrator employees or sub-contractors;
- any claim occurring on account of misconduct, negligence or wrongful acts of omission and commission of employees of the System Integrator, and/or its sub- contractors;
- any claim occurring on account of misuse or negligent application, misuse of systems, failure to follow established procedure by the System Integrator and/or sub-contractor's employees;
- System Integrator shall ensure compliance with all applicable laws, local and Central, including all labour laws like ESI, EPF, Minimum Wages Act, Odisha Shops & Establishments Act, Contract Labour (Regulation and abolition) Act 1970, Payment of Bonus Act etc. and shall keep First Part indemnified and harmless in case of any action for violation by Second Part of any of the applicable laws so long as this arrangement is in force. For all purposes the persons deployed will be employees of second part and they will have no relation whatsoever with First Part. Second Part shall be responsible to furnish all such information/documents to First Part in this regard as may be required by it from time to time. Furthermore, Second part shall be responsible to furnish self- attested copies of all returns/challans filed by second part in the office of ESI, EPF, Minimum Wages Act, Contract Labour etc. on monthly basis to the first party, in case, the second part fails to submit or not willing to submit the copies of returns, first part shall be entitle to stop the payments till the submissions of the returns.
- In event of any theft, loss, damage, destruction, or any other act of vandalism or sabotage of the property of the Customer in the possession of the System Integrator by virtue of this agreement, the System Integrator shall be liable to indemnify the first part to the extent of damage or loss so caused.
- System Integrator has all the requisite consents, licenses and permissions to (I) enter into this Agreement (ii) carry out the obligations set out in this Agreement and it shall keep all such consents, licenses and permissions renewed and valid at all times during the continuance of the Agreement.
- SI indemnifies OCAC against third-party claims and other specified liabilities.

7.14. Limitation of Liability

- Neither Party; nor its subsidiaries or its affiliates will be liable to the other Party, whether in contract, or (including negligence), strict liability or otherwise, for loss of business, revenue, profits, loss of goodwill or reputation; or indirect, consequential, or special loss, arising in connection with any order, product, service, related documentation, information and/or the intended use thereof, even if a Party has been advised, knew or should have known of the possibility of such damages.

- Subject to the above and not withstanding anything to the contrary elsewhere contained herein, the total Liability of the bidder in connection with any damage or loss under this contract is maximum 100% of the project cost
- Both parties' liability limitations outlined, with the total liability capped at 100% of the project cost.

7.15. Dispute Resolution

- **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.

7.16. 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 either party initiates arbitration proceedings within sixty days of such decision.
- Arbitration proceedings will be held in Bhubaneswar, Odisha, and conducted in English.

7.17. 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.

7.18. Force Majeure:

- Force Majeure is herein defined as any cause, which is beyond the control of the SI or OCAC as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:
- 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 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 as a result of an event of Force Majeure.
- In case of a Force Majeure, all Parties will endeavour to agree on an alternate mode of Performance in order 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 last date of termination in case of force majeure
- If force majeure conditions continue for more than 30 days and the services are suspended, then either party has the right to terminate this agreement.
- Force Majeure events excuse parties from performance obligations.
- The System Integrator must promptly notify OCAC of Force Majeure conditions and continue performance to the extent feasible.
- If Force Majeure lasts over 30 days, either party can terminate the agreement.

7.19. 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 proprietary 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 purposes 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.

7.20. Fraud and Corrupt Practices:

- 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.
- 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 during a period of < period, suggested 2 (two) > 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.

- For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:
- “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;
- “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
- “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;
- “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
- “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.
- Prohibits corrupt, fraudulent, coercive, undesirable, and restrictive practices during the selection process.
- OCAC may reject a proposal and declare the System Integrator ineligible in case of prohibited practices.

7.21. Exit Management Plan:

- The SI shall not exit from the contract within stipulated time period of five (5) years after Go-Live. However, in the event that the 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.
- 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 in annual basis and need to be submitted to OCAC.

7.21.1. Purpose of Exit Management Plan

- 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 Master Service Agreement with detailed information about exit criteria and exit management plan.
- The exit management period starts, exactly period of 30 days before, in case of expiry of contract, or on the date when the contract comes to an end and up to 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.
- At the beginning of the exit management period, the System Integrator shall ensure that
- 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 OSDC 2.0 Project is compliant with the Specifications and Standards set forth in the RFP, Agreement and any other amendments made during the contract period;
- The System Integrator delivers relevant records and reports pertaining to the OSDC
- 2.0 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;
- 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;

- 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 OSDC 2.0 Project free from all encumbrances absolutely and free of any charge or tax to OCAC or its nominee
- 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;
- 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 State Data Centre 2.0 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.
- 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.
- Hand Over of Assets/ Documents; SI shall handover 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.
- 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.
- Existing SI will hand over the documents to OCAC or new SI, pertaining to the operation of OSDC

i.e. all configuration records, purchase orders, installation reports, FAT/PAT records, SLA records, SLA methodology, SLA calculation template, MIS reports, ISO documents (procedures, records, templates, standards), Audit records, security assessment and risk records, all SOPs, warranty documents, AMC documents, Knowledge documents (KEDB), Training records etc.

- The SI must provide a written exit plan if exiting before the stipulated five-year period.
- OCAC reserves the right to terminate the contract in case of premature exit, with conditions for bidder replacement.

7.22. 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.
- If any provision is deemed illegal or unenforceable, parties will negotiate a valid substitute.
- No waiver of rights, remedies, or provisions unless explicitly stated.

7.23. Applicability of Liquidated Damages:

- The System Integrator shall accomplish the scope of work under this Agreement as per the Project Timelines and as per the Service Level Agreements. If the System Integrator fails to achieve the Project Timelines or if it fails to achieve the Service Levels (in the SLAs) for any reason whatsoever, the System Integrator shall be liable to pay liquidated damages as provided in QGR SLA and Penalty Table & LD Table of this Agreement. 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. Liquidated damages would be 1 % of the undelivered portion of the Capex / products, for delay of every week, and capped at 10% of the cost of Capex as mentioned in the Agreement.

- If the liquidated damages exceeds the cap as mentioned in the Agreement, the Purchaser or OCAC shall have the right to terminate the agreement for default and consequences for such termination as provided in the agreement shall be applicable. In case it leads to termination, OCAC shall give Sixty days' notice to the SI of its intention to terminate the contract and shall so terminate the contract unless during the Sixty days' notice period, the SI initiates remedial action acceptable to OCAC.
- Each of the Parties shall ensure that the range of the Services/Deliverables under the SLA shall not be varied, reduced or increased except with the prior written agreement /consent between the Purchaser and the SI in accordance with the provisions of change request procedure as set out in this Agreement.
- If the Goods and Related Services supplied do not meet the minimum specifications as per the Contract, and the same is not replaced/modified by the SI to meet the requirements within 14 days of being informed by the OCAC, the OCAC shall be free to impose any penalty as deemed fit. In addition, the OCAC shall reserve the right to terminate the contract and recover liquidated damages by forfeiting the performance bank guarantee submitted by the SI.
- Liquidated damages apply if the System Integrator fails to meet project timelines or service levels.
- The cap for liquidated damages is set at 10% of the cost of Capex.

7.24. Intellectual Property Rights:

- OCAC retains exclusive rights to project-related intellectual property.
- All Intellectual Property of OCAC under the Letter of Invitation and/ or the Contract will belong exclusively to GoO, except the pre-existing intellectual property rights of the Bidder, its subcontractors (if any). On payment of all of consultant's fees in connection with this Agreement and subject to the other provisions of this Agreement, GoO shall at all times retain to use within its internal business all right title and interest in and to any Intellectual Property Rights in the deliverables to be provided by the Bidder under this Agreement and any modifications thereto or works derived from there except the pre- existing intellectual property rights of Consultant or its subcontractors (if any, and Consultant Technology. It is hereby expressly clarified that Bidder shall have no right, title or interest in or to such Intellectual Property Rights of OCAC for any purpose, except the right to use, modify, enhance and operate such designs, programs, modifications as per requirement of OCAC. Bidder shall not use such Intellectual Property of OCAC for any other purpose during and after the term of the Contract.
- No services covered under the Contract shall be sold or disposed by the Bidder to OCAC in violation of any right whatsoever of third party, and in particular, but without prejudice to the generality of the foregoing, of any patent right, trademark or similar right, or any charge mortgage or lien.

- Subject to clause (c) below, the Intellectual Property Rights of all the database, programs, reports, formats etc. developed/created for this project would be of OCAC / GoO.
- The Bidder shall continue to retain sole ownership of the pre-existing proprietary knowledge, tools, source code, records, SOPs, application configurations, drawings, methodology, templates, works of authorship, materials, information plus any modifications or enhancements thereto and intellectual property content brought in by Bidder to this engagement and/or incorporated in the deliverables submitted by Bidder to OCAC or created independently of the performance of the Services ("Consultant Technology"). For avoidance of doubt, it is clarified that Consultant or its subcontractor shall have the right to use any works of authorship or other intellectual property that may be included in the Deliverables, to develop for themselves, or for others, materials or processes that may be similar to those produced as a result of the Services. Further, any third party licenses other than the hardware and software to be used by the Bidder resources for delivering the deliverables under this Agreement, necessary for the performance of the Services under this Agreement, would need to be procured by OCAC. Bidder hereby undertakes;
- Not to provide access to the Intellectual Property of OCAC to persons other than authorized users to ensure that all authorized users are appropriately notified of the importance of respecting the Intellectual Property Rights of OCAC and that they are made aware of and undertake to abide by the similar terms and conditions of the this Agreement. Not to permit any person, other than the authorized users, to copy, duplicate, translate into any language, or in any way reproduce the Intellectual Property of OCAC. To effect and maintain reasonable security measures to safeguard the Intellectual Property of OCAC from unauthorized access or use by any third party other than the authorized users. To notify OCAC promptly of any unauthorized disclosure, use or copying of the Intellectual Property of OCAC of which Bidder becomes aware. To change the manpower deployed if OCAC notifies issue (along with the justifiable ground) in the satisfactory performance of the respective resource.
- The SI shall retain exclusive ownership of all methods, concepts, algorithms, trade secrets, software documentation, other intellectual property or other information belonging to the SI that existed before the effective date of the contract.
- The System Integrator retains ownership of pre-existing proprietary knowledge.

7.25. Notices:

- Parties must provide written notices regarding the agreement at specified addresses.
- Any queries or other document, which may be given by either Party under this Agreement or under the SLA, shall be given in writing in person or by pre-paid recorded delivery post or by facsimile

transmission or through email to the notified address.

- In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

To OCAC:
Attention: General Manager (Admin) Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

To
[Name and Address of Successful Bidder]

- Any notice or other document shall be deemed to have been given to the other Party (or, if relevant, its relevant associated company) when delivered (if delivered in person) if delivered between the hours of 10.00 am and 5.00 pm on a working day at the address of the other Party set forth above or if sent by fax, provided the copy of the fax is accompanied by a confirmation of transmission, or on the next working day thereafter if delivered outside such hours, and 7 days from the date of posting (if by letter).
- Notice can also be given through email address furnished by the System Integrator. The time of the sent message in outbox of the sender will be considered to be time of delivery of the message.
- Either Party to this Agreement or to the SLA may change its address, telephone number, facsimile number and nominated email for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.
- Notices may also be delivered via email.

7.26. 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).

7.27. Audit, Access, and Reporting

- The System Integrator shall grant access to OCAC or its nominated agencies to all data related to OSDC 2.0. 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 OSDC 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.

7.28. 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.

7.29. 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.

7.30. 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.
- All IT products quoted should be supported by the SI for the next 5 years from the start date of O &

M services, with the SI committing to support for an additional 2 years if necessary.

- The Bidder warrants that all equipment supplied under the contract is newly manufactured and free from defects in design, materials, or workmanship, under normal use in the prevailing conditions.
- Services provided under the contract must adhere to the Service Level Agreement (SLA) defined in the tender.
- This warranty for all equipment remains valid for Five (5) Years after the complete installation, final commissioning, and Go-Live of the Data Centre.
- If any component or documentation/media is not delivered, installed, operational, or acceptable to OCAC after final acceptance testing, the installation is deemed incomplete.
- All IT products quoted should be supported by the SI for the next 5 years from the start date of O & M services or end of FAT, whichever is earlier.
- OCAC shall promptly notify the Bidder of any claims arising under this warranty, and the Bidder must repair/replace/reconfigure/re-provision the defective equipment or service.
- The supplier must ensure during the comprehensive warranty period that all supplied stores continue to function as per the parameters mentioned in the technical specification.
- The supplier is responsible for maintenance/preventive maintenance of the complete system. Any malfunctioning or defective items shall be replaced by the supplier free of cost at the project site under specified conditions.
- All software and hardware used for providing data Centre services shall be licensed to OCAC and will be the property of OCAC, with perpetual licenses for all supplied items.
- The SI is responsible for end-to-end implementation and should quote and provide/supply any items required for commissioning of the cloud, network equipment, including any Compute equipment. OCAC will not pay for items not quoted by the SI but necessary for the project's successful completion.

7.31. OEM Certificate of Equipment

- The bidding company, as the Original Equipment Manufacturer (OEM), must provide an OEM Certificate as per the applicable Proforma (11, 12, 13 & 14).
- The certificate should state the bidding company's authorization to offer the equipment and a commitment to provide maintenance support during the comprehensive warranty period.
- If stores are supplied by an authorized supplier of the OEM, the OEM certificate should state that the OEM will take over maintenance responsibility if the authorized supplier fails during the

comprehensive warranty.

- 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.

7.32. Comprehensive AMC of Equipment

- The selected bidder is responsible for operating and maintaining OSDC 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 OCAC under this contract upon the successful completion of the final acceptance test.

7.33. 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 obligated 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.

7.34. 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.

7.35. 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 before three months of the contract expiry date.

8. Detailed Scope of Work

The broad specified scope of work to be undertaken by the “Selection of System Integrator for Design, Supplying, Installation, Testing & Commissioning, of ICT Infrastructure at OSDC 2.0 for the period of 5 years, has been outlined below.

The selected System Integrator shall ensure an uptime more than 99.982% on a quarterly basis for period of five years from the Go Live date.

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:

- Design integration of all the building blocks including the existing Data Centre.
- Design, Supply, Installation and Commissioning {final acceptance test (FAT)} of IT Infrastructure for Data Centre.
- Design, Supplying, installation, and configuration, testing and commissioning of computer infrastructure (hardware & software) such as Servers, Operating systems, and virtualization etc.
- 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).
- 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.
- Design, Supply, installation, and configuration, testing and commissioning of security infrastructure (hardware & software) such as D-DoS, AAA, Firewall, Anti-APT, DLP etc.
- 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.
- System Integrator to get following Data Centre Certification within 6 months from Go-Live and all related cost for the certification will be borne by System Integrator :

a. ISO/IEC 27001 (latest)
b. ISO/IEC 20000 (latest)
c. ISO/IEC 9001 (latest)
d. ISO/IEC 27017(latest)

- Cost of sustenance audit for above certification shall be responsibility of the successful System Integrator for the entire contract period.
- Testing & Commissioning
- Post-Implementation: Management & Maintenance
- Security management
- Migration of the existing applications and hardware of OSDC 1 to OSDC 2.
- Training on IT infrastructure, SLA, Various Data Centre related polices etc.
- Onsite support for Data 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.
- Operation and Maintenance of OSDC 2.0 for a period of 5 years after go live.

8.1. Data Centre Architecture

8.1.1.Guiding Principles for the Architecture

One of the business requirements is to provide a secure, highly available and resilient Data center platform to Smart City applications.

Following are the agreed upon guiding principles for the new Data Center Architecture.

- Driving competitive advantage through mature and proven technology solutions
- Highly resilient and highly available network Architecture
- Preferred Virtualized Data Center to mitigate cost and to optimize resource utilization.
- Highly scalable and flexible and be able to support different Application and Security tiers requirements.
- Fault domain isolation and reduce policy complexity.
- 40 / 100 Gb Ready Infrastructure; Potentially 10-Gb to the server.
- Streamlining operations to gain efficiencies, reduce costs and improve time to market.

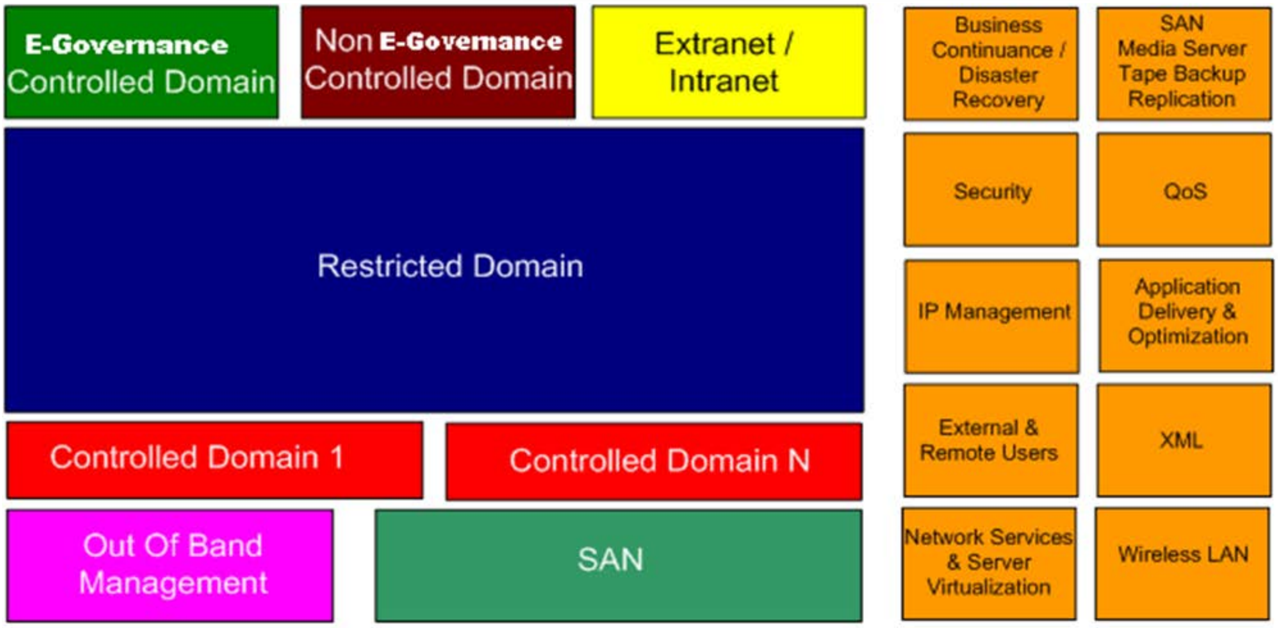

E-Governance Controlled Domain
Non E-Governance Controlled Domain
Extranet / Intranet
Business Continuance / Disaster Recovery
SAN Media Server Tape Backup Replication
Restricted Domain
Security
QoS
IP Management
Application Delivery & Optimization
Controlled Domain 1
Controlled Domain N
External & Remote Users
XML
Out Of Band Management
SAN
Network Services & Server Virtualization
Wireless LAN

Figure: Data center Building Blocks

8.1.2.DC Core Layer / Aggregation Layer

The data center core connects the City Network to the data center aggregation layer using high-speed Layer 3 links. The core is a centralized Layer 3 routing layer in which one or more data center aggregation layers connect. The data center networks are summarized, and the core injects the default route into data center aggregation. The data center core also needs to support IP multicast to provide connectivity to the growing use of IP multicast applications.

The data center core layer is a best practice component of larger data center networks. Mid-sized data centers may use a collapsed core design combining the aggregation layer and core layers together.

Core Switches should be included in the features below.

- Should be chassis based & modular architecture for scalability with Redundant Route Processor, Power supply, switching fabric and any failure should not result in any performance degradation.
- The switch should support at least 2Tbps (full Duplex) switching bandwidth per slot to avoid any bottle neck.
- Support 100Gig interface to meet future requirements.
- Must support Virtual Extensible LAN (VXLAN) is a network virtualization technology scalability problem with large deployments.
- Must support Layer 3 Routing protocols like OSPF, BGPv4 along with IPv6 Support.

8.1.3.Access Layer / Server Farm

The data center access layer's main purpose is to provide Layer 2 and Layer 3 physical port density for various servers in the data center. In addition, data center 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.

- Should be fixed / chassis-based support 10Gig access ports and 40Gig or 100Gig for uplinks to core switch with redundant Power supply
- Must support Virtual Extensible LAN (VXLAN) is a network virtualization technology scalability problem with large deployments.
- Must support Layer 3 Routing protocols like OSPF, BGPv4 along with IPv6 Support.

8.1.4.Guiding Principles for the Architecture

One of the business requirements is to provide secure, highly available and resilient Data center platform to Smart City applications.

Following are the agreed upon guiding principles for the new Data Center Architecture.

- Driving competitive advantage through mature and proven technology solutions
- Highly resilient and highly available network Architecture
- Preferred Virtualized Data Center to mitigate cost and to optimize resource utilization.
- Highly scalable and flexible and be able to support different Application and Security tiers requirements
- Fault domain isolation and reduce policy complexity
- 40 / 100 Gb Ready Infrastructure; Potentially 10-Gb to the server.
- Streamlining operations to gain efficiencies reduce costs and improve time to market.

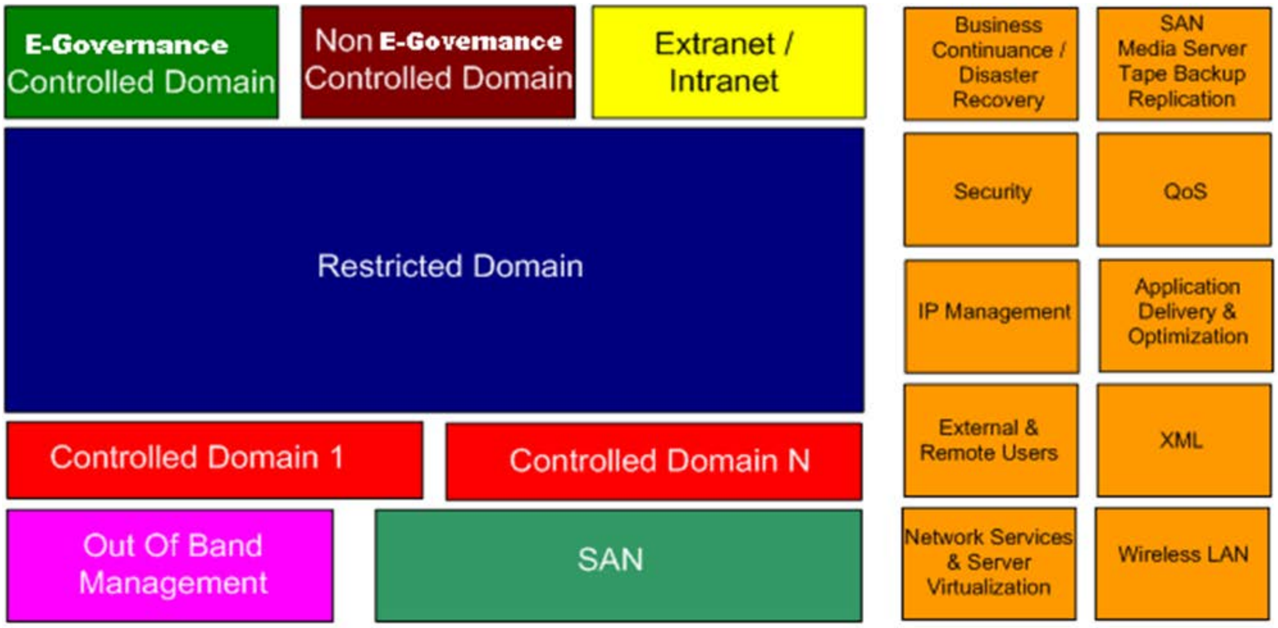

E-Governance Controlled Domain
Non E-Governance Controlled Domain
Extranet / Intranet
Business Continuance / Disaster Recovery
SAN Media Server Tape Backup Replication
Restricted Domain
Security
QoS
IP Management
Application Delivery & Optimization
Controlled Domain 1
Controlled Domain N
External & Remote Users
XML
Out Of Band Management
SAN
Network Services & Server Virtualization
Wireless LAN

Figure: Smart City Building Blocks

8.1.5.DC Core Layer / Aggregation Layer

The data center core connects the City Network to the data center aggregation layer using high-speed Layer 3 links. The core is a centralized Layer 3 routing layer in which one or more data center aggregation layers connect. The data center networks are summarized, and the core injects the default route into data center aggregation. The data center core also needs to support IP multicast to provide connectivity to the growing use of IP multicast applications.

The data center core layer is a best practice component of larger data center networks. Mid-sized data centers may use a collapsed core design combining the aggregation layer and core layers together.

Core Switches should be included in below features.

- Should be chassis based & modular architecture for scalability with Redundant Route Processor, Power supply, switching fabric and any failure should not result in any performance degradation.
- Switch should support at least 2Tbps (full Duplex) switching bandwidth per slot to avoid any bottle neck.
- Support 100Gig interface to meet future requirements.
- Must support Virtual Extensible LAN (VXLAN) is a network virtualization technology scalability problem with large deployments.
- Must support Layer 3 Routing protocols like OSPF, BGPv4 along with IPv6 Support.

8.1.6.Access Layer / Server Farm

The data center access layer's main purpose is to provide Layer 2 and Layer 3 physical port density for various servers in the data center. In addition, data center 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.

- Should be fixed / chassis-based support 10Gig access ports and 40Gig or 100Gig for uplinks to core switch with redundant Power supply
- Must support Virtual Extensible LAN (VXLAN) is a network virtualization technology scalability problem with large deployments.
- Must support Layer 3 Routing protocols like OSPF, BGPv4 along with IPv6 Support.

8.2. Project Implementation Phase and Key Deliverables

The complete Datacenter project shall be implemented in the following phases and SI has to follow the implementation cycle.

8.2.1.Inception Phase

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

1. Define an organized set of activities for the project and identify the interdependence between them.
2. 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.
3. Establish and measure resource assignments and responsibilities.
4. Highlight the milestones and associated risks.
5. Communicate the project plan to stakeholders with meaningful reports.
6. Measure project deadlines and performance objectives.
7. **Project Progress Reporting.** During the implementation of the project, System Integrator should present weekly reports. This report will be presented in the meeting to OPEC. The report should contain at the minimum the under mentioned:
   a. Results accomplished during the period (weekly)
   b. Cumulative deviations from the schedule date as specified in the finalized Project Plan.
   c. Corrective actions to be taken to return to planned schedule of progress.
   d. Plan for the next week.
   e. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of System Integrator.
   f. Support needed.
   g. Issues/Concerns
   h. Risks/Showstoppers along with mitigation
8. Identify the activities that require the participation of client personnel (including OPEC, the Program Management Unit etc.) and communicate their time requirements and schedule early enough to ensure their full participation at the required time.

8.2.2.Requirement Phase

System Integrator shall required to survey before the submission of the commercials. All the System Integrators shall conduct Site-survey of all the project locations followed by the preparation & submission of Bid. The survey shall include the details of the location positioning of new building for data Centre and all prerequisite for final Solution for establishment of the Data Centre

System Integrator must perform the detailed assessment of the business requirements and IT Solution requirements as mentioned in this DPR. Based on the understanding and its own individual assessment, System Integrator shall develop & finalize the System Requirement Specifications (SRS) in consultation with OCAC/OSDC and its representatives. While doing so, System Integrator at least is expected to do following:

1. System Integrator shall conduct a detailed survey and prepare a gap analysis report, detailed survey report of the physical and field infrastructure requirements. System Integrator shall duly assist the department in preparing an action plan to address the gaps.
2. System Integrator shall study and revalidate the requirements given in the DPR with OCAC/OSDC and submit as an exhaustive FRS document. System Integrator shall develop the FRS and SRS documents.
3. System Integrator shall develop and follow standardized template for requirements capturing and system documentation.
4. System Integrator must maintain traceability matrix from SRS stage for the entire implementation.
5. System Integrator must get the sign off from user groups formed by OCAC/OSDC.
6. For all the discussions with OCAC/OSDC team, System Integrator shall be required to be present at OCAC/OSDC office with the requisite team members.
7. All existing road signs which are likely to be affected by the works are to be carefully taken down and restored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with OCAC/OSDC guidelines. Road signs, street name plate, etc. damaged by System Integrator during their operation shall be repaired or replaced by System Integrator at no additional cost.

8.2.3. Design Phase

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

System Integrator should consider to development of solution considering disabled friendly solution to extend possibilities.

8.2.4. Development Phase

System Integrator shall carefully consider the scope of work and provide a solution that best meets the project’s requirements. Considering the scope set in this DPR, System Integrator shall carefully consider the solutions it proposes and explicitly mention the same in the technical proposal. The implementation of the application software will follow the procedure mentioned below:

1. Software Products (Configuration and Customization): In case System Integrator proposes software products the following need to be adhered:
   a) System Integrator will be responsible for supplying the application and licenses of related

software products and installing the same so as to meet project requirements.

b) System Integrator shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.

c) System Integrator shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. System Integrator shall report any exceptions to license terms and conditions at the right time to OCAC/OSDC. However, the responsibility of license compliance solely lies with System Integrator. Any financial penalty imposed on OCAC/OSDC during the contract period due to license non-compliance shall be borne by System Integrator.

d) As per requirement of complex solution implementation System Integrator has to put requirement that OEM own resource &System Integrator best technical resources are deployed in this project.

2. OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with Customer to meet their business requirements.

3. System Integrator shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, System Integrator shall supply:

   a) Software & licenses.

   b) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.

4. 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/OSDC regularly:

   1 Functional Requirement Specification (FRS)

   2 High level design of whole system

   3 Low Level design for whole system

   4 System Requirements Specifications (SRS)

   5 Any other explanatory notes about system

   6 Traceability matrix

   7 RACI Matrix (Responsible, Accountable, Consulted and Informed)

   8 Technical and product related manuals

   9 Installation guides

10 User manuals

11 System administrator manuals

12 Toolkit guides and troubleshooting guides.

13 Other documents as prescribed by OCAC/OSDC

14 Quality assurance procedures

15 Change management histories

16 Version control data

17 SOPs, procedures, policies, processes, etc.

18 Developed for OCAC/OSDC Programs:

a) Entire source codes as applicable

b) All programs must have explanatory notes for understanding.

c) Version control mechanism

d) All old versions to be maintained.

e) Test Environment:

f) Detailed Test methodology document

g) Module level testing

h) Overall System Testing

i) Acceptance test cases

(These documents need to be updated after each phase of project and to be maintained during entire project duration. The entire documentation will be the property of OCAC/OSDC.)

8.2.5.Supply/ Installation

The selected System Integrator would be required to undertake all the necessary work required towards completion of IT infrastructure for SDC.

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 OSDC 2.0.

Necessary clearances as would be required shall be arranged by the selected System Integrator only.

8.2.6.Integration Phase

System Integrator is required to provide open APIs for integration with third party applications in data centers. SI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed / customized and the solution. The testing should be comprehensive and should be done at each stage of development and implementation to enable OCAC/OSDC for better decision management and planning.

8.3. Testing and 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/OSDC will review. Once OCAC/OSDC provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by OCAC/OSDC 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.

The following table depicts the details for the various kinds of testing envisaged for the project:

Type of Testing	Responsibility	Scope of Work
System Testing	✓ SI	▪ SI to perform System testing. ▪ SI to prepare test plan and test cases and maintain it. OCAC/OSDC may request SI to share the test cases and results. ▪ Should be performed through manual as well as automated methods. ▪ Automation testing tools to be provided by SI. OCAC/OSDC doesn’t intend to own these tools
Integration Testing	✓ SI	▪ SI to perform Integration testing. ▪ SI to prepare and share with OCAC/OSDC the Integration test plans and test cases. ▪ SI to perform Integration testing as per the approved plan. ▪ Integration testing to be performed through manual as well as automated methods. ▪ Automation testing tools to be provided by SI

Type of Testing	Responsibility	Scope of Work
Performance and Load Testing	✓ SI ✓ OCAC/OSDC / Third Party Auditor (to monitor the performance testing)	▪ SI to do performance and load testing. ▪ Various performance parameters such as transaction response time, throughput, and page loading time should be taken into account. ▪ Load and stress testing of the Project to be performed on business transaction volume ▪ Test cases and test results to be shared with OCAC/OSDC ▪ Performance testing to be carried out in the exact same architecture that would be set up for production ▪ SI need to use performance and load testing tool for testing. OCAC/OSDC doesn't intend to own these tools ▪ OCAC/OSDC if required could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by OCAC/OSDC
Security Testing (including Penetration and Vulnerability testing)	✓ SI ✓ OCAC/OSDC / Third Party Auditor (to monitor the security testing)	▪ Solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data center (s), security monitoring system deployed by SI ▪ Solution shall pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure. ▪ Security testing to be carried out in the exact same environment/architecture that would be set up for production. ▪ Security test report and test cases should be shared with OCAC/OSDC ▪ Testing tools if required, to be provided by SI. ▪ During O&M phase, penetration testing to be conducted on a yearly basis and vulnerability assessment to be conducted on half-yearly basis.

Type of Testing	Responsibility	Scope of Work
		▪ OCAC/OSDC will also involve third party auditors to perform the audit/review/monitor the security testing carried out by SI. Cost for such auditors to be paid by OCAC/OSDC
User Acceptance Testing of Project	✓ OCAC/OSDC or OCAC/OSDC appointed third party auditor	▪ OCAC/OSDC appointed third party auditor/consultant to perform User Acceptance Testing ▪ SI to prepare User Acceptance Testing test cases. ▪ UAT to be carried out in the exact same environment/architecture that would be set up for production. ▪ SI should fix bugs and issues raised during UAT and get approval on the fixes from OCAC/OSDC /third party auditor before production deployment. ▪ Changes in the application as an outcome of UAT shall not be considered as Change Request. SI has to rectify the observations.

Note:

a. System Integrator needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by SI for testing in its technical proposal. OCAC/OSDC does not intend to own the tools.

b. SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. SI must ensure deployment of necessary resources and tools during the testing phases. SI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of SI to ensure that the product delivered by SI meets all the requirements specified in the RFP. SI shall take remedial action based on the outcome of the tests.

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

d. All the Third-Party Auditors (TPA) as mentioned above will be appointed and paid by OCAC/OSDC directly. All tools/environment required for testing shall be provided by SI.

e. STQC/Other agencies appointed by OCAC/OSDC shall perform the role of TPA. SI needs to engage with the TPA at the requirement formulation stage itself. This is important so that unnecessary re-work is avoided, and the audit is completed in time. The audit needs to be completed before Go-Live of different phases. SI needs to prepare and provide all requisite information/documents to third party auditor and ensure that there is no delay in the overall schedule.

f. The cost of rectification of non-compliances shall be borne by SI.

g. Commissioning shall involve the completion of the Data Centre IT infrastructure including supply and installation of the required IT components and making the Data Centre IT Services available to OCAC for carrying out live Operations and getting the acceptance of the same from the OCAC. Testing and Commissioning shall be carried out before the commencement of Operations. It should be noted that Successfully System Integrator has to arrange all the necessary equipment's / tools / other resources / manpower / power etc. which are required for carrying out such testing of the OSDC. The cost of such shall be borne by the System Integrator itself.

h. After successful completion of Building construction, SI shall inform OCAC about the same and submit a report as work has been completed as per the standard and specification mentioned in the DPR.

8.3.1. Acceptance Testing Phase

The OCAC/OSDC shall review and finalize the detailed acceptance test plan proposed by the SI. The OCAC/OSDC would also conduct audit of the process, plan and results of the Acceptance Test carried out by the SI for IT components. If required OCAC/OSDC may carry out the testing from the third party. The OCAC/OSDC would issue certification of completion for which OCAC/OSDC shall verify availability of all the defined services as per the contract signed between the SI and OCAC/OSDC. The SI shall be required to demonstrate all the services, features, functionalities as mentioned in the agreement.

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

8.3.2. Partial Acceptance Testing

Partial Acceptance Test shall involve scrutiny of documents for various IT components to verify if the specifications conform to the technical and functional requirements mentioned in the Tender and subsequent corrigendum, if any. OCAC/OSDC reserves right to conduct physical inspection of the equipment delivered to ensure that they arrive atheists in good condition and are free from physical damage and incomplete shipments and shall return the products to the supplier at the supplier's expenses if required quality is not maintained. Physical inspection of hardware will also include physical checking and counting of the delivered equipment in presence of the successful SI. This equipment will only be acceptable as correct when each received item corresponds with the checklist that will be prepared by the successful SI prior to shipment. Any short falls in terms of number of items received may render the delivered equipment incomplete.

8.3.3.Final Acceptance Testing

The final acceptance shall cover 100% of the Connected OCAC/OSDC Project, after successful testing by the OCAC/OSDC. The Final Acceptance Test Certificate (FAT) shall be issued by the OCAC/OSDC to the SI.

Prerequisite for carrying out FAT activity:

1. Detailed test plan shall be developed by the SI and approved by OCAC/OSDC. This shall be submitted by SI before FAT activity to be carried out.
2. All documentation related to Project and relevant acceptance test document Should be completed & submitted before the final acceptance test to the OCAC/OSDC.
3. The training requirements as mentioned should be completed before the final acceptance test.
4. For IT equipment, software manuals / brochures / Data Sheets / CD /DVD/media for all the Project supplied components should be submitted to the OCAC/OSDC.

The FAT shall include the following:

1. All hardware and software items must be installed at respective it's as per the specification.
2. Availability of all the defined services shall be verified.
3. The SI shall be required to demonstrate all the features/facilities/functionalities as mentioned in the RFP.
4. The SI shall arrange the test equipment required for performance verification and will also provide documented test results.
5. The SI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by OCAC/OSDC.

Any delay by the SI in the Final Acceptance Testing shall render him liable to the imposition of appropriate penalties. However, delays identified beyond the control of SI shall be considered appropriately and as per mutual agreement between OCAC/OSDC and SI.

8.3.4.System Documents and User Manuals

The SI shall provide documentation which follows the ITIL (Information Technology Infrastructure Library) standards or IEEE/ISO Acceptable Documentation Standards. This documentation should be submitted as the project undergoes various stages of implementation and provide all traceability documentation on changes made on the IT components during the course of the implementation of the solution. Indicative list of documents includes:

1. **Project Commencement:** Project Plan should provide micro level activities with milestones & deadlines.
2. **Delivery of material:** Original manuals from OEMs.
3. **Training:** Training material will be provided which will include the presentations used for training sandals and other required relevant documents for the topics being covered.
4. **Process Documentation:** The SI shall be responsible for preparing process documentation related to the operation and maintenance of each component of the Project. The prepared process document shall be formally signed off by OCAC/OSDC before completion of final acceptance test.
5. The SI shall document all the installation and commissioning procedures and provide the same to the OCAC/OSDC within one week of the commissioning of Project.
6. The SI shall submit a complete set of Single Line diagrams, a complete cabling system layout (as installed), including cable routing, telecommunication closet sand telecommunication outlet/connector designations. The layout shall detail locations of all components and indicate all wiring pathways.
7. Manuals for configuring switches, routers etc. shall be provided by the selected SI.

The SI shall be responsible for documenting the configuration of all devices and keeping backup of all configuration files, so as to enable quick recovery in case of failure of devices.

8.4. Pilot Deployment Phase

1. SI shall conduct Pilot deployment and testing for meeting OCAC/OSDC’s business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. SI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on OCAC/OSDC’s feedback for incorporating changes as required and appropriate, SI shall train staff involved in the Pilot implementation.
2. Pilot shall be demonstrated to the OCAC/OSDC’s representatives. If for any reason the pilot is found to be incomplete, these will be communicated to the SI in writing on the lapses that need to be made good. A one-time extension will be provided to the SI for making good on the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to Client.

8.4.1.Go-Live Preparedness and Go-Live

1. SI shall prepare and agree with OCAC/OSDC, the detailed plan for Go-Live (in-line with OCAC/OSDC's implementation plan as mentioned in RFP).
2. SI shall define and agree with OCAC/OSDC, the criteria for Go-Live.
3. SI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.
4. 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/OSDC team on the same.
5. Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

8.4.2.Handholding and Training Phase

In order to strengthen the staff, structured capacity building shall be undertaken for identified resources of OCAC/OSDC, Municipal Corporation, and stakeholder departments. It is important to understand the training needs to be provided to each and every staff personnel of NOC Center, Data center and ICCC. These officers shall be handling emergency situations with very minimal turnaround time. The actual number of trainees will be provided at design stage.

6. SI shall prepare and submit detailed Training Plan and Training Manuals to OCAC/OSDC for review and approval.
7. 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.
8. 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.
9. Types of Trainings: Following training needs is identified for all the project stakeholders:

8.4.2.1. Administrative Training

- ✓ System Administration Helpdesk, BMS Administration etc.
- ✓ Master trainer assistance and handling helpdesk requests etc.

8.4.2.2. Senior Management Training

- ✓ Usage of all the proposed systems for monitoring, tracking and reporting,
- ✓ MIS reports, accessing various exception reports

8.4.2.3. Post-Implementation Training

- ✓ Refresher Trainings for senior officials
- ✓ Functional/Operational training and IT basics for new operators

- ✓ Refresher courses on System Administration
- ✓ Change Management programs.

8.5. Operations and Maintenance Phase

System Integrator will operate and maintain all the components of the Data center, City Surveillance and City fiber network for a period of five (5) years after Go-Live date. During O&M phase, SI shall ensure that service levels are monitored on a continuous basis; service levels are met and are reported to OCAC/OSDC. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the System only after proper induction procedures are followed including hardening and security testing. SI needs to implement suitable Performance Improvement Process (PIP) in the project.

8.5.1.Applications Support and Maintenance Phase

Application support includes, but not limited to monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change requests etc. The System Integrator shall keep the application software in good working order. Perform changes and upgrades to applications as requested by the OCAC/OSDC team.

8.5.2.Annual Technology Support

SI shall be responsible for arranging for annual technology support for the OEM products to OCAC/OSDC provided by respective OEMs during the entire O&M phase.

8.5.3.Application Software Maintenance

i. SI shall provide unlimited support through onsite team/telephone/Fax/E-mail/Video Conferencing/installation visit as required.

ii. SI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the SI (vis-à-vis the FRS, BRS and SRS signed off) at no additional cost during the O&M phase.

iii. All patches and upgrades from OEMs shall be implemented by the SI ensuring customization done in the solution as per the OCAC/OSDC requirements are applied. A technical upgrade of the installation to the new version, as and when required, shall be done by the SI. Any version upgrade of the software / tool / appliance by SI to be done after taking prior approval of OCAC/OSDC and after submitting impact assessment of such upgrade.

iv. Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the SI to ensure that the changes implemented in the system meets the specified requirements and doesn’t impact any other function of the system. Release management for application software will also require OCAC/OSDC’s approval. A detailed process in this regard will be finalized by SI in consultation with OCAC/OSDC.

v. In case of critical security patches/alerts, the SI shall inform about the same immediately along with his recommendations. The report shall contain SI’s recommendations on update/upgrade, benefits, impact analysis etc. The SI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, SI will carry it out free of cost by following defined process.

8.5.4.Problem identification and Resolution

i. Errors and bugs that persist for a long time, impact a wider range of users and is difficult to resolve becomes a problem. SI shall identify and resolve all the application problems in the identified solution (e.g. system malfunctions, performance problems and data corruption etc.).

ii. Monthly reports on problem identified and resolved would be submitted to OCAC/OSDC along with the recommended resolution.

8.5.5.Maintain configuration information.

SI shall maintain version control and configuration information for application software and any system documentation.

8.5.6.Maintain System documentation.

- High level design of whole system
- Low Level design for whole system / Module design level
- System requirements Specifications (SRS)
- Any other explanatory notes about system
- Traceability matrix
- Compilation environment

SI shall also ensure updating of documentation of software system ensuring that:

- Source code is documented.
- Functional specifications are documented.
- Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS, in accordance with the defined standards.
- User manuals and training manuals are updated to reflect on-going.
- changes/enhancements
- Standard practices are adopted and followed in respect of version control and management.

8.5.7.Patch Management

The System Integrator will be required to provide services related to Patch Management. This will help in the evaluation of threats posed by known vulnerabilities and assign a risk factor to them. The patch management solution should be executed efficiently for all kinds of environments like for operating systems and Databases.

8.5.8.ICT Infrastructure Support and Maintenance

ICT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related ICT infra required for running and operating the envisaged system. SI shall define, develop, implement and adhere to IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services defined and managed as part of this project.

8.6. Maintenance of ICT Infrastructure at the DC

8.7. Management of DC

The selected System Integrator will provide 24 x 7 x 365 operating and maintaining services for a period of 5 years from the date of Go Live for OSDC 2.0. SI needs to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICT infrastructure deployed at DC. All resources deployed in the project should be employees of SI and be Indian citizens. All the required resources proposed for the project need to be dedicated to the project. Any change in the team once deployed will require approval from OCAC/OSDC. It is expected that resources have a proven track record and reliability. Considering the criticality of the project, OCAC/OSDC 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/OSDC and keep the same updated. A detailed process in this regard will be finalized between OCAC/OSDC 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 OCAC/OSDC on a monthly basis. OCAC/OSDC 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 OCAC/OSDC. SI shall comply with this.

The scope of work for infrastructure and maintenance includes the following:

The scope of work during the operations phase is divided into following areas which are listed below:

- **a.** System Administration, Maintenance and Management Services
- **b.** Network Management Services
- **c.** Server and Storage Administration and Management Services
- **d.** Security Administration and Management Services
- **e.** Physical security services
- **f.** Backup & Restore Services
- **g.** Helpdesk Services
- **h.** Database Management
- **i.** Preventive Maintenance Services
- **j.** Corrective Maintenance Services

k. Asset Management Services

l. Configuration/ Reconfiguration Management Services

m. Vendor Management Services

n. EMS/NMS or other system

o. Threat Management

p. Certifications

q. Patch Release Update management (patch update for all software components possible and must give a report every fortnight to OCAC)

r. DC operations to be in compliance with industry leading ITSM frameworks like ITIL,

s. ISO 20000 & ISO 27001

t. Ensure compliance to relevant SLA's

u. 24x7 monitoring & management of availability & security of the infrastructure and assets.

v. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process.

w. Ensure overall security – ensure installation and management of every security component at every layer including physical security.

x. Prepare documentation/policies required for certifications included in the scope of work.

y. Preventive maintenance plan for every quarter

z. Performance tuning of system as required.

aa. Design and maintain Policies and Standard Operating Procedures

bb. User access management

cc. Other activities as defined/to meet the project objectives.

dd. Updation of all Documentation.

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.

8.7.1.System Maintenance and Management

a. SI shall be responsible for tasks including but not limited to setting up servers, 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 the SI may also be reviewed by OCAC/OSDC.

b. SI shall provision skilled and experienced manpower resources to administer and manage the entire system at the Data Center.

c. 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.

d. SI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.

e. SI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with OCAC/OSDC and based on the industry best practices/frameworks. SI shall also create and maintain adequate documentation/checklists for the same.

f. 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 OCAC/OSDC on need basis.

g. SI shall implement a password change mechanism in accordance with the security policy formulated in discussion with OCAC/OSDC and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.

h. The administrators shall also be required to have experience in the latest technologies so as to provision the existing and applicable infrastructure on a requirement-based scenario.

8.7.2.System Administration

1) 24*7*365 monitoring and management of the servers in the DC.

2) 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 the SI may be reviewed by OCAC/OSDC.

3) 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.

4) 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.

5) SI shall also be responsible for proactive monitoring of the applications hosted.

6) SI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability to OCAC/OSDC at all times.

7) OCAC/OSDC 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 CERT-In Guidelines so as to ensure their alignment with the practices followed.

8) 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.

9) 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.

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

11) 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.

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

13) 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.

14) The administrators will also be required to have experience in the latest technologies so as to provision the existing and applicable infrastructure on a requirement-based scenario.

8.7.3.Storage Administration

i. 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 the SI may be reviewed by OCAC/OSDC.

ii. 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.

iii. 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.

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

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

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

vii. To facilitate scalability of solution wherever required.

viii. The administrators will also be required to have experience in technologies such as virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement-based scenario.

8.7.4.Database Administration

i. SI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

ii. SI shall be responsible for performing physical administrative functions such as reorganizing the database to improve performance.

iii. SI shall be responsible for tuning the database, ensuring the integrity of the data and configuring the data dictionary.

iv. SI will follow guidelines issued by OCAC/OSDC in this regard from time to time including access of database by system administrators and guidelines relating to security of database.

v. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.

vi. 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.

vii. System Integrator 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.

viii. System Integrator shall periodically perform configuration checks and fine-tune the databases with respect to performance and proactive identification of potential problems.

ix. System Integrator shall provide performance monitoring, Maintenance and tuning of the databases on a regular basis as well as proactive health check-ups.

x. System Integrator shall manage database upgrade, patch upgrade, patches, and updates as and when required with planned minimal downtime.

xi. System Integrator shall provide database performance and health reports to the OCAC as per standards.

xii. System Integrator shall assign rights on database for different users as per the requirement with necessary approval from OCAC or concern authority.

xiii. System Integrator shall upload / create/alter users and assign privileges and Roles as per the requirement with necessary approval from OCAC or concern authority.

xiv. System Integrator shall create logical objects/procedures/triggers/functions/packages in the database on the request of designer/developer of the applications.

xv. System Integrator shall be responsible for taking database backups, restoration and recovery of Database as per the policy.

xvi. The backup policy would be framed by the SYSTEM INTEGRATOR keeping in view of severity of different databases and MTTR. The policy would be approved by the Tendering Authority and gradually be updated as per requirements.

xvii. System Integrator shall be responsible to maintain optimum utilization of all the equipment’s w.r.t. database operations and keeping close watch on optimum performance of Hardware/OS/Network software/processes/database objects with detecting contention, wait state and queue of jobs on the equipment’s/memory objects/ processes/ Network/ I/O/ storage/concurrent load on the devices, etc. and implementing necessary measures to rectify the issues. A performance matrix has to be provided by the System Integrator to the Tendering Authority on monthly basic and as and when required.

xviii. System Integrator shall implement monitoring of uses of devices/objects/users as and when required.

xix. System Integrator shall be responsible for implementing Database Audit of devices/ objects/ transactions/ users to identify malicious/suspected activities as and when required through database tools or writing its own scripts.

8.7.5.Backup/Restore/Archival

i. SI shall be responsible for implementation of backup & archival policies as finalized with

OCAC/OSDC. The SI is responsible for getting acquainted with the storage policies of OCAC/OSDC before installation and configuration. It should be noted that the activities performed by the SI may be reviewed by OCAC/OSDC.

ii. 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.

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

iv. 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.

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

vi. SI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre(s).

8.7.6. Network monitoring

i. SI 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 the SI may be reviewed by OCAC/OSDC.

ii. SI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.

iii. SI shall also be responsible for break fix maintenance of the LAN cabling within DC/ICCC etc.

iv. SI shall also provide network related support and will coordinate with connectivity service providers of OCAC/OSDC/other agencies who are terminating their network at the DC/ICCC for access of system.

8.7.7. Security Management

i. Performing security services on the components that are part of the OCAC/OSDC environment as per security policy finalized with OCAC/OSDC

ii. IT Security Administration – Manage and monitor safety of information/data

iii. Reporting security incidents and resolution of the same

iv. Proactively monitor, manage, maintain & administer all security devices and update engine, signatures, and patterns as applicable.

v. Managing and monitoring of anti-virus, anti-malware, phishing and malware for managed resources.

vi. Ensuring 100 percent antivirus coverage with patterns not old more than period agreed on any given system

vii. Ensuring APT (Advanced Threat Protection)

viii. Reporting security incidents and co-ordinate resolution

ix. Monitoring centralized pattern distribution (live update) and scan for deficiencies

x. Maintaining secure domain policies

xi. Secured IPsec/SSL/TLS based virtual private network (VPN) management

xii. Performing firewall management and review of policies on at-least quarterly basis during first year of O&M and then after at-least on half-yearly basis

xiii. Providing WAF (Web Application Firewall)

xiv. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/ software and alerting OCAC/OSDC as appropriate

xv. Performing patch management using software distribution tool for all security applications including content management system, antivirus and VPN

xvi. Providing root cause analysis for all defined problems including hacking attempts

xvii. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to OCAC/OSDC

xviii. Maintaining documentation of security component details including architecture diagram, policies and configurations

xix. Performing periodic review of security configurations for inconsistencies and redundancies against security policy

xx. Performing periodic review of security policy and suggest improvements

xxi. 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

xxii. Policy management (firewall users, rules, hosts, access controls, daily adaptations)

xxiii. Modifying security policy, routing table and protocols

xxiv. Performing zone management (DMZ)

xxv. Sensitizing users to security issues through regular updates or alerts – periodic updates/ Help OCAC/OSDC issuance of mailers in this regard

xxvi. Performing capacity management of security resources to meet business needs

xxvii. Rapidly resolving every incident/problem within mutually agreed timelines

xxviii. Testing and implementation of patches and upgrades

xxix. Network/device hardening procedure as per security guidelines from OCAC/OSDC

xxx. Implementing and maintaining security rules

xxxi. Performing any other day-to-day administration and support activities

8.7.8.Other Activities

i. SI shall ensure that it prepares configuration manual for OS, appliances, middleware, all tool, servers/devices and all equipment's and the same need to be submitted to OCAC/OSDC, any changes in the configuration manual need to be approved by OCAC/OSDC. Configuration manual to be updated periodically.

ii. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.

iii. If the Operating System or additional copies of Operating System are required to be installed/reinstalled/un-installed, the same should be done as part of O&M.

iv. SI should carry out any requisite adjustments/changes in the configuration for implementing different versions of Application Software.

v. Updates/Upgrades/New releases/new versions: The SSI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems as required. The SI should provide free upgrades, updates & patches of the software and tools to OCAC/OSDC as and when released by OEM.

vi. SI shall provide patches to the software as part of IT infrastructure, operating system, databases and other applications.

vii. Software License Management: The SI shall provide for software license management and control. SI shall maintain data regarding entitlement for software updates, enhancements, refreshes, replacements, and maintenance.

viii. Data backup/recovery management services

ix. All other activities required to meet the project requirements and service levels.

x. It is responsibility of the SI to scale up the Operations & Maintenance (O&M) team as and when required to ensure smooth project execution throughout the project duration.

8.7.9.Cloud Services

The minimum specified scope of work to be undertaken by the SYSTEM INTEGRATOR for supply, installation, Commissioning, testing, Training, knowledge transfer and Support for OSDC Cloud Enablement Infrastructure as mentioned below:

- Finalize the deployment architecture/layout with the OSDC/OCAC.
- Procure, supply, installation & commissioning of all the components & subcomponents including all necessary hardware & software as per the proposed solution. The System Integrator has to ensure that the solution works as desired and the System Integrator is also responsible for supplying and install any other components that is inadvertently not in the BoM but required for the overall solution to work.
- The System Integrator shall be responsible for integrating the proposed solution with the infrastructure and solutions present in the OSDC. The System Integrator should ensure that the Cloud solution should be able to integrate with the security devices like, firewall, IPS such that entire functionality of these devices can be used to monitor security features and provide alerts, alarms, reports, proactive actions on virtual environment similar to provide in physical environment. The System Integrator should also ensure that the cloud solution should be able to integrate with the EMS/or any other related tool so that entire functionality of these tools can be extended to the virtual environment similar to physical.
- The successful System Integrator shall handover working solution to the State and thereafter provides all the necessary support for the project period to the OSDC for operating the solution as per the uptime requirement of the OSDC 2.0 (99.982%) The system designed by the System Integrator should be in line with the SLAs in place.

The implementation shall also include comprehensive training of the OSDC. Comprehensive training shall hold key to successful operations and maintenance; hence the System Integrator is required to undertake robust training.

8.7.10. Compliance to SLA

System Integrator (SI) 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 OCAC/OSDC.

1) SI shall ensure compliance to uptime and performance requirements of project solution as indicated in the SLA and any upgrades/major changes to the Data Center shall be accordingly planned by SI for ensuring the SLA requirements.

2) SI shall be responsible for measurement of the SLAs at the Data center level as well as at the user level with the help of the enterprise monitoring tool on a periodic basis.

3) Reports for SLA measurement must be produced by OCAC/OSDC officials as per the project requirements.

8.7.11. Warranty support

10.7.1 SI shall provide comprehensive and on-site warranty for 5 years from the date of Go-Live for the infrastructure deployed on the project. SI needs to have OEM support for these components and documentation in this regard need to be submitted to OCAC/OSDC on annual basis.

10.7.2 SI shall provide the comprehensive & onsite manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. SI 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.

10.7.3 SI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

10.7.4 SI 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 SI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the OCAC/OSDC in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.

10.7.5 During the warranty period SI shall maintain the systems and repair/replace at the installed site, at no charge to OCAC/OSDC, all defective components that are brought to the SI's notice.

10.7.6 The SI shall carry out Corrective Maintenance for maintenance/ troubleshooting of supplied hardware/ software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. The SI 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 OCAC/OSDC team as well.

10.7.7 SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

a. The SI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

i. 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.

ii. 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).

iii. The SI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of Data Center.

8.7.12. Factory Testing

Success SI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.SI has to provide MAF (OEM certificate) where applicable.

8.7.13. Compliance to Standards & Certifications

a. For a large and complex set up such as the Project, it is imperative that the highest standards applicable are adhered to. In this context, SI will ensure that the entire Project is developed in compliance with the applicable standards.

b. During project duration, SI will ensure adherence to prescribed standards as provided below:

#	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Cloud Certification	ISO 27017
5.	Project Documentation	IEEE/ISO (where applicable) specifications for documentation

c. Apart from the above SI need to ensure compliance of the project with Government of India IT security guidelines including provisions of:

- The Information Technology Act, 2000" and amendments thereof and
- Guidelines and advisories for information security published by Cert-In/MeitY (Government of India)

issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

d. While writing the source code for application modules SI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:

- The name of the module
- The date when module was created.
- A description of what the module does
- A list of the calling arguments, their types, and brief explanations of what they do
- A list of required files and/or database tables needed by the module.
- Error codes/Exceptions
- Operating System (OS) specific assumptions
- A list of locally defined variables, their types, and how they are used.
- Modification history indicating who made modifications, when the modifications were made, and what was done.

e. Apart from the above SI needs to follow appropriate coding standards and guidelines inclusive of but not limited to the following while writing the source code.

- Proper and consistent indentation
- Inline comments
- Structured programming
- Meaningful variable names
- Appropriate spacing
- Declaration of variable names
- Meaningful error messages

8.7.14. Quality Audits

1) OCAC/OSDC, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. SI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with SI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.

2) SI should comply with all the technical and functional specifications provided in various sections in this RFP document.

8.8. Advisory & Guideline for System Integrator

System Integrator follows the MEITY Advisory Designing/Supplying/ Development and Implementation of Smart solutions in Data center Project.

a. System Integrator shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development).

b. The System Integrator shall adhere each product or technology should have quality certifications like ISO 9001/ ISO 20000/ISO 14001/ISO 27001 or equivalent.

c. System Integrator shall adhere the Advisory no- 87 issued by the Government of India and Ministry of Urban Development) for roll of Information and Communication Technology (ICT) in the development of smart infrastructure.

d. System Integrator shall adhere the Advisory no- 11 issued by the Government of India and Ministry of Urban Development) for Strategy for ensuring Universal Access IT systems to empower citizens with disability to access these systems with ease for development of Data Centre Software.

e. System Integrator shall adhere the Advisory of Exclusion for restrictions under rule 144 of the general finance rules (GFRS).

f. System Integrator shall adhere the Advisory no- 18 issued by the Government of India and Ministry of Urban Development) for (DPPIT) Department of Promotion Preference make in India order 2017(PP-MII).

g. Apart from the above the SI need to ensure compliance of the project with Government of India IT security guidelines including provisions of:

i) The Information Technology Act, 2000" and amendments thereof and

ii) Guidelines and advisories for information security published by Cert-In/Deity (Government of India) issued till the date of publishing of tender notice. Periodicchanges in these guidelines during project duration need to be complied with.

8.8.1.Another requirement for Project Implementation

- The successful System Integrator has to carry out the complete Procurement, Supply, installation and commissioning of required IT infrastructure at all the designated locations of the OSDC 2.0 as identified in the Bill of material. During this phase, the successful System Integrator has to submit stage-wise reports and it should be done strictly in accordance with the scope of work in the Tender document.

- The successful System Integrator is expected to adhere to all technical and non-functional specifications for IT Infrastructure. Any additional design guidelines as provided in the Tender document/ proposed solution document has to be achieved as per established delivery timelines.
- A detailed project plan for the implementation of OSDC 2.0 is to be provided during the Kick-off meeting. A work breaks down structure with all milestones for the entire commissioning timeline is to be provided by the successful System Integrator.
- The successful tenderer would be required to submit detailed Design documents with all necessary design drawings for all IT infrastructures and would be approved by the Steering Committee before actual execution of work.
- A supply schedule for all materials with make and model is to be prepared and submitted in line with the Work breakdown structure of the project plan.
- All materials are to be dispatched as per expected delivery timelines with no additional dispatch or delivery costs. Any deviation from the expected timelines of delivery is to be intimated in advance for appropriate actions and reason.
- The materials should be brand new and as per the tender specifications/requirements. System Integrator should take care of Insurance against the material loss.
- All components of OSDC 2.0 must support scalability with adequate licensing, accessories and modules to provide continuous growth to meet the requirements and demand of various departments.
- Stage wise reports encapsulating the details of the work executed for all IT components including Server, Storage, backup appliances, networks routing & switching, network security, and all necessary common infrastructure IT services as part of the scope.
- UAT test reports will be verified and approved by the Consultant following which the commissioning certificate will be issued by OCAC.
- All IT systems are to be installed and tested as per the tender and continuous status reports are to be submitted. Consultant and OCAC will participate in the active project management and monitoring of timelines to ensure adherence to delivering on schedule. Commissioning certificate will be issued by OCAC after completion of the project components as per scope of work.
- During installation/ uninstallation of any equipment, SI shall not cause any damage to government buildings/ premises/ property. However, if any damage occurs, the System Integrator shall restore it to the original state at his own cost up to the satisfaction of the GoO. Trenches, path/road-cutting etc. should be back-filled and restored to the original condition immediately after laying of the conduit/cable at no extra cost. SI shall also plug conduits and entrance holes where the cabling has been installed with suitable sealing material. The System Integrator shall lay all the cables power or networking with proper casing.

- During the implementation period, the System Integrator shall provide, on a weekly basis, the implementation progress report to the designated agency.
- The System Integrator shall perform the work in a conscientious manner as per the best industry practices and in compliance to the applicable regulatory norms. The System Integrator at his own cost shall obtain approvals required, if any.

8.8.2.Enterprise Management System (EMS)

The EMS system should provide for the regular monitoring, management and reporting of the ICT infrastructure of the Data Centre. It should be noted that the activities performed by the System Integrator would be under the supervision of OCAC. The EMS system must have the following features including but not limited to:

Following functionalities are desired by use of such EMS tools:

- Availability Monitoring, Management and Reporting.
- Performance Monitoring, Management and Reporting.
- Securing critical servers using Server based Access Control & recording user activity through audit logs.

To ensure that IT systems are delivered at the performance level envisaged, it is important that an effective monitoring and management system be put in place. It is thus proposed that approve Enterprise Management System (EMS) is to be proposed by the bidder for efficient management of the system, reporting, SLA monitoring and resolution of issues. Various key component soft he EMS to be implemented as part of this engagement are –

1. Network Monitoring System (NMS)
2. Server Performance Monitoring System
3. Centralize Helpdesk System

The solution should provide a unified web-based console which allows role based access to the users.

8.8.3.NMS (Network Monitoring System)

Solution should provide fault & performance management of the servers' ide infrastructure and should monitor IP\SNMP enabled devices like Routers, Switches, computers etc. Proposed Network Management shall also help monitor key KPI metrics like availability, in order to measure SLA's. Following are key functionalities that are required which will assist administrators to monitor network faults & performance degradations in order to reduce own times, increase availability and take proactive actions to remediate & restore network services:

a. The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map.

b. Proposed solution should provide customizable reporting interface to create custom reports for collected data.

c. The system must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.

d. The system should be able to clearly identify configuration changes and administrators should receive an alert in such cases.

e. The system should provide report on the uptime of various components monitored through the NMS with the input of date range.

8.8.4.Server Performance Monitoring System

- The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as par to this Project.
- The proposed tool must provide information about availability and performance for target server nodes.
- The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.

8.8.5.Centralized Helpdesk System

1. Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
2. System should also automatically create tickets based on alarm type. All incidences reported by EMS and NMS should be auto registered in the Help Desk with Ticket ID for all locations connected on this OFC network as well as other locations which are / will be connected through leased line / MPLS / Dark.
3. The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident via web interface for issues related to the project.
4. SI will do necessary coordination with his team in case of issue with OFC network or with the other service provider team for all customer complains / tickets for service interruption issues as per the instruction of OSDC/OCAC.

The outlined scope of work encompasses the comprehensive responsibilities to be undertaken by the bidder for the Design, Supply, Installation, Testing, Commissioning, Operations, and Maintenance of the proposed OSDC 2.0 in Bhubaneswar. The bidder is mandated to achieve an uptime exceeding 99.982% on a quarterly basis throughout a five-year period post Go-Live.

The specified work to be carried out by the bidder for establishing and managing the proposed Data Centre OSDC 2.0 is categorized as follows:

- Supply, install, test, and commission the IT infrastructure for OSDC 2.0 in Bhubaneswar.
- Perform data and application migration for a selected set of applications (five in total) from the existing State Data Centre to the new OSDC 2.0.
- Consider the Go-Live achieved post the successful integration and commissioning of the equipment supplied under SDC 2.0 with the existing SDC 1.0.
- Provide operations and maintenance services for the complete infrastructure at OSDC 2.0 in Bhubaneswar for a period of five years from the date of successful acceptance by OCAC.

Note: Bidders are required to submit proposals for these schedules in the same bid for combined evaluation purposes.

8.9. IT System Design Consideration

Supply, Installation, Testing, and Commissioning (SITC) of IT Infrastructure:

Moving ahead, the comprehensive scope of work in this phase includes, but is not limited to, the following:

OSDC 2.0 aims to establish a resilient infrastructure, empowering the Government of Odisha to deliver services efficiently to its stakeholders. The State Government envisions creating a highly secure, flexible, automated, and managed cloud service environment, deploying cutting-edge industry computing infrastructure to ensure the security, scalability, and availability of user department applications.

The goal is to provide a logically unified and shared infrastructure capable of rapidly responding to varied infrastructure requirements. This includes accommodating future technology enhancements, distributed applications, database applications running on bare metal, virtualized applications in multi-hypervisor environments, and on-demand cloud-based applications, each imposing distinct demands on infrastructure.

The Bidder is expected to provide all necessary installation equipment and tools required for the system installation. Installation, integration, and commissioning of active network equipment, as well as passive network components, shall be carried out in accordance with the approved deployment design, adhering to OEM guidelines and industry best practices. The system will undergo inspections at various stages, with strict adherence to local regulations and codes. The Bidder is obligated to follow Safety Regulations and practices, ensuring no damage to the existing server farm of OSDC, government buildings, or other premises. Any damage incurred must be promptly restored. Trenches and path-cutting activities will be back-filled and restored to their original condition immediately after conduit/cable laying. Conduits and entrance holes used for cabling installation shall be sealed with suitable materials.

The Bidder is tasked with establishing a centralized cloud environment to host multiple applications, ensuring simplified operations and enhanced application responsiveness for both new and existing virtualized and non-virtualized environments.

- Deliver IT as a service, starting with IaaS, PaaS, CaaS, SaaS, DaaS, etc.
- Provide responsive IT-based services to government/departments on demand at scale and anywhere.
- Ensure reliable user experience.

The IT infrastructure for OSDC 2.0 in Bhubaneswar necessitates various sets of IT components for running applications, with telecom racks provided by the Bidder. The Bidder is responsible for supplying, installing, configuring, testing, and maintaining the entire solution for a period of five years from the Go-Live date. The Bidder should propose a single solution in accordance with RFP specifications.

The following categories of components are expected to be supplied, installed, configured, and tested by the Bidder:

a. Computing Infrastructure, including Servers, Operating Systems, and Hypervisors.

b. Network Infrastructure, including Routers, Spine and Leaf switches, SDN Controller, etc.

c. Security Infrastructure, including Firewalls, HIPS, D-DOS, AAA, Anti-APT, DLP, etc.

d. Centralized Enterprise Management Solution, Patch Management, Antivirus, Cloud Management – Orchestration layer.

e. Implementation of an Enterprise-Class Storage Area Network, inclusive of an Enterprise-Class Storage System, SAN switches, Tape Library, etc.

f. The Go-Live phase will be deemed successful after the integration and commissioning of OSDC 2.0 with the existing SDC 1.0.

g. Provision of operation and maintenance services for a duration of 5 years from the Go-Live date.

While the above list serves as an indication, the Bidder is required to furnish an infrastructure that is scalable and incorporates cutting-edge technologies such as virtualization, cloud computing, orchestration, etc. The Bidder retains the flexibility to incorporate additional components deemed necessary for delivering a comprehensive solution. In proposing the solution, the Bidder should consider the following:

i. Ensure provision for all peripherals, accessories, sub-components necessary for the functionality and completeness of the solution, encompassing devices, equipment, accessories, software, licenses, tools, etc., aligned with the solution requirements.

ii. OCAC will not assume responsibility if the Bidder fails to provision any components, sub-components, assemblies, or sub-assemblies outlined in the bid response's bill of material. The Bidder is obligated to provide the necessary provisions at no additional cost and within the stipulated timeframe, adhering to OCAC's solution requirements.

iii. Implement a comprehensive 24x7x365 onsite support arrangement for a period of 5 years post Go-Live, involving all OEMs for respective IT components.

iv. Ensure that the equipment/components supplied are supported by respective OEMs for a minimum of 7 years from the bid submission date. In the event of de-support by the OEM for any reason, the Bidder must replace it with an equivalent or superior substitute, acceptable to OCAC, without incurring additional costs or impacting the solution's performance. Any components, subcomponents, assemblies, or sub-assemblies (e.g., server, storage, OS) required for the installation of EMS, Orchestration, backup, patch management, antivirus, or any other software/management software needed for IT infrastructure will be provided by the Bidder without additional cost.

Key Considerations for Designing the Odisha State Data Centre 2.0:

8.9.1.Scalability

- A scalable system efficiently handles increasing requests without compromising response time and throughput.
- The Data Centre must support both vertical (within one operating environment) and horizontal scalability (multiple systems collaborating in parallel).
- Adopting a modular design facilitates growth without major disruptions.
- All Data Centre components must support scalability for continuous growth and future demand.
- A scalable Data Centre should be easily expandable or upgradeable on demand.

8.9.2.High Availability

- Design for high availability anticipates system failures and configures systems to mask and recover from component or server failures with minimal application outage.
- Ensure all Data Centre components have adequate redundancy to ensure high availability of e-Governance applications and other services.
- The Bidder must provision for high availability for all Data Centre services.

- Application availability is the responsibility of the application owner, and the Bidder cannot be held responsible for application-related problems.

8.9.3.Interoperability

- The entire system/subsystem should be interoperable to support information flow and integration.
- Operating systems and storage technologies from various vendors should interact seamlessly.
- Support open architecture solutions allowing data to be ported to any system when required.

8.9.4.Manageability

- Design the SDC for efficient maintenance, ease of configuration, ongoing health monitoring, and failure detection.
- The SDC should match the growth of the environment, including infrastructure and government data.

8.9.5.Cyber Security

- Provide end-to-end security to protect applications, services, data, and infrastructure from intentional, unintentional, or malicious attacks or theft.
- Control and support attacks and theft using next-generation cybersecurity appliances.
- Ensure proper storage of system logs for at least 180 days for future analysis and forensics.

8.9.6.Integration of OSDC with SWAN

- Ensure seamless integration with SWAN, with OCAC responsible for provisioning connectivity.
- The SI should integrate the SWAN link from the existing Data Centre to the newly built Data Centre.
- Plan the termination of the SWAN link at the gateway level of the Data Centre.

8.9.7.IPv6 Readiness

- All hardware and software supplied under the tender should be IPv6 ready from day one.
- Ensure that specified performance meets IPv6 specifications, with components configured for both IPv6 and IPv4 from day one.

8.9.8.Cloud Services Provisioning

- The proposed Cloud solution should offer Infrastructure-as-a-Service and Platform-as-a-Service to various state line departments.
- The selected bidder is responsible for transitioning from the existing cloud service provider, migrating existing cloud setups, and integrating them into the new Data Centre.

- Coordinate with current and new cloud service providers for migration, integration, monitoring, and management of cloud services.

8.9.9.Inter-Intra Rack Connectivity

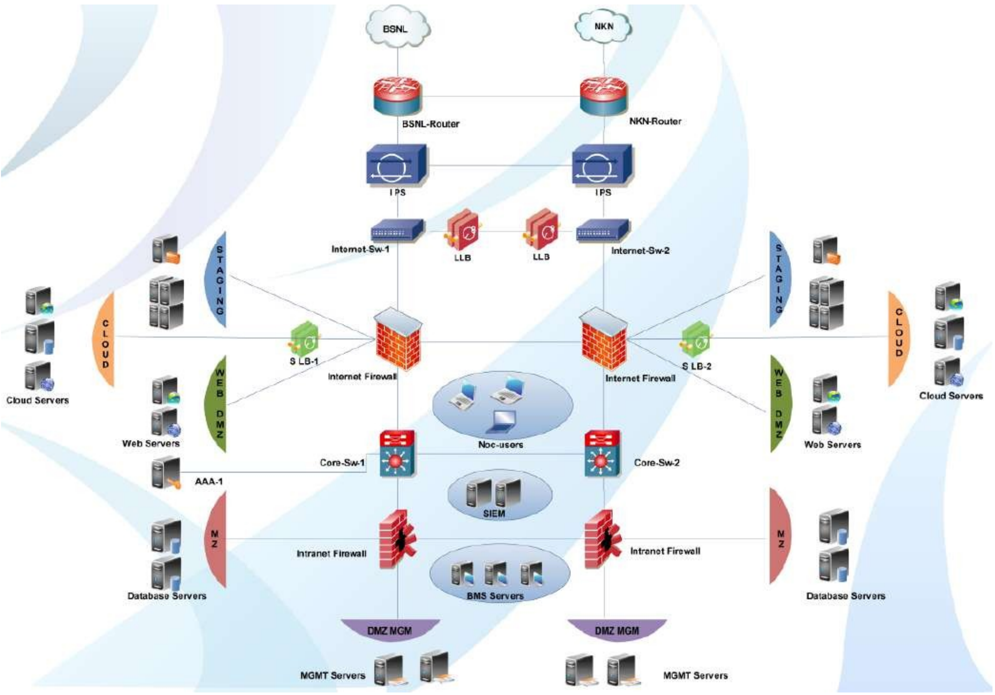
- Specify the connectivity requirements within racks, leaf switches, SAN switches, and server racks for both virtual and cloud environments.

8.9.10. Indicative Logical Schematic

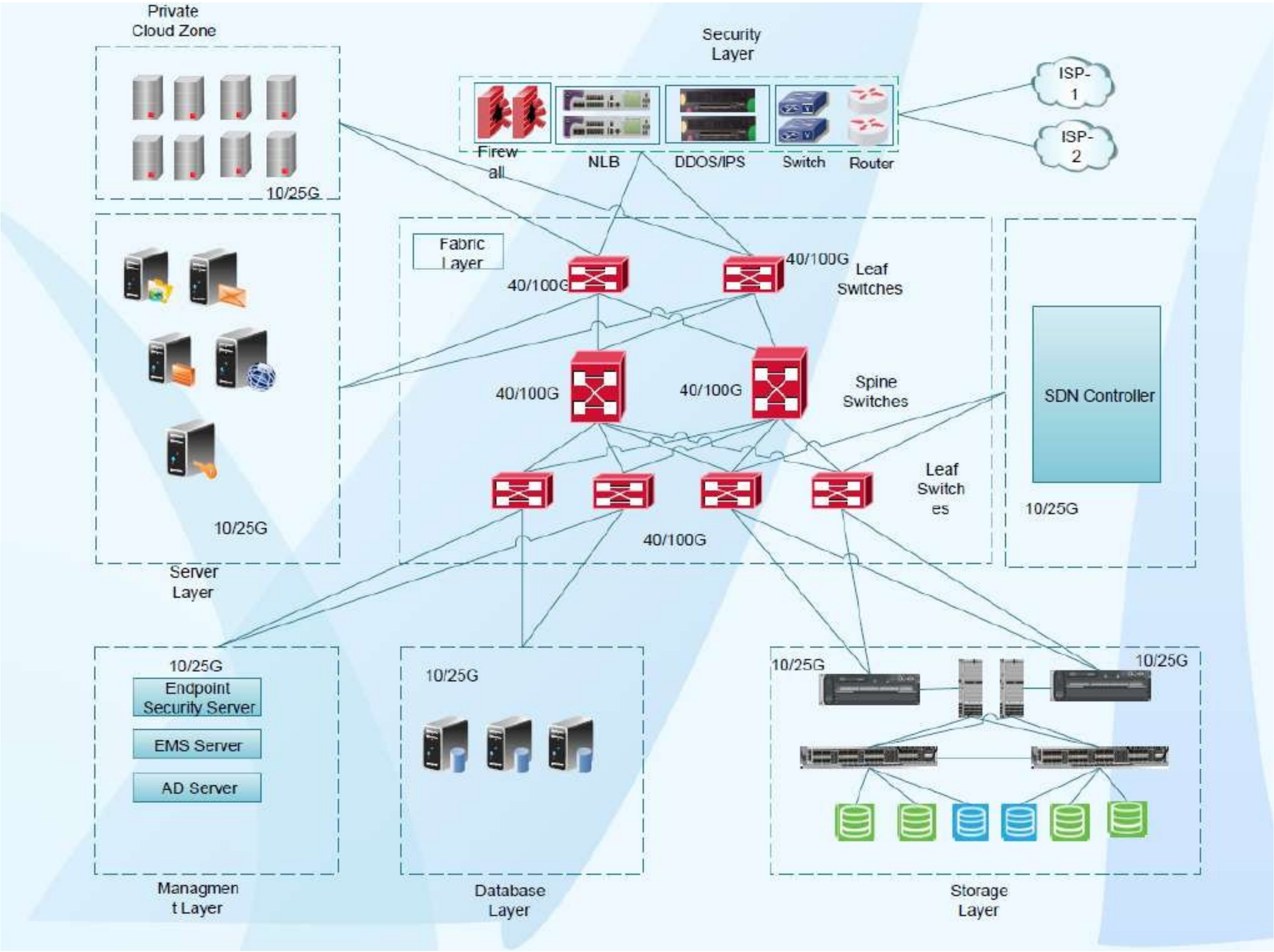
- Present an indicative schematic of the Data Centre design architecture, illustrating major IT components provisioned by the Bidder.
- Describe the compute environment, the approximate number of racks, and the common network/security infrastructure for both environments.

8.10. High Level Indicative Logical Diagram for OSDC 2.0

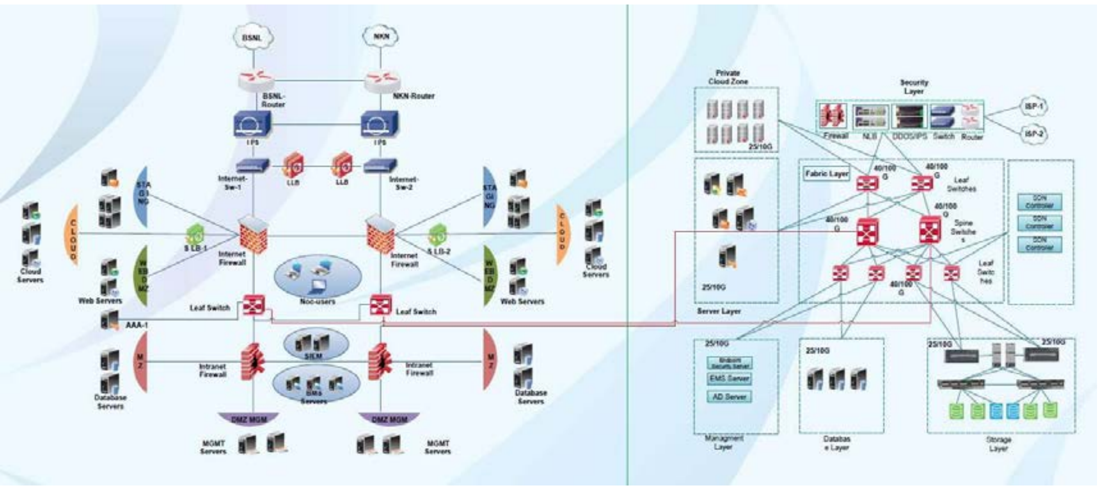
8.10.1. Existing Network Diagram of OSDC 1.0:



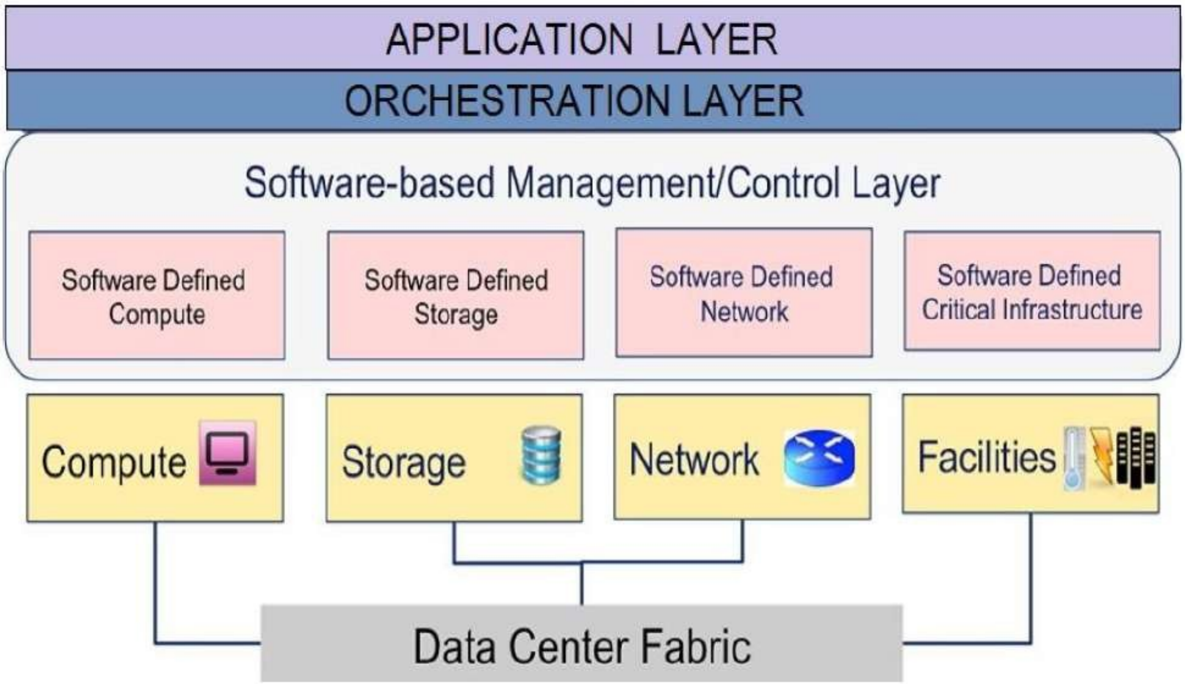
8.10.2. Proposed Indicative Network Diagram of OSDC 2.0



8.10.3. Proposed Integrated Network Diagram (Indicative)



8.10.4. Proposed Broad Architecture of the cloud enabled Data Centre



9. Detailed Functional Scope of Work

- The Bidder is mandated to embrace a fabric-based approach designed to support evolving industry demands comprehensively. This approach facilitates the concurrent operation of traditional enterprise applications and internally developed applications within a dynamically scalable network infrastructure. The Data Centre (DC) architecture should feature a Network fabric design employing the Spine & Leaf model to facilitate management automation, programmatically defined policies, and dynamic workloads for both Virtual and physical devices.

- The Next Generation OSDC 2.0 aims to meet OCAC's functional requirements as follows:

    a. Rapid Service Provisioning: Enable prompt availability of services, minimizing administrative efforts and bureaucratic obstacles. The predominant offerings would manifest as a Private Government cloud running on established Hypervisors.

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. Implement Software-Defined Networking (SDN) with Leaf and Spine architecture, ensuring better utilization of the switching fabric. Establish redundant dark fiber connections linking existing and proposed DCs.

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

d. SDN Solution: Deploy an SDN-ready infrastructure with Spine and Leaf switches supporting SDN capabilities like VXLAN/MP-BGP. Provide open scripting interface for configuring the entire fabric.

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

f. Virtualization: Integrate the proposed SDN solution with the virtualization platform, proposing a compatible Virtual Machine Manager.

g. Next-Generation Data Centre Security: Implement security architecture supporting network virtualization, Layer 4 through 7 virtual network service chaining, and unified security policies.

h. SAN Switching: Offer a highly predictable performance, scalable, and manageable SAN solution compatible with multi-protocol FC, and IP storage environments.

i. Storage Infrastructure: Provide centralized storage with flexible and secure configuration for shared data storage needs.

j. Structured Cabling: Design, lay, and test cabling for approximately 90 racks, ensuring end-to-end connectivity.

k. Enterprise Management System: Implement an EMS solution covering infrastructure performance, event consolidation, server and database performance management, network fault and performance management, and automation.

l. Cloud Infrastructure: Transform OSDC into a "Private Cloud" supporting IaaS, PaaS, SaaS, DbaaS, Bare Metal as a Service, and CaaS capabilities. Gradual migration of existing infrastructure and applications to OCAC cloud is envisioned.

The selected Bidder is tasked with supplying Hardware, Software, and services in accordance with the Schedule of Requirements and meeting the minimum functional and technical specifications outlined in the subsequent sections.

The design and implementation of the private Cloud, inclusive of underlying software components (virtualization, SDN, container, security, storage, etc.), shall be carried out by OEM professionals. Additionally, OEM-certified trainers are to provide training aligning with the SDC team's requirements, and an OEM resident engineer shall be deployed for the entire project period to offer comprehensive technical support regularly.

OCAC's strict requirement is the ability to maintain a common set of templates across all departments, aiming to minimize the creation and management of blueprints.

Key Points:

- The proposed solution should integrate under a single umbrella with the existing Government of Odisha (GoO) Cloud for enhanced management and operation.
- The solution should create customized workflows, aligning with IaaS, PaaS, SaaS, DbaaS, STaas, Backup as a Service, Bare Metal as a Service, and CaaS capabilities for SDC 2.0, as per defined functional requirements and services scope.
- The Bidder is responsible for supporting any required version/software/hardware upgrades and patch management throughout the entire contract period.
- The Bidder must supply OS, database, or other licenses required for Cloud management components.
- The solution should offer multi-tenant environment capabilities.

- Automation of IaaS, PaaS, SaaS, STaas, Backup as a Service, Bare Metal as a Service, and CaaS capabilities for SDC 2.0 without manual intervention is a prerequisite.
- The Cloud platform must support and manage cloud services across proposed hypervisors, heterogeneous compute, storage, and network environments.
- Auto-scaling capabilities should be configured to automatically create additional VMs with assigned network, security, and load balancing upon changes in utilization.
- Full automation should be achieved through integration from cloud portal, orchestration, virtualization, virtual network, security, and load balancing.
- The solution should support Open standards with enterprise support.
- Cloud operations layer integration with an automation layer providing proactive monitoring, alerts, management, capacity planning, and performance management is essential.
- The solution should monitor VM and Container utilization in a unified management console in an automated fashion.
- Automated security measures for micro-segmentation and zero-trust security, along with workload provisioning, must be supported.
- Integration of existing/new AD/LDAP with the cloud management platform is required.
- The solution should define roles, limit management scope based on various criteria, and automatically enforce network, security, storage, and configuration policies during cloud instance provisioning.
- Automated compute, network, and storage for containers, along with automated deployment of Container orchestration, networking, and security, must be provided.
- The Container-as-a-Service (CaaS) solution should include kernel-level security deployment, a built-in container scanner, integrated service mesh for microservices deployment, and capabilities for physical server deployment.
- Developer productivity tools such as IDE, Dev Metrics, Dev logging, Packaging, Service catalog, runtimes, etc., should be included in the offered solution.
- The proposed solution should have the capability to provide approvals and customized integrated workflows.
- Customization of costs and addition of additional cost drivers should be possible.
- The proposed cloud solution should allow assigning costs to individual services provided by the OCAC Service catalogue.

10. Functional Requirements & Technical Specifications

i. Orchestration Layer:

A robust multi-cloud architecture is expected to support Software Defined Networking, policy-based orchestration, strong API support, and Life Cycle Management workflows for provisioning, decommissioning, and extensible capabilities for "Self-Management." The solution should facilitate multitenancy and user management through an on-demand, self-service provisioning portal. It should provide automated creation of virtual and physical instances, and the assignment of virtual infrastructure through appropriate tooling to support end-to-end automated provisioning, including bare metal provisioning. Integrated billing with the proposed cloud solution and REST-based APIs for all functional components of the compute service are crucial. Role-based policy management, administration, and enforcement of role-based policies should also be supported.

ii. Patch Management:

The Bidder is required to provide services related to Patch Management, evaluating threats posed by known vulnerabilities, assigning risk factors, and testing patches before deployment. The patch management solution should efficiently cover all types of environments, including operating systems (Windows/Linux/Ubuntu, etc.) and databases (MySQL, PostgreSQL, MongoDB, Oracle, etc.). The tool should correlate required patches based on findings from a Vulnerability Assessment (VA) tool and automate the deployment process through the change management process.

xvii. Enterprise Management System (EMS):

The EMS system should offer regular monitoring, management, and reporting of the IT infrastructure of the SDC. Key features include:

- Availability monitoring, management, and reporting for compute and networking.
- Performance monitoring, management, and reporting for compute and networking.
- Securing critical servers using server-based Access Control and recording user activity through audit logs.

iii. Penetration Testing:

Penetration Testing includes identifying exploitable vulnerabilities, exposing potential entryways to sensitive data, and providing clear reports on security issues and recommendations. Penetration Testing must be performed before Go-Live, and regular intervals are specified, including a six-month frequency. Application details shall be shared before the commencement of Penetration Testing.

iv. Server Security (HIPS) Deployment:

The Bidder is required to deploy Host-based Intrusion Prevention System (HIPS) with a management console, ensuring regular updates and policy management. Endpoint security deployment for desktops and laptops, along with a management console, is also mandated.

v. Backup Software:

The Bidder is responsible for backup activities per OCAC policies, including monitoring and enhancing the performance of scheduled backups, regular testing, real-time monitoring, log maintenance, and reporting. Media management tasks, 24x7 support for file and volume restoration, and adherence to retention policies are essential.

vi. OS Hardening:

OS Hardening includes activities like removing non-essential. OS Hardening includes activities like removing non-essential tools, utilities, and services, activating and configuring security features, and varies based on different Operating Systems. Activities include identifying unused ports, disabling unnecessary services, removing rogue connections, setting up filters for malicious content, testing backup and restoring procedures, defining account policies, local server policies, event log settings, system services, registry settings, file and folder permissions, etc. OS hardening will be done by the Bidder according to OCAC's hardening policy.

vii. Design Validation and Change

The successful Bidder is obligated to create a comprehensive deployment design document encompassing both physical and IT aspects. This document must be submitted for approval within two weeks of the contract Agreement signing with OCAC. It is crucial for the Solution design to be provided during the bidding process. In crafting the design, the Successful Bidder is expected to consider the existing DC setup on the 2nd Floor of the OCAC Building, ensuring scalability requirements are met, and planning for minimal downtime during implementation.

10.1. Installation and Configuration of the Commissioned IT Infrastructure

The successful Bidder will need to conduct pre-installation planning at the SDC, covering aspects such as civil design, construction, interiors, rack planning, structured cabling, SAN cabling, power points, etc.

a. The Bidder assumes responsibility for the delivery, installation, testing, and commissioning of servers, storage, network, security, cloud orchestration, EMS, and associated equipment in the Data Centre. b. Planning and layout design for equipment placement in the provisioned Data Centre fall under the Bidder's purview. This design should optimize the utilization of resources and facilities provided at the Data Centre efficiently. c. The developed plan and design documents require submission to OCAC for approval, and acceptance must be obtained before the installation commences. d. Installation of equipment should align with the approved plans and layout designs. e. Licenses required for devices should be configured for active-active status from day one.

10.2. Deployment Phase

a. The Bidder must actively engage in planning, designing, and final acceptance to ensure the seamless functionality of the proposed solution in accordance with the tender requirements. The System Integrator (SI) is tasked with procuring the materials and equipment specified in the SI’s response. It is essential to note that the SI is expected to acquire all necessary equipment for the proposed expansion setup. Should it be identified that specific components are essential for required functionality but are not included in the Tender Bill of Quantity (BOQ), the SI should incorporate such equipment in the bid value, quoting them as “others or miscellaneous.” This should include a detailed list of the items with individual descriptions and unit costs.

b. The bidder is responsible for the holistic seamless integration of all IT devices before the final acceptance test. The technical proposal of the bidder should detail the integration and upgrading of IT-device OEM professional services for optimal utilization of these devices.

c. Upon the successful commissioning and completion of the Factory Acceptance Test (FAT) of the project, the bidder must ensure a complete handover and knowledge transfer from OEMs for operations and management.

10.3. Procurement & Delivery of IT Infrastructure Components

The Bidder is mandated to procure and supply all components and subcomponents, both active and passive, as per the requirements outlined in the RFP/Contract. This includes responsibility for the supply and installation of:

• All active and passive components needed for the expansion area of the server farm at the Odisha State Data Centre. • IT infrastructure components such as storage, networking, security components, and other IT components required at the Data Centre.

The System Integrator (SI) is responsible for delivering the equipment to the Data Centre site. The SI is required to supply all the necessary installation materials, accessories, and consumables (e.g., screws, clamps, fasteners, ties, anchors, supports, grounding strips, wires, etc.) needed for the installation of the systems.

The SI is obligated to prepare and submit a delivery report containing details of all components supplied, which will be validated by the Odisha Computer Application Centre (OCAC).

Any additional equipment procured by the Bidder will be supplied by the respective Original Equipment Manufacturer (OEM). The Bidder is responsible for inventory checks, testing, and the installation of the equipment, coordinating with the supplier as required.

The Scope of Work encompasses the procurement of various IT components required for the implementation of the Solutions, as outlined but not limited to the items mentioned in the Bill of Quantity.

S. No.	Item Description	UoM	Quantity

The bill of quantities provided is indicative, and the purchaser retains the right, at the time of contract award, to adjust the quantity of goods and/or services from the originally specified amounts in the RFP. Any such modifications will not impact on the unit price or alter any other terms and conditions outlined in the original procurement documents.

10.4. Implementation

a. The Bidder must furnish a comprehensive Data Centre solution to OCAC as part of their technical bid. Any activities essential for the implementation of the Data Centre, not explicitly mentioned here, should be duly acknowledged.

b. The solution proposed by the Successful Bidder must align with all specified service level requirements. While the fundamental bill of material remains unchanged, any alterations to the basic BOM shall be conducted in collaboration with OCAC. It is advised that the Bidder thoroughly review the RFP to ensure adherence to the specified service levels outlined in the document.

c. The Bidder is accountable for the entire project management in accordance with the terms and conditions of the RFP.

d. The Bidder should guarantee that the entire infrastructure is fully supported by the respective OEM’s support services.

e. Solution Capability: The professional experts from the OEM team are expected to provide support through periodic reviews during different stages of the project implementation.

   i. Technical Solution Preparation

ii. Solution Implementation

iii. Final Preparation for Go-Live

iv. Stabilization period

v. Final Go Live.

10.5. Migration to ODYSSEY

The Bidder is tasked with executing all activities related to migrating the existing OSDC 1.0 infrastructure to the planned OSDC 2.0.

a. Data migration from existing storage to new storage, following OCAC guidelines. Migration includes transitioning data from the existing tape library and VTL to newly procured devices.

b. Application migration in coordination with application owners/departments and under OCAC guidelines.

c. Migration of Servers, network, security stack, and other necessary items based on business requirements, minimizing downtime before FAT. Proposed access switches shall replace the existing 11 switches in OSDC 1.0.

d. The Bidder's scope is solely the migration and management of the physical infrastructure, providing facilitation to the Application owner. Application migration responsibility rests with individual application owners.

e. Bidder ensures required dependencies are met and included in their solution for application migration to OSDC 2.0. Application enhancement, however, is not Bidder's responsibility, and no penalty will be charged for any delay in application readiness.

f. Existing cloud Infrastructure solution of OSDC 1.0 must be migrated from existing SDC 1.0 to OSDC 2.0, including hardware relocation.

g. Bidder provides an approach and methodology for migrating infrastructure solution and applications from OSDC 1.0 to OSDC 2.0.

h. Bidder envisions implementing IPv6 enablement during the migration process, with support from existing SI/DCO.

10.6. Operations & Maintenance

The Bidder is expected to deliver the following operations and maintenance services under OCAC's supervision:

a. Ensure a robust support model aligning with indicative manpower planning for optimal Data Centre performance, meeting designed availability levels and predictable restoration times in case of failure.

b. After deployment, Bidder takes complete responsibility for managing the entire support model to ensure SLA uptime.
c. Provide comprehensive onsite support 24x7x365, ensuring 99.982% uptime for IT infrastructure at OSDC 2.0 in line with the SLA in the tender.
d. Commit to providing necessary onsite manpower resources to resolve issues/incidents, effect changes, optimizations, and modifications.
e. Assign onsite manpower resources for 24x7x365 troubleshooting, diagnosis, and resolution of Data Centre services-related issues. Staff should possess capabilities for preventive and break-fix maintenance, troubleshooting, problem resolution, tuning, etc. Provision offsite support for OSDC 2.0 operational continuity.
f. Provide comprehensive technical support services for all hardware and software proposed throughout the contract period, covering upgrades, updates, and patches released by respective OEMs.
g. Offer comprehensive onsite warranty on a 24x7x365 basis for five years from the Go-Live date for all IT infrastructure within the tender scope, starting from the system's acceptance date.

10.7. Onsite Support

The Bidder ensures the entire IT Infrastructure solution operates in line with stipulated service standards:

a. Provide comprehensive onsite warranty 24x7x365 for five years from the Go-Live date for all IT infrastructure in the scope of work, starting from the system's acceptance date.
b. Onsite technical support includes upgrades, updates, major or minor patches released by OEMs during the contract period.

10.8. Technical Support

The onsite Technical team collaborates with OCAC's technical support desk:

a. Log and issue/complaint related to IT infrastructure at the Data Centre, issuing an ID number against each issue/complaint.
b. Assign severity levels to categorize and differentiate incident criticality through priority, severity, and impact levels.
c. Track each issue/complaint to resolution.
d. Escalate issues/complaints to OCAC officials if necessary, following the escalation matrix defined in consultation with OCAC.
e. Analyze issue/complaint statistics and Bidder’s SLA.
f. Provide channels for reporting issues to the onsite technical team, including email, telephone

(mobile phone alerts), and web-based reporting.

g. Implement a call logging system aligned with severity levels in the SLA.

10.9. System Maintenance and Management

Key deliverables sought from the Bidder regarding System Maintenance and Management include:

a. Responsible for tasks such as server setup, configuring and allocating storage space, account management, periodic data backups, automating reporting tasks, and executing hardware and software updates under OCAC supervision.
b. Provision skilled and experienced manpower resources for administering and managing the entire IT Infrastructure solution for ODYSSEY.
c. Ongoing responsibility for troubleshooting issues in the IT infrastructure to identify areas requiring fixes and ensuring timely resolution.
d. Identify, diagnose, and resolve problem areas concerning the IT Infrastructure, adhering to defined SLA levels.
e. Implement and maintain standard operating procedures for IT infrastructure maintenance, based on policies formulated in consultation with OCAC and industry best practices/frameworks. Create and maintain adequate documentation/checklists.
f. Manage user names, roles, and passwords for all relevant subsystems, including servers and other devices.
g. Manage passwords for all relevant components and devices, implementing a password change mechanism in line with security policies formulated in consultation with OCAC and industry best practices/frameworks.

10.10. System Administration

Minimum deliverables sought from the Bidder for System Administration include:

a. 24x7x365 monitoring and management of Data Centre servers.
b. Accountability for proper configuration of server parameters and all hardware maintenance to support the IT infrastructure.
c. Responsibility for Operating system administration, including user management, process management, preventive maintenance, and upgrades.
d. Installation and reinstallation in case of system crashes/failures.
e. Regularly monitor and maintain logs of servers, ensuring their availability to OCAC at all times.
f. Regularly analyse events and logs generated in all subsystems, taking actions based on log analysis results, ensuring log backup and truncation at regular intervals.

g. Adopt a defined process for change and configuration management in areas such as server changes, operating system adjustments, and applying patches.
h. Provide hardening of servers in line with defined security policies.
i. Provide integration and user support for all supported servers and data storage systems.
j. Provide directory services such as local LDAP and DNS services, and user support for all supported servers and data storage systems.
k. Troubleshoot problems with web services, application software, desktop/server relationships, and overall server environment aspects, managing and monitoring server configuration, performance, and activity.
l. Documentation of configuration for all servers and IT infrastructure, managing trouble tickets, diagnosing problems, reporting, managing escalation, and ensuring rectification of server problems as specified in the SLA.
m. Administrators should possess experience in latest technologies like Orchestration, virtualization, and cloud computing for provisioning existing and applicable infrastructure based on requirements.

10.11. Storage Administration

Minimum deliverables sought from the bidder for Storage Administration include:

a. Responsibility for managing the storage solution, including storage management policy, configuration and management of disk arrays, SAN fabric/switches, Virtual Tape Library, etc.
b. Management of space, SAN volumes, RAID configuration, LUN, zone, security, business continuity volumes, and performance in storage management.
c. Remote management of the storage system and components by OCAC, with the Bidder providing the necessary setup.
d. Identification of key resources, interconnects, health, connectivity and access rights in the storage solution, including creating/deleting, enabling/disabling zones and storage volumes.
e. Provision scalability in the solution as needed.
f. Administrators should possess experience in latest technologies like virtualization and cloud computing for provisioning existing and applicable infrastructure based on requirements.

10.12. Database Administration

Under the guidance of OCAC, the Bidder assumes responsibility for monitoring database activity and performance, adapting the database logical structure to accommodate the requirements of new and modified programs.

a. The Bidder performs physical administrative functions, including reorganizing the database to enhance performance.
b. The Bidder tunes the relational database, ensuring data integrity and configuring the data dictionary.
c. The Bidder tests and installs new database software releases under OCAC's supervision.

10.13. Backup / Restore

The Bidder is responsible for storage backup in accordance with OCAC policies, to be discussed during installation and configuration.

a. The Bidder enhances the performance of scheduled backups, conducts regular testing, and ensures adherence to retention policies. During the project period, the existing IT infrastructure of OSDC 1.0 may shift to OSDC 2.0 without additional cost to OCAC.
b. The Bidder promptly executes on-demand backups of volumes and files upon OCAC's request or during system upgrades and configuration changes.
c. The Bidder monitors, maintains logs, and reports backup status regularly, appointing administrators for prompt problem resolution.
d. Administrators handle media management tasks, such as tagging, cross-referencing, storing, logging, testing, and vaulting onsite and offsite in fireproof cabinets.
e. The Bidder provides 24x7 support for file and volume restoration requests at the Data Centre.
f. ODYSSEY will utilize the existing backup software and prerequisite platform (hardware, OS, etc.).

10.14. Network Monitoring

The Bidder offers network environment management services to maintain optimal performance 24x7.

a. The Bidder monitors and administers the network within the Data Centre up to integration points with WAN, providing services for routers, switches, and load balancers.

b. The Bidder creates and modifies VLANs, assigns ports to applications, and segments traffic.
c. The Bidder manages the overall SDN solution within the Data Centre and integrates it with other infrastructure orchestration solutions such as NMS, EMS, and Cloud Management.
d. The Bidder coordinates with the Data Centre Site Preparation vendor for break-fix maintenance of LAN cabling or maintenance requiring civil work.

10.15. Firewall Monitoring and Management

a. Installation and maintenance of the firewall.
b. Initial configuration and hardening of the firewall.
c. Performance monitoring and regular monitoring of LAN errors.
d. Rule-based policy changes for the firewall.
e. Configuration of security policies.
f. Creation and maintenance of Network Access Policy (NAP) documents agreed upon by the parties.
g. Review and analysis of log files on traffic flow.
h. Trend upgrade and analysis of log files.
i. Compliance testing.
j. Design, configuration, and maintenance of Network Address Translation (NAT) services.
k. Access control management through creation of Network Access Policy and firewall rules.
l. Implementation and maintenance of access to F/W logs policies and performance statistics.
m. Management of regular reports for detailed auditing of configuration history and change journals.
n. Incidence response.
o. Lifecycle Management of all hardware and software components.
p. Firewall backup.

10.16. Network-Based Intrusion Prevention System - Monitoring and Management

a. Traffic profiling.

b. Definition of alert levels and incident response levels.

c. Root cause analysis.

d. Technical support.

e. 24x7 monitoring of NIPS availability.

f. Restoration of NIPS availability.

g. Determination of intrusion occurrences.

h. Upgrade of vendor-provided intrusion signatures.

i. Security event correlation.

j. Regular monitoring of attack logging rules' logs.

k. Regular monitoring of generic deny rules' logs.

l. Regular monitoring of attack bandwidth utilization.

m. Analysis of network attacks and serious attack attempts.

n. Assessment of uncovered new vulnerabilities.

o. Proposal of corrective and preventive actions.

p. Monitoring and subscription to external network security information.

q. Installation and configuration of NIPS Software and Hardware.

r. Maintenance and upgrade of service component software.

s. Reporting of intrusions and actions through web-based access.

t. Regular reports.

u. Incidence response.

v. Prevention of all known network-based attacks.

w. Filtering out IP and TCP illegal packet types.

x. Design and configuring of IPS services in response to flooding limits.

y. Technical support desk support.

z. Lifecycle Management of all hardware and software components.

aa. 24x7 real-time monitoring and response.

10.17. Patch Management

The Bidder provides services related to Patch Management, ensuring adherence to security precautions.

a. Ensure documentation of approval for allowed traffic to the internal network is available. Personnel evaluating patch stability should be experts in mission-critical systems and capable of verifying system stability after patch installation.

b. Before installing any patch, a full backup of all data and server configuration information must be made. Periodic testing of the restore process is recommended for disaster recovery. Efficient execution of patch management is essential for all environments, including operating systems and databases.

10.18. Monitoring & Management

a. The proposed service management system offers a detailed service dashboard view of each department/office's health in the organization, service health, and SLAs.

b. The system provides an outage summary indicating the high-level health of each service and details of any outage's root cause.

c. The system manages IT resources, specifies and monitors service obligations, associates users/departments/organizations with the services they rely on, and tracks Service/Operational Level Agreements. Services include E-mail, Internet Access, Intranet, and others.

d. The Service Level Agreements (SLAs) definition facility supports defining one or more services specifying obligations stipulated in an SLA contract for a specific time period (weekly, monthly, quarterly, and as required by OCAC).

e. SLA violation alarms notify whenever an agreement is violated or at risk.

f. The system designates planned maintenance periods for services, considers maintenance periods defined at the IT resources level, and exempts service outages from impacting an SLA when necessary.

10.19. Other Support Services

a. Hardware support for the IT infrastructure solution, diagnosing problems, and coordinating with vendors for resolution to ensure OCAC's IT infrastructure uptime as per SLAs.

b. Maintenance of records for all hardware changes in the IT infrastructure solution.

c. Scheduled maintenance of the IT infrastructure solution as defined by the OEM and discussed with OCAC.

d. Installation, upgrade, update, and management of all patches, including servers and switches.

e. Maintenance of the inventory of hardware and software assets at the Data Centre.

f. Documentation maintenance for material movement, network diagrams, manuals, and licenses in both hard and soft formats.

g. Updates to documents for changes in IP addresses, machine layout, network additions, and alterations.

h. Implementation and enforcement of procedures, policies, and guidelines like Security policy, Network access policy, Anti-virus policy, etc., formulated in discussion with OCAC.

i. Liaison with Data Centre teams for utilities such as Power, UPS, Air Conditioning, etc., as needed.

j. Onsite Support for ICT Infrastructure hosted by other Government Agencies: Co-location

k. OCAC provides Data Centre rack space to other Government agencies and user departments for hosting their IT Infrastructure.

11. Minimum Technical Specification – IT

The following outlines the minimum technical requirements for the specified devices, equipment, and solutions. Bidders are kindly requested to indicate their level of compliance (partial, no, or full) against each listed item. The bidder has to ensure the followings:

a. All the Items supplied should be with minimum 5 years of comprehensive onsite OEM warranty from the date of Go-Live.

b. All the required licenses should be perpetual. However, any subscription based licenses required, should have validity for minimum 5 years from the date of Go-Live.

c. All the Datacentre IT Infra should be in N+N redundancy for power and cooling and should be with hot swappable for avoiding any downtime & easy operations.

d. Installations of the items like Network Solution. Storage Solution, Load Balancer Solution, Security Solutions, EMS, NMS & Helpdesk Management System Solution, Cloud Solutions, etc., need to be done by the respective OEM manpower or OEM Authorized Professional Services.

11.1. Rack Server- Type-1

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make **Model**				
1	Processor	The server should have 2 nos. of Intel Xeon/AMD EPYC Processor should be from latest 4th Gen or higher announced series. Processor: 2 x 16 core, minimum 3.6 GHz OR Higher clock rate. 64-bit x86 processor fully binary compatible to 64/32-bit applications. Number of cores on a single die/socket will be treated as a single processor.		
2	Memory	Minimum 1TiB or higher latest DDR5 memory using 64 GB DIMMs or higher. 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. The memory should have native capability of identifying and reporting the genuineness of the memory installed in the server. OR The server should be integrated in the factory, tested, certified, chassis intrusion switch enabled.		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
3	HDD Controller	12 Gbps Tri-mode SAS/SATA/NVMe RAID Controller supporting RAID 0, 1, 5 and 6 with 8GB battery backed up cache.		
4	HDD	2 x 480 GB NVMe SSD or Higher		
5	Video Controller	Integrated Graphics Controller		
6	Network Controller	Minimum 4 x 1 Gbps ports and 4 No's (2 x 2 on each network adapter card) of 10/25 Gbps SFP28 ports with 25 Gbps SFP28 LC transceiver SR Type		
7	Fiber Channel HBA	Two no's Dual FC Port 32 Gbps (i.e. 4 Nos. of 32 Gbps.) with LC fibre transceiver SR Type		
8	Slots	Minimum one free PCI-Express 5.0 slot.		
9	Ports	2* USB 3.0; 1* Keyboard Port & 1 * Mouse Port (on board/dongle), One dedicated Ethernet Port for OS independent out-of-band hardware management		
10	Bays	Support for up to minimum 8 Hot Swap drive bays		
11	System Chassis	Rack Mount, 2U (max) chassis with security bezel and chassis intrusion detection. Redundant Hot Swappable Power Supply with Platinum Efficiency		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
12	OS Certification	Certification for latest Server version of Windows and minimum two Linux flavours		
13	Drive / 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 Management	Remote management of Server over LAN & WAN with SSL encryption through OOB gigabit management port, Remote KVM, Server Health Logging, Virtual NIC, REST API, IEEE 802.1x & IEEE 802.1AR, HTML5 Remote Console, TPM module, Encrypted Virtual Media, and virtual folder with required advanced IPMI license, AD or LDAP, Config backup, Syslog (local and remote). UEFI Secure Boot and Secure Start, Security feature to ensure servers do not execute compromised firmware code, digitally signed, and verified updates, Security Dashboard for Server to detect possible security vulnerabilities, Precision Time Protocol (IEEE 1588 PTP)		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
15	Serviceability	System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone support. The 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. Should provide remote firmware update functionality as well as Runtime Firmware verification and compliance check including automated recovery.. Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD Solution should be provided for monitoring & analysis feature to predict, prevent and auto-resolve problems and by providing automating case creation and log file submission for the problems that can't be auto-resolved. Should provide silicon based hardware root of trust, automatic secure BIOS & firmware recovery, cryptographically		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
		signed firmware updates. One-button or one-click or RESTful API based secure erase of all user data on the server with respect to secondary storage and NVRAM compliant to NIST 800 standards.		
16	Virtualization	Should support industry standard virtualization software		
17	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.		
18	IPv6 Support	All devices should be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		
19	Power Cord	Server should supply with compatible IEC C13/C14 3pin power cord suitable for PDU.		

11.2. Rack Server-Type-2

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
1	Processor	The server should have 2 nos. of Intel Xeon/AMD EPYC Processor should be from latest 4th Gen or higher announced series Processor: 2 x 32 cores, minimum 2.1 GHz OR Higher clock rate. 64-bit x86 processor fully binary compatible to 64/32-bit applications. Number of cores on a single die/socket will be treated as a single processor.		
2	Memory	Minimum 1TiB or higher latest DDR5 memory using 64 GB DIMMs or higher. 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. The memory should have native capability of identifying and reporting the genuineness of the memory installed in the server. OR The server should be integrated in the factory, tested, certified, chassis intrusion switch enabled.		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
3	HDD Controller	12 Gbps Tri-mode SAS/SATA/NVMe RAID Controller supporting RAID 0, 1, 5 and 6 with 8GB battery backed up cache.		
4	HDD	2 x 480 GB NVMe SSD or Higher		
5	Video Controller	Integrated Graphics Controller		
6	Network Controller	Minimum 4 x 1 Gbps ports and 4 No's (2 x 2 on each network adapter card) of 10/25 Gbps SFP28 ports with 25 Gbps SFP28 LC transceiver SR Type		
7	Fiber Channel HBA	Two no's Dual FC Port 32 Gbps (i.e. 4 Nos. of 32 Gbps.) with LC fibre transceiver SR Type		
8	Slots	Minimum one free PCI-Express 5.0 slot.		
9	Ports	2* USB 3.0; 1* Keyboard Port & 1 * Mouse Port (on board/dongle), One dedicated Ethernet Port for OS independent out-of-band hardware management		
10	Bays	Support for up to minimum 8 Hot Swap drive bays		
11	System Chassis	Rack Mount, 2U (max) chassis with security bezel and chassis intrusion detection. Redundant Hot Swappable Power Supply with Platinum Efficiency		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
12	OS Certification	Certification for latest Server version of Windows and minimum two Linux flavours		
13	Drive / 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 Management	Remote management of Server over LAN & WAN with SSL encryption through OOB gigabit management port, Remote KVM, Server Health Logging, Virtual NIC, REST API, IEEE 802.1x & IEEE 802.1AR, HTML5 Remote Console, TPM module, Encrypted Virtual Media, and virtual folder with required advanced IPMI license, AD or LDAP, Config backup, Syslog (local and remote). UEFI Secure Boot and Secure Start, Security feature to ensure servers do not execute compromised firmware code, digitally signed, and verified updates, Security Dashboard for Server to detect possible security vulnerabilities, Precision Time Protocol (IEEE 1588 PTP)		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
15	Serviceability	System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone support. The 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. Should provide remote firmware update functionality as well as Runtime Firmware verification and compliance check including automated recovery.. Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD Solution should be provided for monitoring & analysis feature to predict, prevent and auto-resolve problems and by providing automating case creation and log file submission for the problems that can't be auto-resolved. Should provide silicon based hardware root of trust, automatic secure BIOS & firmware recovery, cryptographically		

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
		signed firmware updates. One-button or one-click or RESTful API based secure erase of all user data on the server with respect to secondary storage and NVRAM compliant to NIST 800 standards.		
16	Virtualization	Should support industry standard virtualization software		
17	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.		
18	IPv6 Support	All devices should be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.		
19	Power Cord	Server should supply with compatible IEC C13/C14 3pin power cord suitable for PDU.		

11.3. Enterprises Storage (1 PiB)

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make **Model**				
1.	ARCHITECTURE: a) Minimum Four Storage controllers/ Nodes configured in Symmetric Active-Active mode, where all the volumes and LUNs shall be active from all the controllers, should support RAID6 or equivalent with automatic failover. Failure of any controller should not affect the path availability and working connectivity between storage system and devices. b) Offered system should be configured in such a way that entire offered cache should be available for all volumes. Once restored the system should auto restore to its original way of functioning. c) Offered storage shall be an enterprise storage array & 99.9999% data availability guaranteed architecture and All Flash cloud native end to end NVMe array only. Shall be marketed / Publish as All NVMe array on the vendor web site. d) The supplied items will be installed on two adjacent racks for power load balancing and high availability. All the required cables and accessories etc. to be factored by the bidder for the complete requirement of the solution. All the controllers and enclosures should be installed in balanced (1:1) ratio on both the racks.			
2.	CAPACITY: Proposed storage array must be offered with 1PiB usable capacity using maximum 15.36TiB NVMe SSD Drives (non-QLC type) in RAID 6 excluding all overheads like RAID parity and file system. Additional global hot spare			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
	drive of same drive capacity for every thirty drives should be configured.			
3.	EXPANDABILITY: a) Storage Array should be scalable up to minimum 2.5 PiB or higher using 15.36 TiB within same storage system without compromising performance of the system. b) Minimum 240 number of NVMe drive supported. c) Proposed storage should support minimum 48 Numbers of FC/iSCSI host ports. Array shall have native support for 16Gbps & 32Gbps FC ports and 10 Gbps & 25Gbps iSCSI ports. d) Proposed system to be configured in such a way that only NVMe drives would be required to meet the capacity scalability mentioned above.			
4.	HIGH AVAILABILITY: No single point of failure (NSPOF); Online firmware upgrades; Remote diagnostic support.			
5.	HOST PORTS: Storage solution should be supplied with minimum port configuration as follows: a) FC Ports: 32 x 32 Gb b) iSCSI ports: 16 x 10Gb c) 8 x 10 Gbps ports for replication, in case storage doesn't have native ports for replication then FCIP router shall be provided at no extra cost to SDC.			
6.	BACK-END PORTS: Offered storage shall have at-least 400Gb NVMe of enabled bandwidth for drive enclosure connectivity and			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
	shall preferably be scalable to 800Gb enabled bandwidth NVMeOF ports.			
7.	CACHE MEMORY: Minimum 1TiB battery-protected Global DRAM cache across all controllers with battery backup for 72Hrs OR equivalent mechanism, to protect data in Cache in case of power failure. (DRAM Cache as asked shall be sum of the DRAM Cache being configured in all offered Storage Controllers in the Storage. DRAM Cache memory of NAS header and/or any other device will not be considered to calculate DRAM cache of the Storage).			
8.	PROTOCOL SUPPORT: a) The storage solution should support FC and iSCSI for Block. 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. c) Proposed storage should be configured with NVMeOF (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			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
11.	DATA ENCRYPTION: Vendor shall provide encryption for data at rest on volume/hardware level which should meet FIPS 140-2 – Level 2 security requirements			
12.	DATA EFFICIENCY: Offered storage array shall support inline data efficiency engine (Supporting Thin Zero detect and re-claim, Deduplication & Compression) and shall be enabled by default. Vendor shall have flexibility to enable / disable the data efficiency engine at the time of Volume creation			
13.	DR SUPPORT: a) Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively without using any third party or software based solution. 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. c) Replication shall support incremental replication after resumption from link failure or failback situations.			
14.	THIN PROVISIONING & SPACE RECLAIM: For effective cloud deployment offered storage should be supplied with thin provisioning and auto thin reclaim to make the volume thin for an extended period for complete array supported raw capacity. It should support automated thin reclaim			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
15.	SNAPSHOT/PIT-COPY/CLONE: a) Offered Storage shall support to make the snapshot and full copy (Clone) of thin / thick volumes as thin volume. 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 automatically d) Storage Array shall have functionality to create virtual lock for retention of read-only snapshots to 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 & DB SUPPORT: Linux, Windows, Unix, Solaris etc.			
17.	CLOUD-ENABLED ANALYTICS: Cloud enabled Analytics engine shall have capability to provide following:			
	a. Shall have capability of global learning – Analytics engine shall collect control information from at-least 50000+ arrays across vendor installed base for meaningful output. Vendor shall provide the documentary proof for it			
	b. Analytics engine shall have capability of proactive recommendation for arresting the issues / problems			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
	noticed at another install base of vendor after idenfying the problematic signature.			
	c. Providing extremely granular per-minute historical capacity and performance trend analysis by default, without the need to enable extra logging, install any appliances (physical or virtual), or install any software.			
	d. Providing overall saturation level of the array while combining while analysing various parameters like IOPS, MB/sec, Block size etc.			
	e. Providing the status of at-least top 5 volumes where latency is extremely high			
18.	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 at storage. It shall be possible to define different service / response time for different application logical units. 2) Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units 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 MONITORING: Storage management software should provide real time monitoring and historical analysis of storage performance data such as total IOPS, read%, write %,			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
	cache-hit %, throughput, etc. for analysing performance of the systems.			
20.	SOFTWARE FEATURES & LICENSING: a) Proposed Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, De-duplication, Compression, Performance Monitoring, and Quality of Service on Day1 for the maximum supported capacity of the offered array. b) Single GUI & WEB based remote management; Should be capable to create, expand & move volumes dynamically; Support for dynamic LUN expansion. Management Software and Licenses to be supplied for full capacity.			
21.	VAAI INTEGRATION: Storage must be complied to 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			
c	Offered Storage shall support over 5000 Vmware VM's using VVOL.			
d	Offered storage array shall be tightly integrated with VMware so that Eager zero disks layout can be used with thin provisioning and thin re-claim.			
22.	CONTAINER INTEGRATION: Offered Storage array shall be integrated with Red-hat OpenShift, Kubernetes and other industry K8 based			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
	container platform through CSI driver set. Vendor shall 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.			
23.	Support for dynamic NFS provisioning to dynamically create persistent volumes			
24.	OEM Ranking: OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for storage OR The proposed Storage OEM must be rated as Leader's in the latest magic quadrants for Primary Storage by Gartner.			
25.	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.			
26.	IPv6: All devices should be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation			

11.4. Spine Switch

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
1	**General**		
1.1	The core/spine layer switches should have hardware level redundancy (1+1) in terms of control plane. Issues with any of the plane should not impact the functioning of the switch. All the switches should be from same OEM		
1.2	The switch should have redundant CPUs from day 1. Switch dual supervisor configuration must allow nonstop forwarding (NSF) with a stateful switchover (SSO) when a supervisor-level failure occurs.		
1.3	The Switch should support non-blocking architecture, all proposed ports must provide wire speed line rate performance		
1.4	The switch should not have any single point of failure like supervisor, switching fabric, power supplies and fans		
1.5	Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch		
1.6	Switch should support the complete STACK of IP V4 and IP V6 services.		
1.7	The proposed switches should be part of Gartner Leader Quadrant for DC Networking for last 2 years		
1.8	All relevant licenses for all the features and scale should be quoted along with switch		
1.9	Switch and optics should be from the same OEM		
2	**Hardware and Interface**		
2.1	Switch should have the following interfaces: 30 x 40/100 G QSFP28 Ports equally distributed in two line cards. Switch should be Populated with 32 Nos 100 Gbps MM Transceiver and scalable up to 192 x 100G QSFP28 ports along with 1G Management port for monitoring.		
2.2	Switch should have minimum 2 Blank slot for future expansion		
2.3	Chassis should be capable of supporting 400G from day1 without change in the base chassis components (sup, fabric, power supplies etc)		
2.4	Switch should have adequate power supplies for the complete system usage with all slots populated and used, providing N+N redundancy		
3	**Performance**		
3.1	Switch should support Graceful Restart for OSPF, BGP etc. Should support uninterrupted forwarding operation to ensure high-		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	availabability during primary controller failure		
3.2	Switch should support minimum 1000 VRF instances with route leaking functionality		
3.3	The switch should support minimum 500K IPv4 LPM routes		
3.4	The line card proposed should have minimum 150MB Packet Buffer per LC		
3.5	The switch should support 100K multicast routes		
3.6	Switch should support a minimum of 28 Tbps BW		
4	**Network Virtualization Features**		
4.1	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN		
4.2	Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center		
5	**Layer2 Features**		
5.1	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)		
5.2	Switch should support VLAN Trunking (802.1q)		
5.3	Switch should support minimum 500K of MAC addresses		
5.4	Switch should support VLAN tagging (IEEE 802.1q)		
5.5	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy		
5.6	Switch should support layer 2 extension over VXLAN across all DataCenter to enable VM mobility & availability		
5.7	The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane		
6	**Layer3 Features**		
6.1	Switch should support static and dynamic routing		
6.2	Switch should support segment routing and VRF route leaking functionality from day 1		
6.3	Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Support Multicast Source Discovery Protocol (MSDP)		
6.4	Switch should support Multicast routing		
7	**Quality of Service**		
7.1	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service)		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	b. DSCP (Differentiated Services Code Point)		
7.2	Switch should support for different type of QoS features for ream time traffic differential treatment using: a. Weighted Random Early Detection b. Strict Priority Queuing		
7.3	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
8	**Security**		
8.1	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy		
8.2	Switch should support for external database for AAA using: a. TACACS+ b. RADIUS		
8.3	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding		
8.4	Switch platform should support 802.1AE in hardware		
8.5	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
9	**Manageability**		
9.1	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
9.2	Switch should provide remote login for administration using: a. Telnet b. SSHv2		
9.3	Switch Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. • Flow path trace (ingress to egress switch) • Per Flow Hop by Hop packet drop with reason of drop • Per Flow latency (per switch and end to end)		
9.4	Should support software telemetry - • Utilization of MAC table, Route table • Hardware resources like interface utilization, BW utilization • Switch environment like CPU, memory, FAN and Power Supply unit • Interface statistics like CRC errors etc.		
9.5	Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP1, SNMP2 and		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	SNMP v3 with Encryption		
9.6	Switch should provide different privilege for login in to the system for monitoring and management		
10	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement for 5 years		

11.5. Leaf Switch Fiber

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
1	**Solution Requirement**		
1.1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing		
1.2	Switch should support the complete STACK of IPv4 and IPv6 services.		
1.3	The proposed solution and switches should be part of Gartner Leader Quadrant for DC Networking for last 3 years		
1.4	The Switch should have the capability to function in line rate for all ports		
2	**Hardware and Interface Requirement**		
2.1	Switch should have the following interfaces: Minimum 48 ports support 1/10/25 Gbps SFP ports for host connectivity and 6*100G ports for Fabric/Spine connectivity. The proposed switch should support native 25G and should be populated with 48 Nos 10/25 Gbps MM fiber Transceiver for downlink connectivity while having the uplink interafces populated with 4 Nos 100 Gbps MM Fiber Transceiver		
2.2	All SFPs should be provided from same OEM		
2.3	Switch should have console port for local management & Out of band management interface for remote management		
2.4	Switch should be 1 RU fixed form factor		
2.5	Switch should be rack mountable and support side rails, if required.		
2.6	Switch should be provided with redundant power supply units		
3	**Performance Requirement**		
3.1	Switch should support dedicated process for each routing protocol		
3.2	Switch should re-converge all dynamic routing protocols at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols like OSPF, IS-IS, BGP.		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
3.3	Switch should support minimum 1000 VRF instances with route leaking functionality		
3.4	The switch should support min 800k IPv4 LPM routes		
3.5	The switch should have MAC Address table size of 500k		
3.6	The switch should support 100K multicast routes		
3.7	Switch should support 4000 VLANs		
3.8	Switch should support minimum 64 ECMP paths		
3.9	Switch should support minimum 3.6 Tbps of switching throughput		
3.10	Device should be based on simple and intelligent shared-memory egress buffered architecture that simplifies the system buffer management and queuing implementation.		
3.11	The Switch should support intelligent buffer management with a minimum buffer of 40MB.		
4	**Network Virtualization Features**		
4.1	Switch should support VXLAN to achieve Network Virtualisation.		
	Switch should support VXLAN and EVPN symmetric IRB for supporting Spine		
4.2	Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualise networking from the single pane of glass		
5	**Layer2 Features**		
5.1	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)		
5.2	Switch should support VLAN Trunking (802.1q)		
5.3	Switch should support minimum 90k of MAC addresses		
5.4	Switch should support VLAN tagging (IEEE 802.1q)		
5.5	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy		
5.6	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures		
5.7	Switch should support layer 2 extension over VXLAN across all Data Centers to enable VM mobility & availability		
5.8	The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).		
5.9	The switch should support Minimum 48 number of port channels		
5.10	A port channel should support up to 32 no. of ports		
5.11	The switch should support BGP EVPN Route Type 2, Type 4 and		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	Route Type 5 for the overlay control plane		
6	**Layer3 Features**		
6.1	Switch should support static and dynamic routing		
6.2	Switch should support segment routing and VRF route leaking functionality from day 1		
6.3	Switch should support VRF, VRF Edge, Virtual Router to achieve multi instance routing		
6.4	Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP), IGMP v1, v2 and v3		
7	**Quality of Service**		
7.1	Switch should support 802.1P classification and marking of packet using CoS (Class of Service) and DSCP (Differentiated Services Code Point)		
	Switch should support different type of QoS features for real time traffic differential treatment using Weighted Random Early Detection and Strict		
7.2	Priority Queuing		
7.3	Switch should support Rate Limiting - Policing and/or Shaping		
7.4	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
8	**Security**		
8.1	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy.Switch must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro-segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification		
8.2	Switch should support external database for AAA using TACACS+ and RADIUS. Switch must provide the capablity of inserting physical and virtual L4 - L7 (FW, LB,IPS) services dynamically between multiple segment using policy-based traffic redirect.		
8.3	Switch should support to restrict end hosts in the network in order to secure the port by limiting the number of learned MAC addresses to avoid MAC address flooding. Switch must support the capability to be used in the network fabric to act as a State-less distributed firewall with the logging capability		
8.4	Switch platform should support encryption of traffic i.e. 802.1AE in hardware		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
8.5	VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware		
8.6	Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined		
8.7	Switch should support DHCP Snooping		
8.8	Switch should support Dynamic ARP Inspection		
8.9	Switch should support IP Source Guard		
8.1	Switch should support unicast and multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port.		
8.2	Switch support broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
8.3	The Switch should support LLDP.		
8.4	Switch should support Spanning tree BPDU protection		
9	**Manageability**		
9.1	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail		
9.2	Switch should provide remote login for administration using SSHv2		
9.3	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures		
9.4	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces		
9.5	Switch should support monitoring status using different type of Industry standard NMS using SNMP1, SNMP2 and SNMP v3.		
9.6	Switch should provide different privileges for login in to the system for monitoring and management		
9.7	Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.		
9.8	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.		
9.9	Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. • Flow path trace (ingress to egress switch) • Per Flow Hop by Hop packet drop with reason of drop • Per Flow latency (per switch and end to end)		

S.No.	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
9.10	Should support software telemetry • Utilization of MAC table, Route table • Hardware resources like interface utilization, BW utilization • Switch environment like CPU, memory, FAN and Power Supply unit • Interface statistics like CRC errors etc.		
10	**Availability**		
10.1	Switch should have provision for connecting to 1:1 power supply for usage and redundancy and high availability		
10.2	Switch should provide gateway level of redundancy IPV4 and IPV6 using HSRP/VRRP		
10.3	Switch should support for BFD For Fast Failure Detection		
11	Miscellaneous Points		
11.1	Console cable and power cable (C19/C21) as per customer requirement to be provided. All Cables shall be factory-terminated.		
11.2	All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.		
11.3	Switches and Transceivers should be from same OEM.		
11.4	All relevant licenses for all the features and scale should be quoted along with switch		
12	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement for 5 years		

11.6. Management Switch/Tor Switch

Sr. No.	Minimum specification	Compliance	Remarks (If Any
Make **Model**			
1.1	**General Features :**		
1.1.1	Switch should be 1U and rack mountable in standard 19" rack.		
1.1.2	Switch should support internal field replaceable unit redundant power supply from day 1.		
1.1.3	Switch should have minimum 2 GB RAM and 2 GB Flash.		
1.1.4	Switch should have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 48 Gbps of stacking thoughput with 8 switch in single stack.		
1.2	**Performance :**		
1.2.1	Switch shall have minimum 176 Gbps of switching fabric and 120 Mpps of forwarding rate.		
1.2.2	Switch shall have minimum 16K MAC Addresses and 250 active VLAN.		
1.2.3	Should support minimum 11K IPv4 routes or more		
1.2.4	Switch shall have 1K or more multicast routes.		

Sr. No.	Minimum specification	Compliance	Remarks (If Any
Make Model			
1.2.5	Switch should support atleast 16K flow entries		
1.2.6	Switch should support 128 or more STP Instances.		
1.2.7	Switch should have 6MB or more packet buffer.		
1.3	**Functionality :**		
1.3.1	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.		
1.3.2	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1		
1.3.3	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.		
1.3.4	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.		
1.3.5	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+ .		
1.3.6	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.		
1.3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.		
1.3.8	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.		
1.3.9	During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.		
1.4	**Interfaces**		
1.4.1	Switch shall have 48 nos. 10/100/1000 Base-T ports and additional 4 nos. of SFP+ uplinks ports populated with 2 Nos 10 Gbps MM Transceiver		
1.5	**Certification:**		
1.5.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.		
1.5.2	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.		
1.5.3	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.		
1.5.4	OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from last 3 years before releasing this RFP.		
1.6	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement for 5 years		

11.7. Access Switch

S.No.	Minimum specification	Compliance	Remarks
Make **Model**			
1.1	**General Features :**		
1.1.1	Switch should be 1U and rack mountable in standard 19" rack.		
1.1.2	Switch should support internal field replaceable unit redundant power supply from day 1.		
1.1.3	Switch should have minimum 2 GB RAM and 2 GB Flash.		
1.1.4	Switch should have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 48 Gbps of stacking thoughput with 8 switch in single stack.		
1.2	**Performance :**		
1.2.1	Switch shall have minimum 128 Gbps of switching fabric and 95.23 Mpps of forwarding rate.*		
1.2.2	Switch shall have minimum 16K MAC Addresses and 250 active VLAN.		
1.2.3	Should support minimum 11K IPv4 routes or more		
1.2.4	Switch shall have 1K or more multicast routes.		
1.2.5	Switch should support atleast 16K flow entries		
1.2.6	Switch should support 128 or more STP Instances.		
1.2.7	Switch should have 6MB or more packet buffer.		
1.3	**Functionality :**		
1.3.1	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.		
1.3.2	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1		
1.3.3	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.		
1.3.4	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.		
1.3.5	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+ .		
1.3.6	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.		
1.3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.		
1.3.8	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.		

S.No.	Minimum specification	Compliance	Remarks
Make **Model**			
1.3.9	During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.		
1.4	**Interfaces**		
1.4.1	Switch shall have 24 nos. 10/100/1000 Base-T ports and additional I 4 nos. of SFP+ uplinks ports populated with 2 Nos 10 Gbps MM Transceiver		
1.5	**Certification:**		
1.5.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.		
1.5.2	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.		
1.5.3	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.		
1.5.4	OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from last 3 years before releasing this RFP.		
1.6	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement for 5 years		

11.8. SDN Controller

S.No.	Minimum Specification	Compliance (Yes/No)	Remark (If Any)
Make **Model**			
1	Fabric Defination		
1.1	Proposed fabric must be the Clos network topology architecture defined using Spine, Leaf switches with VXLAN overlay		
1.2	Fabric should have achieve following functionalities:		
1.2(a)	Flexibility : Should allow workload mobility anywhere in the DC, across the Data Center sites		
1.2(b)	Resiliency : The proposed fabric should be able to sustain multiple link and device (Leaf & Spine), Controller failures		
1.2(c)	Performance: The proposed fabirc should be able with use full cross sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi pathing		

S.No.	Minimum Specification	Compliance (Yes/No)	Remark (If Any)
Make Model			
1.2(d)	Solution should provide latency and drop analysis between end points connected to fabric with reason of drop, if needed in the future with or without an additioanal license		
1.2(e)	Mult-DataCenter design:- The proposed architecture should provide a single pane for provisioning, monitoring, and management to deploy stretched policies across multiple Data centers.		
2	Hardware and Interface Requirement		
2.1	Fabric Connectivity should have the following properties:		
2.2	Leaf switches to Spine connectivity should use uplink port using line rate 100G only		
2.3	In the fabric, the leaf and spine switches quoted should be non-oversubscribed and perform at line rate		
2.4	All switches including Spine and leafs should be of line rate including access and uplink ports non-blocking		
2.5	All switches & proposed Fabric must support for 1000 VRF/Private network without any additional component upgrade or design change		
3	Fabric Features		
3.1	Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change.		
3.2	Fabric must auto discover all the hardware and auto provision the fabric based on the policy.		
3.3	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.		
3.6	Fabric must support Role Based Access Control in order to support Multi - Tenant environment.		
3.7	Fabric must integrate with different virtual machine manager viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualise networking from the single pane of Glass - Fabric Controller/SDN Controller for visibility of VM/Container at the controller level		
3.8	Fabric must integrate with all proposed L4 - L7 Physical and virtual appliances using single pane of glass - Fabric Controller / SDN Controller		
3.9	Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric		
3.1	Solution should provide L2 & L3 extension across sites		
3.11	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc		

S.No.	Minimum Specification	Compliance (Yes/No)	Remark (If Any)
Make Model			
4.1	Fabric Security Features		
4.2	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service		
4.3	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD		
4.4	Fabric /SDN controller should provide micro-segmentation rules and policies for workloads connected to DC fabric for east-west traffic . It must support segmentation of VM based attributes like hostname, OS, VM Tags		
4.5	Fabric must support Micro Segmentation for the Virtualize and Non -Virtualize environment (Baremetal, Container)		
4.6	Fabric must support true multi - tenancy		
4.7	Fabric must act as a State-less distributed firewall with the logging capability		
4.9	Fabric must be capable of dynamically insert physical and virtual L4 - L7 (FW,LB,IPS) services between multiple segment using policy base traffic redirect		
5	Fabric management		
5.1	Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric within Data Center & across all Data Centers		
5.2	Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller.		
5.3	Fabric must be capable of dynamically insert physical and virtual L4 - L7 (FW,LB,IPS) services between multiple segment using policy base traffic redirect for East-West traffic.		
5.4	Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.		
5.5	Solution should support bug, PSIRT etc visibility		
5.6	The proposed solution should have out of the box support for automatic baselining wherein the solution can automatically learn the behaviour of monitored applications and set baseline thresholds automatically for all the monitored metrics, including: i) Application metrics ii) Server metrics iii) End User Metrics		

S.No.	Minimum Specification	Compliance (Yes/No)	Remark (If Any)
Make Model			
	iv) Custom Metrics v) Business Metrics vi) Database Metrics. The solution must also provide an option of fixed as well as rolling time periods to calculate these thresholds.		
5.7	The proposed solution must be able to track web and mobile user sessions to analyse any user's behaviour based on user's unique ID. There must be a provision to query for a segment of users with similar behaviour, such as from a specific geo location or visiting a specific page or using a particular device etc. The solution should also support a seamless ingestion of raw session data to an analytics engine to perform slicing and dicing on the data.		
5.8	The proposed solution must have a robust alert and respond engine that leverages multiple data inputs into analysis (app performance data, machine data, analytics data and user provided data), uses Boolean logic to combine multiple conditions through AND / OR logic, has capability to disable rule evaluation temporarily for predetermined maintenance windows, can trigger alerts or notifications when rules are violated (email, SMS or custom), can utilize complex logic to combine different metrics into one trigger/alert.		
5.9	The proposed solution should provide contextual monitoring of OS level metrics and provide auto correlation to the application performance. The server OS level monitoring should include general server visibility, process, volume and network metrics. There should be seamless correlation between server and application metrics through UI on the same screen without having to switch UIs.		
5.10	Solution should support the capability to provide instant visibility into any applicable bugs, security advisories and field notices for running hardware and configuration, if needed in the future		
5.11	Solution should support a single consolidated view of all the objects including links, devices, their relationships, the real-time status of their utilization, and a quick at-a-glance assessment of the current status of the entire system or any subset of the system for better event corelations		
5.12	Flow telemetry should support hardware acceleration so that it is not impacting CPU performace		
5.13	Centralised management appliance or SDN Controller must communicate to south bound devices using open stardard protocol i.e. OPFLEX / OPENFLOW / OVSDB etc. or using Device APIs.		
5.14	Centralised management appliance or SDN Controller must run in "N + N" redundancy to provide availability as well as function during the		

S.No.	Minimum Specification	Compliance (Yes/No)	Remark (If Any)
Make Model			
	split brain scenario		
5.15	In Event of all Centralised management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration.		
5.16	Centralized management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.		
5.17	Centralised management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.		
5.18	All infrastructure required by fabric controllers to support the listed features and scale, should be provided by the bidder		
6	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement for 5 years		

11.9. SAN DIRECTOR (96 Ports) (96 FC ports with 32Gbps)

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make Model				
1.	The switch should have complete non-blocking architecture with 96 ports in a single domain concurrently active at 32 Gbps full duplex and with no oversubscription.			
2.	The switch should support auto-sensing 8,16 and 32 , 64Gbps capabilities.			
3.	The switch should be rack mountable in 2 RU form factor			
4.	All 48 autosensing Fibre Channel ports should be capable of speeds of 8,16 ,32 Gbps and 64Gbps with 32Gbps of dedicated bandwidth for each port.			
5.	FC buffer credits available for data frames should be up to min. 56 per port			
6.	The switch should support non disruptive software upgrade and configuration file installation on newly deployed switches. Additionally, it provides intelligent diagnostics, protocol decoding, network analysis tools for added reliability, faster problem resolution,and reduced service costs.			
7.	The switch should protect SAN and End devices from corrupted frames (inbuilt CRC and Slow Drain detection and Mitigation)			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make Model				
8.	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.			
9.	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience			
10.	Switch management, the management software must support both Fabric wide and Device level management without the additional purchase of software.			
11.	The switch must be able to load balance traffic through an aggregated link with Source ID			
12.	and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.			
13.	a) Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high-priority traffic.			
14.	The switch using FSPF protocol, the switch must be able to load balance up to 16 equal cost paths across the SAN network			
15.	The switch should have USB port which should be able to provision the switch in addition to storing log files, firmware images and configuration			
16.	The switch should offer fabric wide, per-VSAN role-based authentication, authorization, and accounting (AAA) services using RADIUS, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD), and TACACS+.			
17.	SAN Switch should provide end to end visibility of fibre channel SAN traffic. It should inspect I/O flow to bring out a unified view of the infrastructure irrespective of the architecture or OEM of storage arrays, servers or operating systems.			
18.	Switch should provide proactive and predictive troubleshooting and capable of generating automated alarms. Switch should monitor flows between the compute and storage layers, including			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make **Model**				
	the read and the write transactions between a host and the backend storage.			
19.	Hardware and power redundancy (1:1), hot swappable, Monitoring SNMP			

11.10. SAN Switch

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make **Model**				
1	The enterprise class fibre switch should be quoted with minimum 48 FC ports of 32Gbps speed each with necessary Licenses from day 1			
2	The switch should have non -blocking architecture.			
3	The switch must provide 32Gbps ports per module with no oversubscription for intra-module or inter-module switching			
4	The switch should have support for 32G FC ports without changing the hardware			
5	The aggregate backplane bandwidth of switch should be 3 Tbps or higher			
6	The switch should have No Single Point of Failure (SPOF) and all the components should be hot swappable without even scheduled down time.			
7	The switch should have hot swappable N+N redundant Power Supplies			
8	The switch should have hot swappable N+N redundant Cooling Fans			
9	The switch should have feature for non-disruptive firmware update			
10	The switch should have Real time performance monitoring reporting tool			
11	The switch should have support for POST & online diagnostics			
12	The switch should have capability to interface with host-based adapters (HBA) of multiple OEM, supporting multiple Operating Systems			
13	The switch should have support of all leading SAN / NAS disk arrays and tape libraries			
14	The switch should have following security features: a) Must have hardware & Software zoning. b) Policy based security and centralized fabric management.			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
	c) Encryption. d) FC authentication. e) RADIUS, SSH, SNMP f) Switch should support Port Binding/ Masking			
15	The switch should have Inter Switch linking feature to connect two or more FC switches			
16	The switch should have trunking capability. The required software license should be supplied with switch.			
17	Switch should Provide Adaptive Networking services such as Quality of Service (QoS)			
18	The switch should have high availability feature with no performance degradation of switching operation			

11.11. Link Load Balancer

Sl.No	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
1	OEM should be Parent Technology OEM. OEM/Subsidiary should have TAC & R&D facility in INDIA. OEM should be present in India from last 10 Years.		
2	The proposed appliance should be a dedicated appliance, it should not be part of any Firewall or UTM.		
3	Traffic Ports support: 8 x 10 GE Fiber and 8 x 1G Fiber Port from day-1 Device L4 Throughput: 30 Gbps and scalable upto 75 Gbps Layer 4 connections per second: 1 Million Layer 7 requests per second: 2 Million RSA CPS(2K Key): 50,000 ECC CPS (EC-P256): 25,000 with TLS1.3 Support RAM: 32GB and scalable upto 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, — Persistent Hash, — Weighted Hash, — Round-Robin, — Response Time, — Bandwidth, etc		

Sl.No	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
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(NO Multi-Tenancy) 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 The proposed device should support 5 Virtual Instance from Day 1 and scalable upto 30 Virtual Instances.		
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 Mangement 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		

Sl.No	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
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 certified.		
18	Five years Comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support.		

11.12. Server Load Balancer with 10 no of multiple instances

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
1	The proposed OEM should be Parent Technology OEM(Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).		
2	The proposed appliance should be a dedicated appliance, it should not be part of any Firewall or UTM.		
3	**Traffic Ports support:** 8 x 10 GE Fiber and 8 x 1G Fiber Port from day-1 **Device L4 Throughput**: 30 Gbps and scalable upto 60 Gbps **Layer 4 connections per second:** 1.2 Million **Layer 7 requests per second:** 2.4 Million **RSA CPS(2K Key):** 50,000 **ECC CPS (EC-P256):** 25,000 with TLS1.3 Support **RAM:** 32GB and scalable upto 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, — Persistent Hash, — Weighted Hash, — Round-Robin, — Response Time, — Bandwidth, etc		

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
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(NO Multi-Tenancy) 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 The proposed device should support 5 Virtual Instance from Day 1 and scalable upto 30 Virtual Instances.		
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 Mangement 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		

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
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 certified.		

11.13. Firewall/Next Generation Firewall

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Madel				
1	Eligibility Criteria	The proposed External and Internal firewall solution must not be from same OEM.		
2		The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials with highest level of permissions to raise the technical issues in the name of customer, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful System Integrator must provide the login credentials.		
3		During the support period, the proposed solution shall receive the following: a) Firmware and latest OS Upgrades for the quoted model b) Updates/Signatures c) Patches and Fixes		
4		The proposed solution shall not be End-of-support by the OEM for 5 years from the date of bid submission. Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites.		
5		The appliance should not have any active internal or external Wi-Fi component.		
6	Hardware & Networking/Interface features	Solution should be purpose build hardware appliance with Access & Threat prevention controls. The next generation firewall gateway must be capable of supporting these next generation security applications on a unified platform - Stateful Inspection Firewall, Next Gen Firewall, Intrusion Prevention System, User Identity Acquisition, Application Control, URL filtering, Anti – Bot and Anti – Virus, HTTPS Inspection, Advance Sandboxing, Threat Scrubbing, IPsec VPN,		

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Madel				
		Mobile Access, DNS Security, Zero phishing, Security Policy Management, Monitoring and Logging, Logging and Status, Event Correlation and Reporting, Virtual Systems, Networking & Clustering. These security controls must be exclusively supported, supplied by and managed by the vendor.		
7		NGFW solution must be a dedicated hardware appliance & Architecture should support N+N Clustering to provide high uptime and to address multiple node failure instances		
8		Proposed Firewall must not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats		
9		Appliance must have onboard 10/100/1000 Base-T OOB management, Sync 10/100/1000 Base-T port and USB ports dedicated for console management		
10		The appliance must be fully populated with at least 8 X 1/10G SFP+ port fully Populated with 10 Gbps MM Transceiver, 2x 40/100G QSFP28 port from day 1.		
11		The appliance hardware should be a multicore CPU architecture with hyperthreading enabled Memory. The appliance should have adiquate SSD Storage The appliance should support Hot Swappable redundant power supply and Field replaceable fans		
12		The Next Generation Threat Prevention Throughput must be at least 20 Gbps considering all module from day-1		
13		NGFW must support at least 200K connection per second and 5M concurrent connections from day 1		
14		Firewall must support NAT 66, NAT 64 and NAT 46 functionality from day 1		
15		The firewall solution should support Internet Key Exchange (IKE) Version 1 (IKEv1) or Version 2 (IKEv2) for IPSEC VPN		
16		Solution should be supplied with High Availability with Active-Active Load Sharing functionality and commissioned in Active-Active mode with load balancing between the two devices. Solution must support gateway high availability and load sharing with state synchronization		
17		The proposed solution of appliances should support the dynamic routing protocols with readiness for BGPv4 & OSPF		

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Madel				
18		The proposed solution must support different actions in the policy such as deny, drop, Allow, accept		
19		Solution should have hardened OS for both, the appliance, and the management platform.		
20	NGFW Features	NGFirewall should support Identity based controls for Granular user, group and zone-based visibility and policy enforcement		
21		Application control database must contain more than 8000 known applications. The proposed solution must allow free custom application signatures for Homegrown and custom applications.		
22		NGFirewall should support the Identity based logging, application detection and usage controls		
23		Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc		
24		The Firewall shall provide static as well as hide Network Address Translation (NAT) and Port Address Translation (PAT) functionality using automatic and manual NAT		
25		Solution should support remote access VPN module from day one and SI has to provide 50 licenses. The platform should support compliance/risk based access to critical resources.		
26		RA VPN deployment should support split tunneling & full tunneling		
27		The communication between the management servers and the security gateways must be encrypted and authenticated with PKI Certificates.		
28		Solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface		
29		IPS module must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection		
30		IPS module must provide at least two pre-defined profiles/policies that can be used immediately		
31		IPS module must support a software-based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage		
32		IPS application must have a centralized event correlation and reporting mechanism		
33		IPS must support network exceptions based on source, destination, service or a combination of the		

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Madel				
		three.		
34		The administrator must be able to automatically activate new protections, based on configurable parameters (performance impact, threat severity, confidence level, client protections, server protections)		
35		IPS must provide an automated mechanism to activate or manage new signatures from updates		
36		IPS must have a mechanism to convert SNORT signatures and upload in the IPS signatures database.		
37		IPS must have options to create profiles for either client or server based protections, or a combination of both.		
38		Should support more than 10,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy		
39	VPN Features	Overall perimeter security framework to be designed keeping hybrid workforce use case. the appropriate security controls shall be factored to meet the security requirements for all the users. The solution shall provide secure remote access to department applications. The SI can consider the dedicated /integrated VPN solution offerings in the overall architecture.		
40		VPN agent shall have integrated security to detect advanced sophisticated attacks against users including zero day malware and phishing (by scanning form fields), Web form protection, account takeover protection, browser based attacks, and fake login pages. Security capabilities to be provided natively or through 3rd party security agent/solution.		
41		Identity protection – while connected to internet, in work from home scenario, solution must restrict department corporate identity exposure on untrusted web sites. For instance, users shouldn't be allowed to use corporate username & password on external websites.		
42		Conditional access - provide the conditional access based on the organization department security policy. The solution should provide following compliance checks to validate end point posture before opening the access to application-Applications,		

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Madel				
		File name, File path registry, Process names, Domain name		
43	Threat prevention	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall		
44		Anti-bot application must be able to detect and stop suspicious abnormal network behaviour		
45		Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications		
46		Anti-Bot and Anti-Virus must have real time updates from a cloud-based reputation services. Look for C&C traffic patterns, not just at their DNS destination		
47		The solution should have detection and prevention capabilities for DNS tunnelling attacks		
48		DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication		
49		Solution must protect from DNS Cache Poisoning and prevents users from accessing blocked domain addresses. DNS Exfiltration and Domain Generation Algorithm (DGA) to protect against the DNS tunnelling. System Integrator has to provide additional license to achieve DNS protection.		
50		Antivirus engine must be integrated on the NGFW platform with inspection of 75+ file type		
51		Anti-virus application must be able to prevent access to malicious websites		
52		Anti-Virus must be able to scan archive files. Anti-Virus policies must be centrally managed with granular policy configuration and enforcement		
53		The solution should support detection & prevention of Cryptor's & ransomware viruses and variants (e.g. WannaCry, Crypt locker , Crypto Wall…) through use of static and/or dynamic analysis		
54		The proposed NGFW OEM must support on-prem Sandboxing solution (not cloud based) to prevent from Zero day attacks. The Sandboxing solution must have CDR functionality in which infected content from files can be stripped and cleaned version of files can be delivered to recipients.		

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Madel				
55		The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques.		
56	Administration, Management and Logging	Management and Firewall should be two separate systems. Management can be virtual appliance or bare metal hardware installation. SI has to provide the pre-requisites to implement the solution.		
57		NGFW appliances must be managed from a centralized dedicated management system separate from the NGFW appliance		
58		Device Management system includes Centralized Management, logging, reporting and basic event correlation functionality in the single appliance.		
59		Device Management system should provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections or the connections per second counter. It must provide a security rule hit counter in the security policy.		
60		Management platform should provide autonomous threat prevention security policy.		
61		Management server must have the capability to manage both NGFW and Anti-APT device from same management console to have a holistic view/reporting of threat vectors. On-prem firewall and firewall deployed on cloud for DR must be manage from same management console.		
62		Solution must be able to segment the rules base in favor of delegation of duties in which changes in one segment will not affect other segments on the same autonomous system.		
63		The device must provide a minimum basic statistic about the health of the firewall and the amount of traffic traversing the firewall.		
64		Solution must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant policy segment for an autonomous system		
65		Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat		

S.No.	Parameters	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make **Madel**				
		Prevention policy		
66		The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance		
67		optionally, Solution must have capabilities for multi-domain management and support the concept of global security policy across domains.		
68		Support A new MITRE ATT&CK view to investigate security issues according to the MITRE defense models, and extract immediate action items based on the mitigation flow		
69		DR security infrastructure on cloud must be in sync with the external firewall therefore, cloud security solution must be from same OEM.		
70		The Appliance should be supplied with minimum 10 virtual license (perpetual)		

11.14. Web Application Firewall with 10 no of multiple instances

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
1	The proposed OEM should be Parent Technology OEM(Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).		
2	The proposed appliance should be a dedicated appliance, it should not be part of any Firewall or UTM.		
3	**Traffic Ports support:** 8 x 10 GE Fiber and 8 x 1G Fiber Port from day-1 **Device L4 Throughput**: 30 Gbps and scalable upto 60 Gbps **Layer 4 connections per second:** 1.2 Million **Layer 7 requests per second:** 2.4 Million **RSA CPS(2K Key):** 30,000 **ECC CPS (EC-P256):** 20,000 with TLS1.3 Support **RAM:** 64GB and scalable upto 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	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2		

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
5	The solution must be able to decrypt SSL web traffic between clients and web servers		
6	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1		
7	**<u>The proposed appliance should support the below metrics:</u>** — Hash, — Persistent Hash, — Weighted Hash, — Round-Robin, — Response Time, — Bandwidth, etc		
8	**Following 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		
9	The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature(NO Multi-Tenancy) 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 The proposed device should support 5 Virtual Instance from Day 1 and scalable upto 30 Virtual Instances.		
10	The proposed Hardware must have Bandwidth Mangement feature from Day 1		
11	The proposed device should support standard VRRP (RFC - 2338) or Equivalent for High Availability purpose (No Propertary Protocol)		
12	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend		
13	The solution should have support for multiple VLANs with tagging capability		

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
Make Model			
14	The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure		
15	Should have ability to upgrade/downgrade device software Images.		
16	Device should be accessed through the below: • Using the CLI • Using SNMP • REST API • Using the Web Based Management		
17	The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.		
18	WAF should have the flexibility to be deployed in the following modes: Reverse proxy Out of Path (OOP)		
19	Solution should dynamically understand the Changes on the Web/Application Server		
20	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats		
21	The WAF should support the following escalation modes: a) Active, b) Bypass, c) Passive		
22	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications		
23	**Hiding Sensitive Content Parameters:** It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)		
24	WAF should support for IPv4 and IPv6 traffic along with DNS functionality from day-1		
25	**Auto Policy Optimization**		
a	• Known Types of Attack Protection - Rapid Mode		

Sl.no	Specifications	Compliance (Yes/No)	Remarks (If Any)
Make Model			
b	• Zero Day Attack Blocking - Extended Mode		
c	• Working in Learn Mode		
d	• Auto Discovery		
26	**Following Threats should be protected by the proposed WAF solution:**		
a	Parameters Tampering		
b	Cookie Poisoning		
c	SQL Injection		
d	Session Hijacking		
e	Web Services Manipulation		
f	Stealth Commands		
g	Debug Options		
h	Backdoor		
f	Manipulation of IT Infrastructure Vulnerabilities		
g	3rd Party Misconfiguration		
h	Buffer Overflow Attacks		
f	Data Encoding		
g	Protocol Piggyback		
h	Cross-Site Scripting (XSS)		
f	Brute Force Attacks		
g	OS Command Injection		
h	Cross Site Request Forgery (CSRF)		
g	Information Leakage		
h	Path (directory) Traversal		
f	Predefined resource location		
g	Malicious file upload		
h	Directory Listing		
27	**The proposed WAF should support the Activity Tracking, which should include the following:**		
a	Dynamic IP		
b	Anonymity		
c	Scraping		
28	**Device Fingerprint-based tracking**		
a	The Proposed WAF should support Device Fingerprint technology or equivalent by involving various tools and methodologies to gather IP agnostic information about the source.		
29	Bidder should propose Centralized Management & Reporting Solution from Day 1.		
30	The proposed appliance/software should be EAL2 certified.		

11.15. DLP Solution

Sr. No.	Technical Specification	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
1.	**Network Data & Cloud Monitoring and Prevention**		
1.1.	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to enforce policies by URL's, domains or URL categories either natively or by integrated Web Security solution. The solution should be able to monitor FTP traffic including fully correlating transferred control information and should be able to monitor IM traffic even if its tunneled over HTTP protocol.		
1.2.	The bidder to sure the proposed DLP Solution OEM's should provide proxy solution for content inspection nativelty and also make sure the seemless and centralized deployment for DLP and URL filtering(proxy)		
1.3.	The solution should be able to block outbound emails sent via SMTP if its violates the policy		
1.4.	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.		
1.5.	The solution should be able to prevent content getting posted or uploaded to destinations (Web,Email domains etc..). The gateways protecting the email and web traffic should be hardware based provided by the OEM.		
1.6.	The solution should support Email DLP in Microsoft Azure/on prem for Gsuite. All licenses required for the same should be included and management should be from the same centralized management platform		
1.7.	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document.The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI		
1.8.	The DLP solution should be able extend the policies to the known public sanctioned cloud applications with a license upgrade in future for the application data risk.		
2.	**Endpoint Data Monitoring & Protection**		
2.1.	The solution should have more than 50 pre-defined applications and multiple application groups and allow each application/application		

Sr. No.	Technical Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application.The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.		
2.2.	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network. The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads. The solution should be able to enforce different policies for desktops and laptops.		
2.3.	The solution should Provide "Cloud Storage Applications" group which monitor sensitive content accessed by these cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Windows 10,11 and MAC OSX) -Amazon Cloud Drive, Box, Dropbox, Google Drive, SkyDrive, ICloud.		
2.4.	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media. It Should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.		
2.5.	Endpoint solution should support win 32 and 64 bit OS, Mac & Windows OS,Support wide variety of platforms(Below support from Day1):Windows 8, Windows 8.1, and 10, Windows server 2012 R2, Windows server 2016, Windows server 2019, Mac OS X -10.14.X,10.15.x,11.x VDI (Citrix and VMWare)		
2.6.	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.		
2.7.	The solution should have ability to detect cumulative malware information leaks. The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns. The solution should able to detect and Block the sensitive information uploads to Group of P2P software :-		

Sr. No.	Technical Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	Bit Tornado, Bit torrent, eMule and eMule FrostWire		
2.8.	The Endpoint DLP Solution must be able to encrypt data when business classified data is sent to removable media drives. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement		
2.9.	The Proposed Endpoint DLP Solution must be able to apply DLP policies to Microsoft RMS encrypted files on Windows endpoints to have better understanding oh how RMS is being used by employees to protect sensitive data.		
2.10.	Endpoint must support the following operations on sensitive data that your DLP endpoint can address: • Copy and paste controls (i.e., clipboard activities) • Control of printing to local or network printers • Save content to different locations, including saving to: • Local folders • Remote file shares • Removable drives attached to an endpoint system, such as USB drives • Saving to cloud storage locations		
2.11.	The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments. Encryption Keys are also should be isolated between the different departments. The endpoint installed should have the capability to create the Bypass ID after validation by the administrator by generating the Passcode.		
2.12.	The solution should have a comprehensive list of pre-defined policies and templates with over 1700+ patterns to identify and classify information pertaining to different indutry like Energy, Petroleum industry vertical etc and India IT Act.		
2.13.	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file		
2.14.	The solution should be able to detect and block encrypted and password protected files without reading the encrypted content.		
2.15.	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders		
2.16.	The solution should be able to recursively inspect the content of compressed archives		
2.17.	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different		

Sr. No.	Technical Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	columns in a database		
2.18.	The solution support the print content to detect data leaks over print channel.		
2.19.	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.		
2.20.	The solution should enforce policies to detect low and slow data leaks		
2.21.	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.		
2.22.	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document also solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.		
2.23.	The Proposed DLP Solution must be GDPR Compliant with each state PII information proposed DLP Solution must be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis.		
2.24.	DLP Solution must have data classfication intgeration and also the integration with Data classification tools cush as Bolden James , Titus , AIP to import classification labels into the DLP system and to correct the mistakenly classified labels in DLP discovery as per the DLP defined policies		
2.25.	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.		
2.26.	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.		
2.27.	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI		
2.28.	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the		

Sr. No.	Technical Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	match and should allow opening of original attachment directly from the UI		
2.29.	The incident should display the complete identity of the sender(Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager		
2.30.	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view along with Single management for managing policies for DLP, Anti-spam and URL filtering(proxy).		
2.31.	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients		
2.32.	The reports should be exported to at least PDF/ HTML formats.		
2.33.	The system should provide options to save specific reports as favorites for reuse		
2.34.	The system should have lots of pre-defined reports which administrators can leverage		
2.35.	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console		
2.36.	The DLP Solution must provide visibility into Broken Business process. For ex:-if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong.		
2.37.	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the sameuser that have the same classification are combined into a group and DLP case card.		
2.38.	The DLP solution should support as an API be able to provide the risk adaptive based protection by dyanimcally calling the action plan based on the Risk.		
2.39.	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce an report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.		

Sr. No.	Technical Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
2.40.	The system should allow automatic movement or relocation of file, delete files during discovery		
2.41.	The system should display the original file location and policy match details for files found to violate policy		
2.42.	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes		
2.43.	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.		
2.44.	The OEM should have own technical support center in India.		
2.45.	The OEM should be present in India for more than 10 years and large customer reference		
2.46.	The OEM should be listed in Gartner Peer Insight with 4.5 and above on rating of more than 300 reviews.		
2.47.	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator		
2.48.	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.		
2.49.	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notifciation email itself.		
2.50.	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identify of the user and the forensics of the incident		
2.51.	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint		
2.52.	The system should allow a role only to view incidents but not manage or remediate them and system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents also system should allow incident managers and administrators to use their Active directory credentials to login into the console		

11.16. DDoS

Sl.No	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make **Model**			
1	OEM should be Parent Technology OEM. OEM/Subsidiary should have TAC & R&D facility in INDIA. OEM should be present in India from last 10 Years.		
2	The Proposed solution should be a Dedicated appliance (NOT a part of Router, UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).		
3	DDoS Flood Attack Prevention Rate: 14MPPS (In addition to Legitimate throughput) Mitigation Throughput: 20Gbps Legitimate throughput handling: 5Gbps from day-1 and scalable upto 10Gbps Attack Concurrent Sessions : Unlimited Inspection Ports: 8 x 10 SFP+ and 4 x 1G RJ45 Ports fully Populated with 10 Gbps MM Transceiver Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available		
4	System should support horizontal and vertical port scanning behavioral protection.		
5	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms and stateless solution to detect and defend against threats.		
6	Behavioral DoS (Behavioral Denial of Service) Protection should 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, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood • ICMP flood • IGMP flood		
7	System should have DNS Flood protection for each type of query including, A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV etc.		
8	Positive Security Model should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic		

Sl.No	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
9	System should support DNS Challenge and DNS Rate Limit.		
10	System should support HTTP Challenge Response authentication without Scripts		
11	System should have SIP Flood Protection, UDP and UDP Fragmented Flood.		
12	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support inbuilt Signatures apart from custom Signatures from Day 1.		
13	Solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment. Also, it should transparent to L2TP, GRE, IP in IP traffic.		
14	The Proposed Solution should protect against Zero Day DDoS Attacks within few seconds, without any manual intervention.		
15	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. DNS Protections.. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection.		
16	System should protect from DDoS attacks behind a CDN Network.		
17	The proposed Device should use the following Block Actions : 1) Drop packet, 2) Reset (source, destination, both), 3) Suspend (source IP address, source port, destination IP address, destination port or any combination), 4) Challenge-Response for TCP, HTTP and DNS suspicious traffic		
18	System should have atleast below tracking mechanism to counts and act upon ; 1. All 2. Per Source 3. Per Destination 4. Per Source & Destination Pair 5. Track Returning Traffic from Destination and Suspend Corresponding Sources		
19	The solution should provide Geo-Location blocking, Active Attacker Feeds and Signature Update Service from day-1		
20	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks. All the baseline information including attack footprint should		

Sl.No	Minimum Specification	Compliance (Yes/No)	Remarks (If Any)
Make Model			
	be sync b/w appliance and scrubbing centre.		
21	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1.		
22	Five years Comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support.		

11.17. Advanced Persistence Threat - Anti APT Solutions

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
1	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance and should have capabilities to configure files, IP, URLs and Domains to Black list or white list			
2	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard and must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations where applicable.			
3	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment and should detect lateral movement (attack activities) inside the network (beyond C&C connections) also should have utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behaviour.			
4	Should have Advanced Threat Scan Engine to detect zero-day threats, embedded exploit code, rules for known vulnerabilities and enhanced parsers for handling file deformities also should have a built-in document vulnerabilities detection engine to			

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make **Model**				
	assure analysis precision and analysis efficiency also should be able to store packet captures (PCAP) of all malicious communications detected by sandbox also should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.			
5	Solution must be a custom built on premise dedicated Anti-APT solution and should not leverage same firmware as Firewall also should not be from NGFW, Routing, switching based vendor to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.			
6	Should performs static and dynamic analysis to identify an object's notable characteristics: AutoStart or other system configuration, Anti-security and self-preservation, Deception and social engineering, File drop, download, sharing, or replication, Hijack, redirection, or data theft, Malformed, defective, or with known malware traits, Process, service, or memory object change and Rootkit, cloaking, Suspicious network or messaging activity			
7	Should have extensive detection techniques utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behaviour also Virtual Analyzer generates analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations			
8	Should detect from Targeted attacks and advanced threats, Targeted and known ransomware attacks, Zero-day malware and document exploits, Attacker behaviour and network activity, Web threats, including exploits and drive-by downloads, Phishing, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, keyloggers and Disruptive applications			
9	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and data Exfiltration.			
10	Proposed solution should be able to provide customizable sandbox to match customer's endpoint environments. Access different information about Affected Hosts on the following views: Displays a summary of affected hosts by attack phase,			

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make **Model**				
	provides access to Host Details views and Displays host event details in chronological order displaying affected Hosts information that have been involved in one or more phases of a targeted attack			
11	Should have combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits & threats used in targeted attacks including Detection of zero-day threats, Detection of embedded exploit code, Detection rules for known vulnerabilities and Enhanced parsers for handling file deformities			
12	Should provide Threat execution and evaluation summary and In-depth tracking of malware actions and system impact, including the following: Network connections initiated, System file/registry modification and System injection behavior detection also should have capability to do retrospective scan on CnC, Script Analyzer, Automatically send executable to sandbox, can crack password protected compressed files			
13	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 100+ protocols for inspection also should support In- line deployment mode supporting TLS decryption along with monitor Inter-VLAN traffic on a Port Mirror Session/TAP mode.			
14	OEM must have contributed at least 50 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.			
15	Proposed solution should have seemless natively integrate with Endpoint Security, HIPS and NIPS components as per RFP specifications having common threat sharing platform for suspicious object Sync to achieve holistic visibility and mitigation of any unknown/Zeroday threat also Integration with 3rd party vendors for SO distribution i.e. Check Point Open Platform for Security (OPSEC), Palo Alto Firewalls, IBM Security Network Protection and Tipping Point			
16	Should support extensive File Types i.e. Compressed Files (7z, rar, zip, cab, jar, gz, tar, bz2), Script Based (bat, ps1, vbs, js), Executables (exe, dll, scr) and Office Documents / PDF (doc / docx, ppt / pptx, xls / xlsx, pdf, mdb), .bat, .cmd, .cell, .chm, .csv, .class, .cla, .dll, .ocx, .drv, .doc, .dot, .docx, .dotx, .docm, .dotm, .cpl, .exe, .sys, .crt, .scr, .gul, .hta, .htm, .html,			

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make **Model**				
	.hwp, .hwpx, .iqy, .jar, .js, .jse, .jtd, .lnk, .mov, .pdf, .ppt, .pps, .pptx, .ppsx, .psl, .pub, .rtf, .slk, .svg, .swf, .vbe, .vbs, .wsf, .xls, .xla, .xlt, .xlm, .xlsx, .xlsb, .xltx, .xlsm, .xlam, .xltm, .xml, .xht, .xhtml, .url			
17	Should monitors all inbound and outbound network traffic and should allow administrator to categorize files as safe based on Hash values. Solution must support scanning of 1400 samples/hour processing capacity, also should able to run at least 20 parallel sandboxes images scalable up to 60 for analysis of payload, also support 1 Gbps of aggregated inspection throughput using single appliances by intercepting traffic of different segments also should have 2 TiB in RAID 1 of on box storage from day one with a scalability of 8 TiB			
18	Should support custom sandbox images without any programming effort including Domain Check, Software Check, Patches, OS Language, Configurations, User Settings check, Requisite file check Office version check, Windows License check Browser Check (Sandbox Customized with OS and Applications in the Environment) also should support customized sandbox solution supporting following operating systems (Win7, Win8/8.1, Win 10, Windows Server 2003,2008, 2012, 2016, 2019, 2022 and Linux)			
19	Proposed solution should have inbuilt mitigation capability at the endpoint have functionalities of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, DLP, EDR / XDR capabilities in a single agent and proposed solution provider should have its own native AV Engine and should not use any 3rd party solution provider			
20	The Proposed solution should have >99% breach detection rate and Security Effectiveness as per NSS BDS 2017/2018 report and ICSA certified having achieved >99% effectiveness as per 2022 Advanced Threat Defence (ATD) Test Report also should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports			
21	Proposed solution should be implemented by OEM engineer also OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the deployed solution and OEM payroll TAM should present health check report to customer premise			

11.18. NIPS (Network Intrusion Prevention System)

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make: **Model:**				
1	Solution should have 5 Gbps of IPS inspection throughput with scalability up to 20 Gbps, supporting scalable architecture delivering 30 million legitimate concurrent Sessions/Concurrent connections and 200,000 new Connections per second from day-1			
2	Should introduce latency <40 microseconds and information should be publicly available and documented also should have inbuilt SSL decryption capability.			
3	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines. Inspection Ports supported : 6 x 10G Fiber and 6 x 1G Copper Ports fully Populated with 10 Gbps MM Transceiver from day-1. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port			
4	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality.			
5	Should support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption and memory errors also should supports inspection of Asymmetric traffic consisting jumbo frames, DGA Defense filters, Machine learning, Virtual patching capability.			
6	Should protect all Inter-VLAN traffic in the same way as in-line deployment protecting all Inter-VLAN traffic in the same way as in-line deployment also appliance should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution			
7	Should have Vulnerability based filters covering entire Vulnerability footprint, which understands various exploit patterns and support firmware, signature upgrade/Reboot without require downtime also should have the capability to convert other vendor's signature(such as snort)			
8	Should have machine learning to detect exploit kit landing page, bypass traffic for NIPS internal issues i.e. memory hang, firmware crash having bandwidth rate limit to control the unwanted traffic such as P2P, Online Game, etc.			
9	Should have at least inbuilt 15000 signatures/Filters pertaining to security and applications apart from user define signatures/filters also having a power failure bypass modular that can support hot swappable function which allows traffic to bypass even after a modular get unplugged out of IPS Box during the RMA procedure			
10	Should be deployed in High Availability, Rate limit on non-business traffic i.e. bit torrent and Big data engine in management platform for			

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make: **Model:**				
	faster report generation also solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters			
11	Should be able to support GTP inspection for GPRS/3G mobile networks and should support SPAN,/TAP and Inline mode deployment also should be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score			
12	Should have inbuilt fail-open and fail-close capability for integrated fiber ports also should support out-of-the-box configuration that will protect the network straight from the initial deployment			
13	Should not stabilize performance by configuring/enabling/disabling DSRI/Intelligent mode/HTTP client body extraction depth values having dual plane architecture for Data and Control plane having its local management to configure policies and reporting and supporting zero power interface cards to allow traffic flow without inspection in case of appliance power failure			
14	The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report also support SNMP and a private MIB that can be utilized from an Enterprise Management Application such as HP Openview, MRTG			
15	Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (Eg. Selecting rules, configuring policies, updating policies, etc...) also solution should provide recommendation for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.			
16	Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto-Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.			
17	The management server must support the archiving and backup of events and export to NFS, SMB, SCP and sFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML and should be able to manage locally independently without any centralized management server also should serve as a central point for security policies management including versioning, rollback, import and export (backup) tasks supporting 'threat insights' dashboard that show correlated data such as how many breached			

S.No	Parameters	Specification	Compliance Yes/No	Remarks
Make: **Model:**				
	host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered			
18	Proposed solution should have customized sandbox capability including Domain Check, Software Check, User Settings check, Requisite file check Office version check, Windows License check Browser Check (Sandbox Customized with OS and Applications in the Environment) supporting operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016, 2019 and Linux platforms having >99% breach detection rate and Security Effectiveness as per NSS BDS report.			
19	Proposed solution should get integrate natively with Anti APT solution as per RFP specifications having common threat sharing platform as per RFP specifications to share threat intelligence to mitigate zero-day attacks and proposed OEM should be contributing at least 30 zero-day/Undisclosed vulnerabilities to Microsoft continuously from past 5 years and data should be publicly available			
20	The Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leaders Quadrant of Gartner Magic Quadrant report for Intrusion Prevention Systems in each of the latest last two reports having at least security effectiveness rate 99 % as per 2017/2018 NSS Labs NGIPS report.			
21	Proposed solution should be implemented by OEM engineer also OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the deployed solution			

11.19. HIPS (Host Intrusion Prevention System)

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make **Model**				
1	Proposed solution should support modules including Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention and recommendation scan must be available in single agent supporting multiple platforms of server operating systems i.e. Windows, Linux RedHat, CentOS, Oracle, Debian, SUSE, Ubuntu, Solaris, AIX, Amazon Linux also should offer protection for virtual, physical, cloud and docker container environments.			
2	The firewall shall be bidirectional for controlling both inbound and outbound traffic and should have the capability to define different rules to different network interfaces including filter traffic based on source and destination IP address, port, MAC			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	address, direction etc. and should detect reconnaissance activities such as port scans and should support stateful inspection functionality			
3	Solution should provide policy inheritance exception capabilities and ability to lock computer (prevent all communication) except with management server also should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules and should be able to detect protocol violations of standard protocols and provision inclusion of packet data on event trigger for forensic purposes.			
4	The proposed solution should support Deep Packet Inspection (HIPS/IDS) and should support creation of customized DPI rules if required supporting virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window also virtual Patching should be achieved by using a high- performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.			
5	Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (Eg. Selecting rules, configuring policies, updating policies) also should provide recommendation for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.			
6	The solution should allow imposing HTTP Header length restrictions and have the capability to inspect and block attacks that happen over SSL also should allow or block resources that are allowed to be transmitted over http or https connections and capable of blocking and detecting of IPv6 attacks and should do detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.			
7	Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities) also Deep packet inspection should have			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.			
8	Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.			
9	Solution should work in Tap/detect only mode and prevent mode and support automatic and manual tagging of events also have CVE cross referencing when applicable for vulnerabilities also should provision inclusion of packet data on event trigger for forensic purposes and shall protect against fragmented attacks also should allow to block based on thresholds			
10	Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto- Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.			
11	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions also should be able to monitor System Services, Installed Programs and Running Processes for any changes also extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).			
12	Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored also should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
13	Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/assignment when not required also should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities also Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.			
14	In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so also should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto Provisioned based on Server Posture having an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features and management should support both windows as well as Linux platform in high availability configuration for DC/DR setup.			
15	Solution should support the following: Multiple groups of hosts with identical parameters, Regex or similar rules to define what to monitor, Ability to apply a host template based on a regex of the hostname, Ability to exclude some monitoring parameters if they are not required, Ability to generate E Mail and SNMP alerts in case of any changes, Solution should support creation of custom Integrity monitoring rule and Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.			
16	Anti-malware should support Real Time, Manual and Schedule scan and should have flexibility to configure different real time and schedule scan times for different servers and should have feature to try & backup ransomware encrypted files and restoring the same as well also should support excluding certain file, directories, file extensions from scanning (real time/schedule) and use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
17	The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files, Flash files, RTF files and and/or other objects using Machine learning also should support True File Type Detection, File extension checking and have heuristic technology blocking files containing real-time compressed executable code.			
18	The proposed solution should be able to perform behaviour analysis for advanced threat prevention and have its own threat intelligence portal for further investigation, understanding and remediation an attack also also should have Ransomware Protection in Behaviour Monitoring along with highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.			
19	Solution should have a Log Inspection module which provides the ability to collect and analyse operating system, databases and applications logs for security events also should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules also should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/Windows servers use the same base security profile allowing further fine tuning if required.			
20	Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/assignment of rules when not required also support decoders for parsing the log files being monitored also have customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match also ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.			
21	Solution should allow administrators to control what has changed on the server compared to initial state and should prevent unknown and uncategorized applications from running on critical servers also must support Global Blocking on the basis of Hashes and create blacklist for the environment also should have option to allow to install new software or update			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	by setting up maintenance mode and should have ability to scan for an inventory of installed software & create an initial local ruleset.			
22	Change or new software should be identified based on File name, path, time stamp, permission, file contents etc. and must have ability to enable maintenance mode during updates or upgrades for predefined time period, Logging of all software changes except when the module is in maintenance mode and Should support Windows & Linux operating systems with ability to enforce either Block or Allow unrecognized software and must support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.			
23	solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's and should give the flexibility of deploying features either as agent based and agentless for different modules depending on organization's data center environment also should have seamless integration with Anti-APT solution as per RFP specifications bi-directionally to detect and mitigate zero day threats having common threat sharing platform for holistic visibility and control			
24	Solution should support the logging of events to a non-proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL also administrators should be able to selectively rollback rules applied to agents and should maintain full audit trail of administrator's activity and should have an override feature which would remove all the applied policies and bring the client back to default policies.			
25	Proposed solution should be implemented by OEM payroll engineer also OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit , findings and recommendations of the deployed solution also solution should be Leader in server security market as per IDC latest report also solution provider should be leader in advance Global Vulnerability Research and Discovery market share as per latest Frost & Sullivan Reports also OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publicly available.			

11.20. Zero Trust Network (500 Users)

Sr. No.	Technical Specification	Compliance (YES/NO)	Remarks (If Any)
Make Model			
A	**General Specification**		
1.	The proposed solution must be ON-Premises and the OEM should have services hosted in at least 2 own/ ON-premises / co-located in India with local compute		
2.	The proposed solution must support 500 concurrent users license for ten applications from day one and must support unlimited user license and pay per use model to support future scalability needs.		
3.	The proposed platform must have MSI/software packages centrally push functionality to all the remote laptops/desktops		
4.	The zero trust endpoint agent should be agnostic to the device platform and must support devices running Linux, Windows, iOS, and Android operating systems.		
5.	The proposed solution must have endpoint support including client, clientless, secure browser, admin agent, nand on-admin agent as needed by each application type and supporting secure internet gateway and zero trust network access capabilities		
6.	The proposed OEM must have the following certificates: ISO 27001 certification or CERT-In Certified Solution		
7.	The proposed OEM solution/features must work with a single licensing model and support both Zero trust network access and application access. This is to ensure priviledged administrators have priviledged access and others users have applicaiton access only.		
B	**Platform Support**		
8.	The proposed solution must support filtering of traffic on all ports and protocols including all TCP, UDP ports and for ICMP and must support blocking communication based on user, IP, port etc. It should support FQDN and wildcarded FQDNs as blindable or standalone conditions in firewall filtering policy.		
9.	The proposed solution must include support for IP address-based access policies for private applications to facilitate easy adoption of ZTNA without altering the existing setup.		
10.	The solution shall provide secure remote access to private applications hosted on-premises using leading technologies such as Secure tunnelling with an application connector/gateway and the broker deployed in the customer's Data Center.		
11.	The proposed solution must support VoIP protocols like SIP and h.323 to Secure access with a VoIP phone system.		
C	**Multi-Factor Authentication**		
12.	The solution should provide multi-factor authentication before granting access to applications.		
13.	The solution should be a completely automated orchestration involving Multi-Factor Authentications (Powered by inpackage SMS, E-mail, indeginiously developed T-OTP Mobile Application) and inbuilt homegrown		

Sr. No.	Technical Specification	Compliance (YES/NO)	Remarks (If Any)
Make Model			
	IDP. This means the Solution should have its own authenticator app for authentication of multiple apps and support push notifications with support for android (6 & above), iOS (10 & above) mobile platforms. Note: All the elements defined on the Orchestration should be developed and delivered by a single OEM.		
14.	The Prosposed Solution should have Inbuilt T-OTP based Solution for MFA (Multi-factor Authentication) along with softtware based App authenticators for ios, Android is must as part of ZT Solution [SMS, Email, Push Noticatifcations, app Authenticators, web auth or offline authentication through authenticator application]		
15.	The proposed MFA Solution Should be tightly inbuilt feature with Zerotrust Network Access Solution to provide Encrypted communication to the applications hosted on the Datacentres which are invisible to outside world & 2FA Should be on the Single Console for Ease of Administration. The Solution should have its own authenticator app for authentication of multiple apps and support push notifications with support for android(6 & above), iOS(10 & above) mobile platforms		
16.	The proposed multifactor authentication must support for local user, Active Directory, Open LDAP and Azure AD		
17.	The proposed solution must have own authenticator application for multifactor authentication and also support google authenticator and Microsoft authenticator		
18.	The proposed solution must support third party SMS gateway and Email gateway for OTP delivery		
19.	The proposed solution must be able to integrate Biometric based authentication like finger print and facial authentication as 2FA		
20.	The proposed solution must have option to restrict/allow user MFA authentication traffic based on whitelist/blacklist Public IP Address		
21.	The Proposed Solution should have Capability to generate offline codes without internet , where in user can access the applications hosted in DC post domain joined machine without prodcutivity loss of the users		
22.	The Proposed MFA solution should have the Capability for windows Log-on mechanism before the machine boots up there by interagating with Active directory , including SAML Insertions for all the applications and Single sign on access solution for all the applicatiions hosted in the DC or on cloud based SAAS Application /Web Applications		
23.	The Proposed MFA solution should Support Single Sign-On for All types of Web application using NTLM SSO , Form based SSO & SAML, Customer Connectors for the NON-SAML Based applications		
24.	The Solution should have the Capabilities to capture all activities at admin console shall have an audit trail of all logon attempts and operations. Confidential Logs shall be tamper proof. Tools shall be provided to check the integrity of logs.		
25.	The Proposed MFA solution should accommodate multiple methods of authentication including hardware-based token solutions, software-based,		

Sr. No.	Technical Specification	Compliance (YES/NO)	Remarks (If Any)
Make Model			
	risk based Web auth 2.0, FIDO, HOTP / TOTP based on OATH specifications, Web Auth , FIDO Functionality for passwordless authentication		
26.	The MFA solution shall support authentication mechanisms such as PKI based token, User ID/ Password/ Q and A (challenge response), OTP, RADIUS, out-of-band OTP, any other custom authentication scheme.		
27.	The MFA solution shall support emergency access capability in case of loss, misplace or damage of 2nd factor authentication device (token/card) by offline codes meachnism		
28.	The proposed MFA solution must support for ssh, telnet and rdp protocol through radius and tacacs+ protocol		
29.	The proposed solution should support contextual MFA for all the network devices using Radius protocol		
D	**Security Feature**		
30.	The Zero Trust (ZT) Solution Architecture should be designed such that, Authentication and authorization must happen on a separate channel before allowing user to connect to any service / applications - i.e. only authentication and authorization controls are alloto communicate via a specific port or control channel. All authentication and authorization must happen over an encrypted channel, Dcoumentary evidence should be provided by OEM as per the Cloud Security Allaince Architecture		
31.	Access to applications / services must only be allowed from pre-authenticated and pre-authorized devices and users		
32.	The proposed solution must employ Single Packet Authorization protocol with HMAC or certificates.		
33.	The proposed solution must use SPA protocol followed by mutual TLS protocol to begin the device verification process followed by the user authentication process.		
34.	All users must be authenticated either locally by the Controller or via a 3rd party authentication system such as AD, LDAP, RADIUS, SAML, 2FA providers etc.		
35.	When a client initiates an access to the available service, the Controller is notified first, and the Controller in turn notifies the Gateway to accept the connection from the client.		
36.	The proposed remote agent connects to the central controller using SPA protocol followed by mutual TLS protocol and if both SPA and mutual TLS are successful, the Gateway accepts the connection and provides access to the application / service.		
37.	Any endpoint device without the client software will not be able to connect to the Controller or the Gateway NOR discover/scan the services/applications running behind the Gateway as the SPA will fail. This effectively makes the Gateway invisible to all without a valid client software and valid client certificate. This will defeat many network attacks such as Denial of Service (DoS), MITM and others.		
38.	The proposed solution should apply the principles of least privilege access to give users secure and seamless connectivity to private applications hosted		

Sr. No.	Technical Specification	Compliance (YES/NO)	Remarks (If Any)
Make Model			
	in the customer's data centre while eliminating unauthorized access and lateral movement.		
39.	The proposed solution must support file type control by users, groups and destinations from day 1. File type control should be supported over HTTP, HTTPS, FTP over HTTP and Native FTP protocols from the secure internet gateway service.		
40.	The proposed solution should support providing privilege application access on both TCP and UDP protocols on almost all associated ports. It should support both web- and non-web-thick client-based application access.		
41.	The proposed ZTNA and ZTAA solution must not put remote users on the corporate network and should provide user-to-application segmentation by connecting users to specific authorised apps, limiting lateral movement.		
E	**Manageability**		
42.	The solution must support deployment of Gateways in multiple Data Centre with minimum human interaction.		
43.	The solution must allow simple self-service style with user sign-up and activation method of deployment		
44.	The solution must provide a single web based management console to manage user provisioning, device provisioning and policy management across all Gateways deployed in the enterprise		
45.	The solution must support access policies to be configured centrally irrespective of the location of the applications / services or the location of the Gateways.		
46.	The solution must support role based administration. This will ensure that different administration tasks can be delegated to different administrators / teams.		
F	**Agent based Zero Trust Access Feature**		
47.	The endpoint agent should support USB blocking,Clip board control and Screen shot control with custom water marking to identify the source of data loss.		
48.	The solution must support a device posture check capability on the end user machines for both internet and private application access to ensure applications are being accessed only form a trusted authorized device.		
49.	The device posture check capability must support validating File Path, Registry Key, Client Certificate, Domain Joined, Process Check, Firewall, Encryption, Dand etect Antivirus along with AV signature update, and OS Version before providing access to the private application. The above validation of the mentioned device posture check conditions must be supported directly through the zero trust endpoint agent without requiring the installation of any additional client or application on the endpoint. It should support periodic assessment of the device posture, and the minimum value for posture re-assessment should be as low as 2 minutes to ensure continued compliance.		

Sr. No.	Technical Specification	Compliance (YES/NO)	Remarks (If Any)
Make Model			
50.	The endpoint agent of the proposed zero trust should have a packet capture capability as a built-in feature for ease of troubleshooting with a better user experience.		
51.	The Proposed solution should be able to block a set of exe and bat files as defined by administrators.		
52.	The solution proposed must able to perform Silent Mode Operation where Client automatically connects with ZTNA gateway whenever user boots machine, before windows logon and user is not able to logout ZTNA client		
53.	The solution must provide following restriction during private/public web application access; A. Block copy/paste B. Block Content downloading C. Block pop-ups D. Block Screen Capture and Record Screen E. Record Application screen during access F. Watermark on screen during application access		
54.	The proposed solution should be supported on iOS, Android platforms and should provide granular policy and reporting of mobile devices. It should allow the administrator to enforce not to use of rooted or Jail broken devices.		
55.	The client agents must be lightweight and support silent deployment using popular software distribution systems		
G	**Agentless Zero Trust Access Feature**		
56.	The proposed solution must capable to establish a secure, remote-access VPN tunnel to security appliance using web browser		
57.	The proposed solution must capable to provide secure and easy access to a broad range of web resources, web enabled applications, RDP application, SSH application and file share application		
58.	The proposed solution should provide support for the most commonly used SSO methods, including: A. Basic authentication forwarding, B. Forms based and browser based authentication, C. SAML 2.0 IdP		
59.	The proposed solution must be able to allow or restrict user access to applications from users browser on all or set of combinations of following unique parameters; A. User identity, B. User's role (group/OU), C. User's WAN IP address, D. Device MAC address or Serial Number, E. Type of browser, F. Geo Network Financing (Based on specific City and Country), G. Time based access		
60.	The proposed solution must provide following restriction during web application access; A. Block copy/paste, B. Block Content downloading, C. Block pop-ups, D. Block Screen Capture, E. Record Application screen during access, F. Watermark on screen during application access		
61.	The solution must be capable of providing mTLS based communication encryption.		

Sr. No.	Technical Specification	Compliance (YES/NO)	Remarks (If Any)
Make Model			
62.	The proposed solution must have option to restrict application access from specific public IP		
63.	The proposed solution must be able to provide secure access to applications with layer 4 and layer 7 tunnelling from the browser		
64.	The proposed solution must support all standard protocols like SAML, Oauth/OpenID, Radius and TACACS+.		
H	**Reporting & Backup Specification**		
65.	The proposed solution must have reporting feature like; A. User session logs B. User live, last login and never login C. Primary and secondary authentication logs. D. Application access logs E. Administrator even logs F. Gateway event logs.		
66.	The proposed solution must have option to keep logs for 180 days and must be archive options after 180 days		
67.	The solution must support live monitoring of all user activities including failed logins, invalid access attempts etc.		
68.	The solution must provide detailed logs for all solution administrator activities including login details, configuration changes, etc.		
69.	The proposed solution must support the capability of forwarding both internet and private application access logs to the on-premises SIEM from day 1.		
I	**Support and Services**		
70.	The proposed Zero Trust Network Access Solution must have Next Business day Support. RMA/Hardware replacement shall be initiated within 24 hours of reporting of non-functioning of the device if the reported issue is not resolved.		
71.	The proposed Zero Trust Network Access Solution should continue to provide the following during the entire contract period : a) Upgrades b) Updates c) Patches and Fixes d) Technical Support		
72.	The solution (including all components under Zero trust Architecture) should have direct OEM 24x7x365 Support with 30 Minutes response time for P1 tickets and ticket types.		

11.21. Anti-Virus and End-Point Security and DLP

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
1.	Proposed solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, EDR and DLP in a single agent and should be completely On-premises and should not send any file/sample with cloud to inspect and analyze any threat			
2.	Proposed solution should defend endpoints against malware, ransomware, malicious scripts also support Pre-execution and runtime machine learning to detect and mitigate threats along with File reputation - Variant protection - Census check - Web reputation having True file type scan along with proactive outbreak prevention and Command & Control callback detection supporting IPv4 and IPv6 environments			
3.	Defends endpoints - on or off the corporate network - against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and fileless malware and support CPU usage performance control during scanning - Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.			
4.	Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback/restores any files by taking backup of ransom ware encrypted files and restoring the same before detection also detects script emulation, zero-day exploits, targeted and password-protected malware commonly associated with ransomware having a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.			
5.	Should detect from Targeted and known ransomware attacks, Zero-day malware and document exploits, Attacker behavior and network activity, Web threats, including exploits and drive-by downloads, Phishing, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, keyloggers and Disruptive application having capability to do retrospective scan on CnC, Script Analyzer, automatically send executable to virtual analyser and can crack password protected compressed files			
6.	The Proposed solution should monitor (East-West) traffic of attack for inspection to detect lateral movement (attack activities) inside the network (beyond C&C connections) also			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	solution should have threat emulation capability to cater zero day threat by simulating at least 20 virtual machines scalable up to 60 on same appliance running simultaneously having OS support i.e. Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016,2019 and Linux complete solution should have common threat sharing platform			
7.	Should have data loss prevention capability with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based having visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screen and capability with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based			
8.	Should empowers IT to restrict the use of USB drives, USB attached mobile devices, CD/DVD writers, cloud storage, and other removable media with granular device control and DLP policies and ability to Detects and reacts to improper data use based on keywords, regular expressions, and file attributes having granular device control with the following control actions: Read only, Read and write, Read, write and execute			
9.	Includes a granular list of truly international identifiers to identify specific data by patterns, formulas, positioning, and more. Identifiers can also be created from scratch and should offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP and continuously monitors data at rest, in use, and in motion to prevent data loss			
10.	Discover, monitor, block and provide view of endpoint status and broad coverage of communication systems: email, webmail, IM, P2P, FTP, Skype, Windows File Share, ActiveSync, and detect data-stealing malware: Identify botnets, hidden FTP processes, keyloggers, spyware, and Trojans that attempt to collect and send data and should offers visibility and control of data in motion of sensitive information—			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS and SMTP.			
11.	Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files) also Should have dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application			
12.	Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting containing broad coverage of pre-categorized applications that can be easily selected from application catalogue (with regular updates) having features roll-your-own application whitelisting and blacklisting for in-house and unlisted applications, ensures that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change.			
13.	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability and capable of recommending rules based on vulnerabilities on endpoint and create dynamic rules automatically based on System posture and endpoint posture also blends signature-less techniques, including high-fidelity machine learning, behavioural analysis, variant protection, census check, application control, exploit prevention, and good file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.			
14.	Should performs static and dynamic analysis to identify an object's notable characteristics: AutoStart or other system configuration, Anti-security and self-preservation, Deception and social engineering, File drop, download, sharing, or replication, Hijack, redirection, or data theft, Malformed, defective, or with known malware traits, Process, service, or memory object change and Rootkit, cloaking, Suspicious network or messaging activity			
15.	Solution must support CPU usage performance control during scanning -Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e.			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	High, Medium and low also should be APT ready capable of submitting SO (Suspicious Objects) to On-Premise Sandbox appliance for analysis without additional License on Endpoint.			
16.	Should have Investigation and IOC Sweeping (server-side metadata sweep), Patient Zero ID / Root Cause Analysis and IOA Behaviour Hunting/Detection, API's for query / automation and Unknown file guidance, Variant Protection to detects mutations of malicious samples by recognizing known fragments of malware code, Packer Detection to Identifies packed malware in memory as it unpacks, prior to execution, Runtime Machine Learning scores real-time behaviour against a cloud model to detect previously unknown threats, Root cause analysis for simple or full "kill chain and Search by multiple parameters by OpenIOC rule for disk scans and Yara rules for memory scans			
17.	Should have IOA Behavioural Analysis detects behaviour that matches known indicators of attack (IOA), including ransomware encryption behaviours, script launching, In-memory runtime analysis malicious script detection, malicious code injection, runtime un-pack detection, Isolation, Quarantine, Process kill, Execution block and Damage rollback, achieve context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls, Record detailed system-level activities and perform multi-level search across endpoints using rich-search criteria such as OpenIOC, Yara, and suspicious objects, Detect and analyze advanced threat indicators such as fileless attacks.			
18.	Should have seamless native integration with Anti – APT solution bi-directionally to detect and mitigate zero day threats having common threat sharing platform for holistic visibility and control also should have seamless integration with existing running endpoint security solution having common management platform also proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and data Exfiltration.			
19.	Proposed solution should be able to provide access information about Affected Hosts on the following views:			

S. No	Parameters	Specification	Compliance Yes/No	Remarks
Make Model				
	Displays a summary of affected hosts by attack phase, Provides access to Host Details views and Displays host event details in chronological order having provide Threat execution and evaluation summary and In-depth tracking of malware actions and system impact, including the following: Network connections initiated, System file/registry modification and System injection behaviour detection			
20.	Proposed OEM should have local TAC support centre in India with a coverage of 24x7 support period to address technical issues pertaining to proposed solution also OEM should conduct at least 5 day instructor led training in premise for nominated employees post implementation of proposed Endpoint Security solution and Payroll engineer should implement/configure management platform of proposed Endpoint Security solution following best practices considering current threat landscape also conduct half yearly health check for the deployed solution and health check should cover detailed configuration audit, findings and recommendations of the deployed solution			
21.	Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 5 consecutive years and OEM must have contributed at least 30 zero day/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publicly available.			

11.22. EMS/NMS/Helpdesk

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	General requirements		
1	All proposed EMS modules like Network Monitoring, Server Monitoring including Application and Database monitoring and Service Management tools must be from Single OEM and OEM must issue a single MAF for all the proposed EMS modules if any third party tools are part of the solution.		
2	The proposed Alarm Correlation and Root Cause Analysis system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	performance state of the entire network & system infrastructure shall be visible in an integrated console.		
3	The implementation of proposed EMS solutions needs to be done by the OEM/OEM authorised Partner.		
4	Any additional components (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.		
5	The proposed solution should have the capability to support the deployment on either on-premises data centre platform or the public/private cloud platform like AWS, Azure etc.		
6	The proposed NMS solution should be built on modern container technologies deployable on containerized (like Docker, Kubernetes) mode. The solution should either support built-in Kubernetes technology or Bring Your Own Kubernetes (BYOK) platform provided by the bidder.		
	Server Infrastructure Monitoring		
7	The solution should provide both Agent-based and Agent less Monitoring in a single solution architecture. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure – that will allow an organization to choose the level of management required and deploys the right-sized solution to meet those requirements.		
8	The proposed solution (hardware and software) provisioned from Day 1 should be able to handle 300 devices and shall be scalable to 1000 devices.		
9	The solution should be able to monitor the availability and performance of the servers, business applications, databases, applications using one single solution.		
10	The proposed Enterprise Management tools must be able to monitor end-to-end performance of Server Operating Systems & Databases and Should be able to manage distributed, heterogeneous systems – Windows, UNIX & LINUX from a single management station.		
11	Should be able to monitor bare metal, Hypervisor, KVM, Open stack, VMware, RedHat Virtualization environment.		
12	Solution should provide a web based Central Monitoring Administration console for management, deployment and configuration of monitoring Agents.		
13	Central Monitoring Administration web console should also provide downtime configuration feature to schedule planned outages. The solution should auto calculate the SLA without scheduled planned outages and approved downtime.		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
14	The solution should provide self-monitoring and notifications capability via sms, email etc. SMS and Email Gateway is not part of scope of this Technical Specification.		
15	The system should have context-based analysis and forecasting based on performance data with automated policy deployment with detailed, intelligent monitoring of performance and availability data collection.		
16	The solution should support Service Impact modelling with automated Event to Monitor association.		
17	The solution should have the ability to automate probable cause analysis by automatically grouping events together based on the time that they occur, the business service that they affect and then relating the two to the normal/abnormal behavior of each performance metrics to identify the likely cause of downtime.		
18	The proposed EMS solution must support deployment on latest version of Windows and Linux Operating System or combination of both with open-source database as backend and should be 64-bit application to fully utilize the server resources on which it is installed.		
19	It should have capability to perform cross-domain correlation with alarm correlation from Network Monitoring tool, Systems monitoring tool and other domain monitoring tools.		
20	Multiple dashboards can be created by each user – giving them a streamlined view of what matters most to them, without the noise.		
21	The solution should provide detailed Event and Performance Data reporting capabilities and the system must be FIPS 140-2 compliant, which ensures that cryptographic-based security system are to be used to provide protection for sensitive or valuable data.		
22	The solution should have OOTB remediation workflows for scenarios like Disk Full, Host Down, ESX not responding, and DB Tablespace Full etc. which can be triggered manually or automatically.		
23	The solution must be able to collect following Server Monitoring Parameters:		
a.	Disk failure/utilization		
b.	CPU Failure/utilization		
c.	RAM failure/utilization		
d.	Event logs		
e.	OS Monitoring		
f.	CPU Utilization		
g.	Disk Utilization		
h.	Cluster Monitoring		
i.	Process Monitoring		
j.	Hardware Monitoring		
(i)	Disks - RAID controllers, hard disks, RAIDs, Volume etc.		
(ii)	Environment - temperature, power supplies, fans etc.		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
(iii)	Critical components: processors, memory modules etc.		
k.	Customized reports on performance parameters as when required.		
24	The monitoring systems should have APIs that allow easy integration with third party tools, for Single consolidated dashboard. These should include: a. SNMP adapters, b. parsing log file, c. TCP/UDP Client Server, d. Windows Event logs, e. REST APIs.		
25	It should provide the ability to relate infrastructure topology to business services.		
26	The solution should be fully integrated with the proposed service desk to view the root cause of the issue, the business service affected and the CI that caused the downtime from with the Service desk. Post Integration with a service desk tool should be able to view the ticket number in the events data.		
27	The monitoring solution should be fully integrated with the proposed CMDB to relate event data to the service models in the CMDB to provide visibility into the business impact of downtime.		
	Database Monitoring and Storage Monitoring		
28	Monitoring of standard RDBMs (community and enterprise version) like Oracle, MS-SQL, DB2, MySQL, Sybase, Postgres, MariaDB etc. in standalone and cluster mode. Solution should be able to monitor storage infrastructure and performance.		
	Storage Monitoring -		
i)	Solution must provide failure and performance monitoring for multivendor (Hitachi, Netapp, HP, IBM, Dell EMC, Pure etc) storage devices directly or through integration with Storage Element management system.		
ii)	Solution must provide monitoring of all layers of a storage device (controllers, volumes, storage pools etc.) and provide GUI to easily detect issues.		
iii)	Solution must monitor following in Disk Arrays, Fiber Switches and Tape Libraries:-		
iv)	Monitors the environment (temperature, fans, power supplies).		
v)	Monitoring of fiber links.		
vi)	Customized reports on performance parameters as when required.		
29	The tool should provide ability to easily collect and analyse specific information, including information on:		
o	Buffer pools, Locks and other details about lock resources, Tablespaces / Data files / Log files, Database Usage, Database Errors, Database Status, Database File Group Space Usage Level, Database Mirroring Status, Database Transaction Log Usage Level, Database Transaction State, Server SQL Query Performance, Server Query Tuning, Active Connections.		
o	Microsoft SQL Server Connection Check, Microsoft SQL Server Documents, Mirroring Status, Network Statistics, Processes		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	Blocked, Replication Agent Status, Replication Latency, Transactions Active.		
o	Database Server Status, Server key events, Server CPU Usage by SQL, Server Replication Status, Server Transaction Rate, File group Space Usage.		
o	Workload metrics such as CPU utilization, transaction throughput.		
o	SQL related performance indicators such as percent sorts in memory, disk-sort rate.		
30	The solution should be able to monitor the performance of all the above database and their instances against the defined performance counters and usage of different system resources.		
31	The solution should be able to monitor locks and deadlocks for the instances.		
32	Should proactively identify database problems before they affect end-users and ensure high availability of mission critical databases.		
33	Should monitors SQL statements to identify resource-intensive, inefficient and problematic SQL statements to facilitate SQL query optimization and tuning.		
	Network Fault Management		
34	NMS should provide integrated fault, performance Monitoring, Configuration & compliance Management together in one tool. Compliance Management refers to Audit and compliance reporting against standard policies for network devices and other devices to be monitored.		
35	NMS should support Industry-leading support for physical, virtual, and SDN-enabled devices like Cisco ACI, VMWare NSX, etc.		
36	NMS should support out of the box monitoring of at least 3000+ devices from at least 150+ vendors.		
37	NMS should provide network Trap Analytics out of the box and should provide diagnostic Analytics providing change-Correlated Performance Views and should show the difference either in either a side-by-side, or line-by-line presentation.		
38	NMS should have built-in audit and compliance policies for industry best practices/ Gov. regulations like PCI, NIST, NVD and other vendor specific standards.		
39	NMS should provide Automate Network Operations and Orchestration.		
40	The solution shall provide information regarding capacity utilization and error statistics for WAN links.		
41	The solution should support IPv4, IPV6 and SNMP v1, v2c and SNMP v3 and/ or latest version to provide added security.		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
42	The solution should process events using consolidation, filtering, normalization, enrichment, correlation, and analysis techniques. Then it should notify the appropriate IT operations personnel of critical events. Solution should also automate corrective action wherever possible.		
43	It shall be able to capture, track & analyse traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.		
44	It shall collect the real-time network flow data from devices across the network and provide reports on traffic based on standard TCP/IP packet metrics such as Flow Rate, Utilization, Byte Count, Flow Count, TOS fields etc.		
45	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements: a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware.		
46	The proposed fault management solution must able to perform real-time or scheduled capture of device configurations.		
47	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.		
48	The solution must allow topology maps to be created for network areas; it should automatically detect and displays links between devices and any change in particular network elements or links status.		
49	The solution must generate accurate ("as-built") physical Layer 2 and Layer 3 diagrams with the push of a button.		
50	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, LAN Extender, Servers, Terminal Servers, Thin-Customer and UPS 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. Discovery of devices is a general capability asked for the proposed EMS tool.		
	Network Performance Management		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
51	The solution should Collect, analyse and summarize management data from LAN/WAN, MIBII interfaces, various systems and services for performance management. It should allow identifying trends in performance in order to avert possible service problems.		
52	The solution should provide Performance of Network devices like CPU, memory & buffers etc., LAN and WAN interfaces, Network segments and VLANs.		
53	The solution should give user flexibility to create custom reports, on the basis of time duration, group of elements, custom elements etc.		
54	The solution should provide web-based reports both near real time and historical data for the systems and network devices and should provide reports through e-mail to pre-defined user with pre-defined interval.		
55	The solution should provide Real time network monitoring and Measurement of end-to-end Network/ system performance & availability to define service levels and further improve upon them.		
56	The solution should identify how device resources are affecting network performance, document current network performance for internal use and service level agreements (SLA).		
57	Executive Summary report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.		
58	The tool should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports Reporting and Dashboards.		
59	System must support a large number of out-of-the-box reports in a wide range of categories - Activity, availability, inventory, etc.		
60	System must provide a custom-report generation tool that allows the creation of custom reports via a "drag and drop" web interface.		
61	It shall be able to monitor and report on availability, delay of target IP nodes – i.e. router interfaces - and also monitor and provide reports on historical utilization of CPU, memory, bandwidth for Network devices.		
62	Top N Utilization, Capacity prediction, Availability, Performance, CPU and Memory utilized, Interface errors, Trend report based on Historical Information, Custom report, SLA Reporting, Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports, Availability and Uptime - Daily, Weekly, Monthly, Yearly Basis.		
63	Business owners should have a clear view of the extent of impact to their business services and if need be the reason behind the impact.		
64	The IT organization and business stakeholders should be able to view their tickets by business service and impact from the same		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	solution.		
65	For each section, user should be able to select the time frame to report on data. This could be monthly, quarterly, half yearly, yearly or custom dates.		
	Service Management Framework		
66	The proposed IT Service Management solution should be built on ITIL framework and must comply with at least 9 processes. The ITILv4 processes PeopleCert Gold certified that are relevant and need to be assessed to meet the minimum functional criteria are Incident Management, Problem Management, Change Enablement, Service Configuration Management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management, and Service Request Management. The certification copy to be submitted.		
67	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.		
68	The solution should have a single CMDB across ITSM and Asset Management system.		
69	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.		
70	Provide option for approval engine so that any customized applications developed could incorporate the hierarchy, role based, level based ad-hoc approval structure. Include notification and escalation capability if approval is not performed.		
71	The solution should have the ability to operate all functionality available in the incident, problem, change, assets etc. via a mobile app on iPhone or Android phone.		
72	The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.		
73	A virtual bot should be available, which can respond to user requests, immediate via portal, email or mobile interfaces.		
74	Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT/Non-IT services.		
75	The solutions should allow effectively creating and managing a shared services catalogue for all service request with flexible entitlement controls. The solution should have wizard/ graphical workflow editors allowing definition of new request in minutes – without any programming.		
76	Integrates with any underlying service management including		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	Service Desk, Change Management, Service Level Management and CMDB for request fulfilment.		
77	Beyond mobile iOS and Android apps, Self Service App should be available on any device with an HTML5 browser.		
78	Self Service App should provide a snapshot of your day, displaying your activities feed with upcoming appointments, pending requests, unresolved issues, and alerts from systems you use in your daily work.		
	Service / Help Desk (Incident and Problem Management)		
79	Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.		
80	The solution should provide embedded and actionable best practices workflows i.e., bestpractices process & views based upon implementations.		
81	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively. The tool itself can be able to calculate SLA based on configured parameters automatically (deducting the total downtime and maintenance time under different category) with detailed summary and consolidated reports as per requirement.		
82	The Helpdesk solution should provide analytics feature which intelligently displays an interactive diagram indicating the hot topics among recent incidents so that users can easily discover incident trends and their relative impacts and identify problem candidates. This enables Process Managers and other IT Users to proactively identify trends that can be used to drive action.		
83	Auto assignment must be based on logic for ticket allocation, Engineers geo-location, availability of engineer; as per shift & as per ongoing repairs for resolution, skillset required for the trouble ticket.		
84	The tool should integrate with a directory system to enable recording and accessing user records of information with capability to integrate with multiple LDAP.		
	Change & Release Management		
85	The tool should facilitate the identification of the change type and associated workflow For example: standard, normal, and emergency.		
86	Change management should have fields to record impact analysis and simulate impact, backout plans, within the change record.		
87	The tool should facilitate ability of authorized roles to reject changes For example, status of reject, ability to record reason for rejects notification.		
88	Change management should be capable of integrating with CMDB to facilitate access to CI attributes and relationships to enable change		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	assessment and authorization.		
	Knowledge Management		
89	The tool should integrate with knowledge management OOB - knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions.		
90	The tool should allow the creation of different access levels (i.e. Read only, write, create, delete) to knowledge management system.		
91	The tool should have a powerful search engine to sort, retrieve and search using advanced search options, search content in multiple format, and also search within knowledge records.		
	Configuration Management Database (CMDB)		
92	Should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle.		
93	Should automatically create Service models to describe how IT infrastructure supports business services. Shall support automated relationships between discovered IT assets.		
94	The CMDB should have built-in drift management capabilities to capture and report on infrastructure drift based on infrastructure attributes like RAM, memory, etc.		
	Service level Management		
95	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different KPIs like infrastructure (CPU utilization, disk space), response times , resolution times (eg. incident closed on 2 hours) performance and custom parameters of an enterprise.		
96	Real-time visualization of service level targets, agreement compliance data, penalties and rewards.		
97	The service level management (SLM) tool should facilitate creation and maintenance of SLAs, OLAs and Supplier / Underpinning Contracts For example: scope, supplier, contact names, contact method, support hours, service level targets.		
98	The module should link available support hours to service levels when calculating deadlines as well as suspend SLA calculation for certain criteria – e.g. ‘pending information from customer’.		
99	The service management software should have the ability to tightly integrate (bidirectionally) with enterprise management systems for auto-creation/closing / reporting of events/incidents/trouble tickets Data Centre Discovery.		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
100	The solution should be able to do a complete discovery of IT environment across distributed (i.e., physical, virtual, network, application, middleware, storage, databases) and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services and should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model.		
101	The solution should automatically build visualizations that shows dependency between switches, routers, physical/virtual host, storages, cluster software, business applications and other entities and should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent.		
102	The Discovery solution should come with real-time dashboards that collate and present data that allows organizations to make decision on consolidation, re-use of infrastructure, detecting infrastructure that has never been used etc.		
103	The solution should be able to automatically detect software's that are end of support, end of extended support and end of life.		
	Network & Server Patch Management, Configuration and Compliance Management		
104	The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-vendor network tool.		
105	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements: a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware.		
106	The proposed fault management solution must able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user- defined standard baseline configuration policy.		
107	The proposed system should be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.		
108	The proposed system should also provide end to end change management and approval process automation for any patch or update activity.		
109	Using the automatic remediation of common IT tasks, the fix should be handled automatically after the problem is detected and a service		

S.No.	Minimum Specification	Compliance (Y/N)	Remark (If any)
Make Model			
	desk ticket has been created and recorded.		
110	NMS should support 3-Dimensional Compliance Model - Configuration, Software, Running State and provides out of the box Risk Visibility Dashboards of network infrastructure.		
111	Should Detect, collect and maintain information about Managed Servers, including packaged, unpackaged software, runtime state, host/guest relationships and more.		
112	Enables patch policy creation and flexible patch deployments. Supports native patch formats for all major operating systems. Provides out-of-the-box integration with Microsoft® Patch Network and Red Hat Enterprise Linux.		
113	Provides dynamic, real-time, and historical reports into hardware, software, patches, and operations activities in complex, heterogeneous data Centres. Includes out-of-the-box compliance reports and at-a-glance compliance status with actionable links to servers, policies, and other objects. Exports reports to HTML and comma-separated values (CSV) formats.		
114	The audit trails should be stored centrally and should be digitally signed to prevent tampering.		
	OEM Criteria		
115	The proposed EMS OEM must be an industry standard, enterprise grade solution and shall be present in either Leaders or Challengers (Strong Performers / Major Players) Quadrant of Forrester / Gartner / IDC report for ITSM in the last 3 published reports.		
116	Proposed NMS solution MUST have at least 1 deployments in Indian Government/ Public Sector, monitoring & managing 10000+ nodes in each of such deployments OR 3 deployments in Indian Government/ Public Sector, monitoring & managing 5000+ nodes in each of such deployments. Customer names, solution details and OEM undertaking needs to be provided at the time of bidding.		
117	Similar OEM solution should be deployed in min. 3 project of Data Centre in India. The documentary proof should be submitted at time of the bid submission.		
118	The offered EMS solution shall be covered under 24X7X365 direct OEM remote support for the entire contract duration 5 Years .		

11.23. Cloud Management & Orchestration

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	General Specifications		
1	The bidder shall propose direct back to back highest-level of OEM support 24x7x365 days for proposed products with unlimited number of incidents and Designated support manager should be aligned giving highest level of support		
2	The bidder shall propose - Plan, Design and Implementation Services (Professional Services) from the software provider OEM. The OEM shall not subcontract the design and implementation services to any third party. The OEM engineers designing, deploying and implementing shall have to be on the payroll of the software OEM		
3	The bidder shall ensure that the resources required for management components are called out and are deployed on a separate infrastructure (management cluster) as per best practice. Additional resources for overhead should be called out explicitly in solution document.		
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, HCI and external FC storage without having any dependence on specific make/model of infrastructure components		
5	Bidder should propose Hypervisor, Monitoring, Automation, Cloud Security and Enterprise grade Container solution from single OEM.OEM of the proposed solution should be in the top three vendors of each category Virtualization software, Cloud management Automation and Operation, HCI, SDN as per latest IDC, Gartner reports available.		
6	The Bidder should submit 10 successful private cloud references from India.. The private cloud should comprise of Hypervisor, HCI,Cloud Security, Automation, Orchestration and Management and should be running atleast 500VM+ setup in production environment.		
	Virtualization		
7	The solution shall provide a purpose-built hypervisor to virtualize Compute/Storage/Network with minimal footprint that installs directly on the bare metal x86 server hardware with no dependence on a general-purpose OS for greater reliability and security. This hypervisor should have inbuilt support for software defined storage and software defined network capabilities.		
8	Support for heterogeneous guest OS - Window and Linux (Redhat, Centos, SuSE , Ubuntu, Oracle Linux).Respective windows and Linux guest OS must certify the underlying hypervisor and should be available publicly.		
9	Proposed hypervisor should support standard features that can be		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	useful during planned and unplanned downtime to provide high availability and planned migration of workloads between set of x86 hardware non disruptively		
10	Hypervisor shall provide the ability to hot add CPU and memory , hot-plug disks and NICs (provided the same is supported by guest OS)		
11	The Virtualization layer shoud be capable of prioritizing resoruces across Data center resources like compute, Network and Storage based on business and reosurce contention scenarios.		
12	Hypevisor should support container and openstack integration for cloud native application from day-1. must be a cloud native platform ready from day one		
13	Virtualization Management software should be deployed in clustered mode across nodes & racks and different data stores so that failure of host, OS, virtualization management software component should have zero downtime impact on the availability of Virtualization management.		
14	Hypervisor / Proposed HCI should support Import of Other Disk Styles VMDK,VHD/QCOW2 natively without any external 3rd party tool.		
15	Hypervisor must have capability for OS Catalogue/template and OS provisioning with role based access to virtual machine.		
16	Virtualization software should have capability to distribute compute resources evenly across hosts, this to ensure that the workloads are evenly distributed to avoid imbalnce of host utilization and avoid stress on few hardware resources.		
17	Hypervisor shall provide automated live migration for initial placement and balancing of available resources with the rules to define affinity and / or anti-affnity of workloads for software license requirementsas requried		
18	Hypervisor solution must allow seamless migration across different CPUs with Compatibility mode per-VM during migrations across hosts in a clusters and during power cycles		
19	Hypervisor should support UEFI bios along with legacy BIOS for supported virtual guests OS, when available in hardware to ensure that only signed drivers & OS loaders are loaded while booting		
20	Virtualization Manager must support Directory based/OpenLDAP and SAML based authorization for mangement.		
21	Virtualization software should provide network traffic-management controls to allow flexible allocation of physical NIC between different network- traffic types and allow user-defined network/bandwidth, Enabling multi- tenancy deployment and should support 802.1Q for multi vlan traffic.		
22	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	and update without impacting production.		
23	3rd party support for endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions without the need for agents inside the virtual machine		
24	Hypevisor should support Rest API and Command line management along with GUI interface.		
25	Virtual Machine perfomrance reports for performance and utilization of virutal machines. It shall co-exist and integrate with leading system management vendors.		
26	Proposed Solution should have Memory overprovisioning without impacting VM performance using advanced memory management techniques such as “Memory Balloning” and “Memory Swapping” and “Transparent page sharing” and “Memory Compression”		
27	Should support TPM 2.0 and secure boot which provides protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.		
28	Virtualization software should provide VM-level encryption protects unauthorized data access both at-rest and in-motion without any performance overhead		
	Hyper Converged		
29	The Solution should support checksum of data to ensure data integrity & to enable automatic detection and resolution of inconsistency		
30	The proposed HCI nodes should compulsorily manage from a single control plane and movement of VMs's should be seamless, non-disruptive, without any downtime & VM shutdown/reboot once the private cloud is extended.		
31	The proposed solution must be capable of moving the VM's across the new nodes at the software defined storage level without any downtime		
32	The proposed solution will run critical databases like Oracle, MS SQL, My SQL & MongoDB, Postgress. The HCI Cluster should have the capability to run said Databases		
33	The proposed SDS should be embedded within the hypervisor kernel itself or with an external control VM. Bidder and OEM need to provide the OEM Sizing and overhead requirement over and above the usable resources for HCI, Container, Automation, Orchestration, Replication need to be given in details in excel sheet with public domain reference considering all the services are enabled in HCI file system providing (Physical CPU, vCPU, RAM and Storage for the entire proposed solution).		
34	The proposed HCI must support connectivity (HCI Storage extension) to 3rd party bare metal servers along with load balanced and distributed architecture across all available nodes in cluster (for optimized DB licensing on physical servers) to HCI storage cluster &		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	use the cluster capacity like a iSCSI,NFS target.		
35	HCI solution should support VM's snapshot at storage level, it should not impact guest OS performance during snapshot. It Should also allow Virtual Machines to be able to revert back to an older state, if required		
36	HCI solution should support 3rd party Backup Software integration for tape out or disk based Archival.		
37	HCI solution should support natively Microsoft and Linux based Guest VM's Clustering using block storage and reference architecture should be available		
38	HCI solution should support sync replication for zero RPO & RTO for critical workload. Bank is Looking forward to setup a NDR Site which required 0 Min RPO and RTO (Sync replication).		
39	Proposed solution should avoid performance degradation due to noisy neighbour problem. Solution must have Native QOS at the IOPS level as well as Network BW level for specific VMs. Solution should be policy driven for storage services like performance, availability and capacity.		
40	The solution should have call home capability for remote log collection and proactive support for predictive failure hardware component		
41	HCI solution should have codeless automation native engine to create troubleshooting for alert and remediation as per policy for VMs.		
42	HCI solution should support rest API for third party integration and customized workflow for automation using rest API		
43	SDS licenses should be transferrable to hardware in case of hardware EOL & EOS or nonavailability. Adding of Memory or Disks should not incur any additional software licenses, cache drives		
44	Proposed software storage solution should integrate with hypervisor for planned and unplanned activities like maintenance mode activities or during unexpected failure of hosts and during compute resource crunch due to workload utilization of resources.		
45	The solution should provide enterprise data services such as compression completely in software. Hypercoverged solution must have de-deuplication and compression features licenses and implemented from day one . These functionalities should be part of the proposed solution. The HCI solution must have functionality to to support compression and or Deduplication online on data container without any downtime and data loss as per business requirement without any performance impact on User VM.		
46	The proposed HCI should support native (without any third party software) distributed File Services over NFS, CIFS, SMB across clusters and data centers. It must support Linux and Windows Guest VM with unlimited shares integrated with Active directory/LDAP.		
47	HCI solution should be able to take VM's snapshot/Storage snapshot		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	at any time irrespective of VM's state (Power ON/Power OFF/Suspended) with retention policy		
48	SDS licenses should be transferrable to hardware from any vendor in case of hardware EOL & EOS or nonavailability. Adding of Memory or Disks should not incur any additional software licenses.		
	SDN		
49	The solution shall provide visibility of network traffic between the Apps/VMs.		
50	The solution shall provide a software defined networking & security virtualization layer that allows faithful delivery of network services in software without dependence on specific make/model of networking devices/appliances		
51	The private cloud security solution must enable Layer 2 overlay network across a routed fabric within and across data center boundaries and support overlay protocols like VXLAN or GENEVE.		
52	The solution should provide a stateful distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		
53	The firewall-rule table of the solution should be designed for ease of use and automation with virtualized objects for simple and reliable policy creation		
54	The solution should provide embedded/virtual machine distributed firewall and should provide near line rate performance.		
55	The solution should enable integration of third-party network and security solutions through open architecture and standard APIs. The bidder shall provide a list of ecosystem vendors that integrate with the framework		
56	The solution should provide distributed routing so that routing between Virtual Machines with different IP subnets can be done in the logical space without traffic going out to the physical router thus reducing number of hops		
57	The solution should provide distributed and dynamic routing capabilities like OSPF and BGP		
58	The solution shall lend itself to network monitoring by supporting standards protocols (for remote network analysis)		
59	The solution shall provide ready integration with the proposed platform to automate delivery of networking & security services such as switching, routing and firewalling		
60	The solution should have the ability for On-demand network creation and can define routed, NAT or Private network profiles based on application topology		
61	The solution should be capable to provide agentless guest and network introspection services.		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
62	The solution should have capability to provide stateful micro-segmentation for virtual machines from a single console.		
63	The solution should integrate with Kubernetes to provide app-deployment automation L4 Objects (Kubernetes Services)		
64	The solution should provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services at Layer 2.Solution should support for container networking plug-ins, native support for pod to pod communication, support for ingress controllers		
65	The solution should integrate with industry-leading Solutions for antivirus, malware, intrusion prevention, and next-gen security services.		
66	The solution should provide a stateful firewall with capability of defining security policies on constructs such as IP address, VM names, objects and tags, active directory groups, Security tags etc.		
67	The Security policies must follow the VM in the event of migration (i.e. vMotion) within the datacenter		
68	The SDN solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE, Dell.		
69	Provisioning of virtual/software defined network services should be possible irrespective of make and topology underlying physical network switches and routers.		
70	The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero trust security within the data- center		
71	The proposed SDN solution should be a purely software based solution and should not be dependent on any hardware make and model.		
72	The solution should provide a single unified management console for end to end management of the entire environment.		
73	The bidder shall ensure that all proposed components shall have the ability to run on standard server infrastructure based on the x86 architecture without having any dependence on specific make/model of infrastructure components.		
74	The SDN solution should be highly programmable through APIs integration from a central management point and can be integrated with major industry software automation management / cloud tools to automate end users’ service requests.		
75	The SDN solution should provide overlay network & security virtualization and should work on any underlay physical network devices make and topology.		
76	The SDN solution should support virtual Distributed Switch which is a generic software defined switch platform that is hypervisor independent.		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
77	The SDN solution should provide logical Layer 2 overlay extensions across a routed (Layer 3) fabric within and across data center boundaries and supports network overlays.		
78	The SDN solution should support Management Cluster including control-plane capabilities.		
79	The SDN solution should support the ability to create a cluster of managers of Network & Security virtualization for high availability of the user interface and API.		
80	The SDN solution should support creating VPN services, NAT services & Routing.		
81	The SDN solution should offer to deploy virtualized network functions (like switching, routing & firewalling), administrators can build virtual networks for Virtual Machines or Virtual Desktop Infrastructure without the need for complex VLANs, ACLs or hardware configuration syntax on underlay physical network.		
82	The SDN solution should enable consistent networking and security across data center sites and across private and public cloud boundaries, irrespective of underlying physical topology.		
83	The SDN solution should support multi-site network and security for virtual workloads.		
84	The SDN solution should support VLAN backed as well as distributed overlay switching encapsulated services.		
85	The SDN solution should provide distributed routing, so the Routing between Virtual Machines with different IP subnets can be done in the logical space of hypervisor without traffic going out to the physical router.		
86	The SDN solution should support multi-tenant / Multi-tier network routing for the virtual workload.		
87	The SDN solution should support Virtual edge device as virtual appliance – - Routing Connectivity to physical network - NAT - DHCP server - Firewalling		
88	The SDN solution should support micro-segmentation for east- west traffic of virtual machines, offering security policy on VNIC of the virtual machines.		
89	The security policies in the virtualization layer must be tied to the application VM, which means whenever any application is moved from one virtualized server to another, even between different VLANs, the security policies should follow the application and there should be no need to redefine the security policies for the application at the new location.		
90	The SDN solution should support NAT.		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
91	The SDN solution should support source NAT / Destination NAT.		
92	The SDN solution should support service insertion for all/specific traffic between VMs (north-south and east-west traffic) in the Data Center can be redirected to a dynamic chain of security partner services.		
93	The SDN solution should support Layer-2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.		
94	The SDN solution should support Secure VPN between two datacenters or between on-premise to public cloud.		
95	The SDN solution should support traceflow from source workload to destination workload and provide details of every hop in the path.		
96	The SDN solution should support of backup/restore of the centralized Management appliance configuration.		
97	The SDN solution should provide the ability to provide native application isolation for providing zero trust security for the application and should allow for on-demand creation of security groups and policies.		
98	The SDN solution should support network & security virtualization operations and troubleshooting.		
99	The private cloud security solution should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting. This visbility must also report the amount of East-West, North-South, Internet, virtual machine to virtual machine, virtual machine to physical traffic within the datacenter.		
100	Proposed solution should support IPV4 & IPV6		
101	Bidder should have supplied, installed and maintained the proposed SDN solution with minimum 500 VMs in at least 2 Commercial Banks/ Financial Institutions in India in past 3 Years as on RFP issue date		
102	The proposed solution should also have advanced capabilities like IDPS/NTA/NDR without any dependency on any additional 3rd party hardware/software solution, in case the bank wants to enable these capabilities in the future		
103	The SDN solution should have the capability to extend the same subnet between overlay segments and physical VLAN segments		
104	The proposed solution should natively identify which application a particular packet or flow is generated by, independent of the port that is being used		
105	The proposed solution should provide uniform SDN capabilities across ESXi hypervisors, Bare Metals and micro-services/container based environments		
	Cloud Security		
106	The solution should provide a stateful/Stateless distributed firewall such that the firewalling for Virtual Machines can be provided closest		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	to the application within the server itself without traffic going to a Physical Firewall.		
107	The firewall-rule table of the solution should be designed for ease of use and automation with virtualized objects for simple and reliable policy creation.		
108	The solution should provide embedded/virtual machine distributed firewall and should provide near line rate performance.		
109	The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management.		
110	The solution should enable integration of third-party network and security solutions through open architecture and standard APIs. The bidder shall provide a list of ecosystem vendors that integrate with the framework.		
111	The solution should automatically generate policy recommendations based on intrinsic understanding of application topology. This allows will easily create, enforce, and manage granular microsegmentation policies and leverage object-based policy model for automation.		
112	The solution should have capability to protect applications on the internal network against known malicious IP addresses on the internet such as botnet masters.		
113	The solution should have capability to provide statefull micro-segmentation for diverse workloads covering virtual machines, containers and bare metal servers for supported OS(Linux based and windows) from a single console.		
114	The solution should provide a stateful/stateless firewall with capability of defining security policies on constructs such as IP address, VM names, objects and tags, active directory groups, Security tags etc.		
115	The Security policies must follow the VM in the event of migration (i.e. vMotion) within the datacenter.		
116	The Solution should be capable of supporting major hardware data-centre networking OEMs like Juniper, Arista, Cisco, HPE and Dell.		
117	The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero trust security within the data- center.		
118	The solution should support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses.		
119	The solution should have capability to protect applications on the		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	internal network against known malicious IP addresses on the internet such as botnet masters.		
120	The solution should have capability to provide statefull micro-segmentation for diverse workloads covering virtual machines, containers and bare metal servers for supported OS(Linux based and windows) from a single console.		
121	The solution should provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers.		
122	The solution should have capability to create firewall rules with both kubernetes (K8s) and NSX objects and should support dynamic security groups creation based on NSX tags and K8s labels.		
123	The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console.		
124	The solution should support traffic visibility,network monitoring,distributed firewall planning and management.		
125	The solution shall provide visibility of network traffic between the Apps/VMs and at the process level.		
126	The solution should automatically generate policy recommendations based on intrinsic understanding of application topology. This allows will easily create, enforce, and manage granular microsegmentation policies and leverage object-based policy model for automation.		
127	The solution should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting.		
128	The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero trust security within the data-center		
129	The solution should be able to report the amount of East-West, North-South, Internet, virtual machine to virtual machine, virtual machine to physical traffic within the datacenter		
130	The solution should provide a converged view of virtual and physical network, provide end to end topological view of path between two virtual machines. It should be capable of integrating with leading hardware OEMs like Juniper, Cisco, Arista, HPE, Palo alto networks, Checkpoint, Fortinet to provide this visibility		
	Cloud Automation & Management		
131	The Software should support AD authentication, and synchronization of user list and profiles between Software and Active Directory setup.		
132	The solution should be able to give a complete cost governace across the private, public cloud.		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
133	The solution should provide resource reclamation functionality which identifies and reclaims inactive and abandoned resources by automating the decommissioning and reuse of retired resources. It should also provide reclamation savings reports which would enable organizations to quantify its cost savings		
134	The solution shall support creation of services such as 'Single VM' and a 'Multi-tier application infrastructure (including softwarebased constructs such as load balancers)' as part of a standard template		
135	The solution shall support native (without using any 3rd party component) approval policies integrated with email/SMS notifications such that approvals/rejections can be done		
136	The solution shall support extensibility capabilities to customize machine configurations and integrating machine provisioning /management with other enterprise-critical systems such as load balancers, configuration management databases (CMDBs), ticketing systems, IP address management systems, or Domain Name System (DNS) servers.		
137	The solution shall extend Day 2 operations capabilities to the requestor of the service (e.g. ability to start/stop/suspend virtual machines, request additional resources and access the VM using RDP/SSH protocols) through the self-service portal based on entitlement. Basic day-2 operations should be natively deployed in entire solution from day-1		
138	The solution shall allow administrators to manage and reserve (allocate a share of the memory, CPU and storage) resources for a business group to use.		
139	The solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.		
140	The solution shall provide an orchestration engine with ready workflows and ability to create custom workflows based on SOAP/ REST operations and PowerShell scripts		
141	The solution should be able to define multiple tenants which would enable the administrators to create a secure multitenant infrastructure wherein within a Tenant different business groups can have resources, service levels and automation processes that uniquely meet that group's needs.		
142	The solution should have the ability to create custom workflows to automate the delivery of anything as a service - XaaS (for example Email, Storage as a Service, Network as a Service, Backup as a Service etc.)		
143	The solution should have a Unified graphical canvas for designing machines, software components and application stacks with the ability to extend or define external integrations in the canvas through XaaS		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
144	The solution should have the capability to publish and share software components across Projects		
145	The solution should 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.		
146	The proposed Private Cloud solution must be ready for containers, kubernetes and dockers deployment.		
147	The solution should provide capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.		
148	The solution should provide out of the box capacity analytics and modelling, with granularity ranging from entire datacenter to cluster to individual host and virtual machine level. Single view of all virtual machines, allow Monitoring of system availability and performance and automated notifications with alerts. Monitor, analyze virtual machines, server utilization availability with detailed predict analysis of whats-if Scenario hardware procurement, capacity planning, Capacity forcasting, performance graphs and greater visibility into object relationships. Metric collection intervals should be granular and the platform should have capability to analyse metrics data captured at 10 min intervals or lesser over extended period of time, so that capacity planning and troubleshooting is effective		
149	The solution shall provide ready to use templates to validate configuration standards on the Virtual Machines covering security best practices, vendor hardening guidelines and regulatory mandates such as PCI-DSS, FISMA, CIS, DISA, SOX and custom compliance policies to track & enforce compliance.		
150	The solution should provide advanced trouble shooting capabilties leveraging AI/ML technologies which would provide troubleshooting evidence consisting of events, property changes and metric abnormalities. Should be able to trigger automated actions on event generation		
151	Should have capability to enforce policies/guardrails for provisioned and discovered resources across organisations and projects. Apply consistent policies (tags, names, lease, power schedule, entitlements, approvals, resource limits) across private cloud set-up).		
152	The solution should have log analytics available in one single management window to make troubleshooting easier. Should provide a single location to collect, store, and analyse unstructured data from		

Sr No	Description	Compliance YES/NO	Remarks (If Any)
Make Model			
	OS, VMs, apps, storage, network devices, containers, Kubernetes etc. at scale. Should provide intuitive dashboard and should allow IT teams to search for certain event patterns & types for troubleshooting.		
153	Platform should have support to automate infra, app & service deployments with a release pipeline as a capability within the platform i.e. CI/CD pipelines		
154	The solution shall provide support to export/import the architecture blueprints into standard formats such as YAML for programmatic manipulation through Infrastructure-as-code. Should support bulk Import of underlying hypervisor virtual machines and multi-cloud VMs. Should have repository and versioning for Blueprints		
155	The solution should offer cost control measures such as quotas (limits on what a user can provision) and leases (time-limited provisioning of resources)		
156	The solution must include unique lifecycle management services that automate day 0 to day 2 operations, from bring up to configuration, resources provisioning and patching/upgrades of all the software defined infrastructure layers like Compute, Storage, Network, Operations and Automation components.		
157	the Proposed Solution should be able to identified out of the box top 10 VM's basis on their high resource utilization(CPU/Mem/Storage/Network/IOPS) in a single dashboard		
158	Should support in built CI/CD tool for devsecops to atomate build, release and deploy from from continuous and repeatable basis by integrating on prem cloud and public clouds across VMs and containers. Should be able to track artifacts and automate deployment configurations to ensure correct versions are used across all stages of the development lifecycle.		
159	The Solution should to analytics on capacity behavior and should have capability of showing all under and over utilized VM's with their right sizing information on periodic basis.		
160	The Solution should be capable of creating custom dashboard with reporting as per customer ease and requirements, Solution should be able to scan/search objects with advanced search option for faster access to require information for trouble shooting		
161	HCI solution should support rest API for third party integration and customized workflow for automation using rest API		

11.24. MS Windows Server Standard Edition 2 Core

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make **Model**				
A	**Key Features:**			
1	MS Windows Server Standard Latest Edition 2 Core License with required CAL Licenses			

11.25. Red Hat Enterprise Linux 2 Core with Life Cycle Management

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
Make **Model**				
A	**Key Features:**			
1	Red Hat Linux Standard Latest Edition			

11.26. Multifunction Laser Printer

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
1.	Make			
2.	Model			
3	Key Features			
4	Multifunction Laser Printer			
5	Wi-Fi Printer			
6	A4 Black and White Laser Multifunction Printer, Print only, ADF			
7	Print speed up to 21 or higher ppm (black) USB, Ethernet, Wi Fi			
8	Technology Laser			

#	Parameters	Minimum Specifications	Compliance (Yes/No)	Remarks
9	Number of print cartridges 2 (black) Connectivity, standard Hi-Speed USB 2.0; Fast Ethernet 10/100Base-Tx network port; Wireless 802.11 b/g/n			
10	Network capabilities Via built-in 10/100 Base-TX networking			
11	Wireless capability Yes, built-in Wi-Fi 802.11b/g/n Mobile printing capability Apple Air Print™; Google			
12	Network protocols, supported Via built-in networking solution: TCP/IP, IPv4, IPv6; print: TCP-IP port 9100			
13	Direct Mode, LPD (raw queue support only), Web Services Printing; discovery: SLP, Bonjour, Web Services Discovery; IP Config: IPv4 (BootP, DHCP, AutoIP, Manual), IPv6 (Stateless Link-Local and via Router, Stateful via DHCPv6); management: SNMPv1/v2/v3, HTTP			

11.27. DESKTOP

SL	Parameter	Functionality	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
1	Processor	Intel 12th Generation Core i7- 12700 CPU or Latest		
2	Chipset	Suitable OEM chipset		
3	Motherboard	OEM Motherboard		
4	Memory	32GB DDR4 expandable to 64GB DDR4, Total four DIMM slots		
5	Hard Disk Drive	1 TiB NVME M2 SSD PCIE 3.0 x4		
6	Graphics	Intel HD Graphics (integrated)		
7	Audio	High Definition Audio (all ports are stereo), with Internal Speaker		

SL	Parameter	Functionality	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
8	Ethernet	Integrated Gigabit (10/100/1000 NIC) LAN		
9	Slots	All FULL height Slots		
		(1) PCI Express x16		
		(1) PCI Express x1		
		(1) PCI x1		
10	Bays	(1) 3.5” Internal drive bays		
		(1) 5.25" ODD		
11	Ports	At least 8 USB ports with minimum 4 x USB 3.0 ports and 4 x USB 2.0 ports with at least 2 on the front side		
		PS/2 keyboard and mouse ports		
		(1) VGA video port / HDMI port		
		(1) RJ-45 network connector		
		Rear Line In/Line Out jacks		
		Front 3.5mm headphone output and microphone in jack		
12	Form Factor	MT (Micro Tower)		
13	Power Supply	240 to 300W Active PFC, 85% efficient Power supply		
14	Keyboard	PS2/USB 104 keys keyboard (Same make as PC)		
15	Mouse	PS2/USB 2 Button Scroll Mouse (Same make as PC)		
16	Security	TPM 1.2 Security Chip		
		SATA port disablement (via BIOS)		
		Optional USB Port Disable at factory (user configurable via BIOS)		
		Removable media write/boot control		
		Power-On password (via BIOS)		
		Administrator password (via BIOS)		

SL	Parameter	Functionality	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
		Setup password (via BIOS)		
		Support for chassis padlocks and cable lock devices		
17	Operating System	Preinstalled Genuine Microsoft Windows11 Pro(64- bit) with License and Recovery CD or latest version		
18	Software	Preloaded Genuine Microsoft Office Professional plus (Latest Version)		
19	Compliance and Certification	ROHS and Win certification		
		Energy Star ver 5.2		
		EPEAT certified for India		
20	Warranty	5 years OEM Onsite warranty		

11.28. Display Monitor

SL	Parameter	Functionality	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
1	Monitor	22'' Wide TFT TCO Certified with matching port of workstation/desktop		

11.29. Laptop

S/N	Parameter	Specification	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
1	Processor	Intel 12th Generation Core i7- 12700 CPU or Latest		
2	Mother board / Chipset security features	Integrated with processor .TPM 2.0 (hardware based)and Integrated hardware Diagnostic tool in BIOS.		
3	RAM	Minimum 16 GB (1x 16GB) DDR4 Memory		

S/N	Parameter	Specification	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
4	RAM upgradability and Slots	Minimum 2 nos. DDR4 Memory slots supporting up to 32 GB or higher		
5	HDD	Minimum 1 TiB NVME M2 SSD PCIE 3.0 x4		
6	Communication & I/O Ports (Integrated in the laptop motherboard)	Minimum 4 USB ports out of which 2 No USB 3.1 andOne USB Type C 3.1 Gen1 , HDMI , VGA, RJ-45, SD 3.0 Memory card reader, Universal Audio port Jack security Lock slot.		
7	Keyboard & Mouse	Full size Backlit Keyboard with touchpad		
8	Camera	Minimum Integrated HD Webcam with Integrated microphones.		
9	Graphics	Integrated Intel HD Graphics		
10	Sound Card	Intel High Definition Audio with Integrated stereosound.		
11	Display	Minimum 14.0" FHD (1920 x 1080) Anti-Glare, LCD display or higher		
12	Battery Type	Minimum 4 hrs. back up		
13	Weight	Not more than 1.00 Kg.		
14	Wireless & Connectivity	Minimum Integrated Intel Dual Band Wireless (supporting 802.11a/b/g/n and ac) network and Bluetooth v 5.0 or higher.		
15	Bluetooth	Minimum Integrated Intel Dual Band Wireless (supporting 802.11a/b/g/n and ac) network		

S/N	Parameter	Specification	Compliance (Y/N)	Remark (If Any)
Make: **Model:**				
		andBluetooth v 5.0 or higher.		
16	Power and supply	External AC adapter of same OEM make		
17	Operating Systems	Microsoft Windows 11 Professional 64 Bit, with latest Service Pack Preloaded License. Systems Hardware driver should be available in OEM website against the offered model.		
18	Software	Preloaded Genuine Microsoft Office Professional plus (Latest Version)		
19	Certifications (for the quoted model)	For OEM: ISO 14001:2004 For the quoted Model :UL,FCC ,Energy Star 6.0/BIS ; EPEAT India, quoted model ROHS , Windows 10 Professional Operating system, Linux & MIL 810 Std. Certification		
20	Carry Case (same OEM make)	Standard Good Quality Carrying Case (Standard or Backpack with OEM Logo)		
21	Warranty	5 Years OEM onsite including labor and parts replacement (Battery minimum 3 years warranty). Warranty status must be available in OEM website against the supplied model serial no.		
22	Manageability	Laptop System Serial No, OEM Name, Model No, to be programmed into BIOS (CMOS); Same informationto be provided in Barcode and pasted on the back cover of the laptop for easy readability.		

11.30. Project Plan

SI shall deliver all project activities/milestones/deliverables to the Client as per the timelines stated in this section. OCAC or its authorized representative shall take thirty (30) days to review and provide comments on all respective deliverables. SI shall ensure that all comments provided by the OCAC, or its authorized representative shall be incorporated in the final version of all deliverables/activities.

All deliverables/activities indicated in the tables below are indicative only and shall be read in conjunction with the Scope of Work section and Standard Form of Contract of the RFP for detailed requirements. Client or its authorized representative reserves the right to ask for additional information, documents, and deliverables throughout the Project.

The start date of the project shall be from the date of signing the contract excluding the implementation period. No extensions shall be permitted by OCAC.

T0- Represents the Project Start Date (i.e. agreement signoff).

M – Represents the Milestone for the work.

Entities Involved in the project:

- OCAC: Odisha Computer Application Centre.
- Consultant: 3i Infotech India LLP
- SI: System Integrator

Week	Activity/ Milestones	OCAC	Consultant	Successful Bidder	Remarks
L0	Project Award	√	√	√	Issue of Letter of Intent (LOI). Letter of acceptance by successful bidder within 3 days of LOI. Draft MSA will be shared to successful bidder within 24 hours of acceptance by bidder.

Week	Activity/ Milestones	OCAC	Consultant	Successful Bidder	Remarks
L0+ 1 Weeks	Project Initiation	√	√	√	MSA to be signed within 1 Week from the date of issuance of LOI and PBG @ 10% of the TCV (Total Contract Value) to be submitted simultaneously.
T0	Project Kick-off & Mobilization	√	√	√	Kick-off meeting to happen within 10 days from the date of signing of MSA along with all the stake holders; Project plan to be submitted. T0 = Project Start Date
T0 + 75 Days	Commissioning & Testing of IT Systems, Cloud and Software solution, integration and migration of data & network from existing DC to new DC (PAT of IT System)	√	√	√	Bidder to carry out integrated system testing of all equipment and rectify all snags. Bidder needs to furnish weekly progress report and lay down integration plan, migration plan and User Acceptance Test Plan of IT Infrastructure.

Week	Activity/ Milestones	OCAC	Consultant	Successful Bidder	Remarks
T0 + 90 Days	Project Sign-Off & FAT (Go-Live of the Project)	√	√	√	Successful Final Acceptance Test of all commissioned IT and Non- IT systems and Issuance of Go-Live Certificate from OCAC.
T0+120 Days	ISO Certifications 27001:2013 or latest 9001:2015 20000 :2011 or latest 27017:2015	√	√	√	Submission of ISO Certifications.
T0+140 Days	Operations & Maintenance	√		√	Operation & Maintenance period shall be five years from the Go-Live of OSDC2.0.

* - Its System Integrator responsibility to insure MSA signoff will be complete within 30 Days from issuing of LOI; else T0 will be treated as Project start date

12. Project Bill of Quantity

Below mentioned BOQ are Indicative only, final BoQ may vary depends upon Solution proposed by Selected System Integrator. Selected System Integrator requested to submit detailed BoQ as per the proposed solution.

12.1. BOQ of IT items

Proposed solution is for setting up cloud environment using rack server's compute.

Note: It is an indicative BOQ only. As it is a solution-based project, the final BOQ may differ from System Integrator to System Integrator as per their solution.

#	IT Equipment + Software + Licenses	UOM	Quantity
1.	**Compute**		
a.	Server Type-A (Rack Server)	Nos	6
b.	Server Type-B (Rack Server)	Nos	10
2.	**Network**		
a.	Spine Switch	Nos	2
b.	Leaf Switch (Fibre)	Nos	10
c.	Access Switch	Nos	5
d.	Management Switch	Nos	4
e.	SDN Controller	Nos	1
f.	LR fibre module for OSDC 1.0 Core Switch (100G)	Nos	12
g.	LR fibre Module for Spine Switch(100G)	Nos	12
3.	**Storage**		
a.	SAN DIRECTOR (96 Ports) (96 FC ports of 32Gbps)	Nos	2
b.	SAN Switch (48 Ports)	Nos	4
c.	SAN Storage (1 PiB)	Nos	1
d.	32 Gbps LR fibre module for SAN switch	Nos	8
4.	**Load Balancer**		
a.	Link Load Balancer	Nos	2
b.	Server Load Balancer with 10 no of multiple instances	Nos	2
5.	**Security**		
a.	Next Generation Firewall with 10 no of multiple instances	Nos	2
b.	DDoS	Set	2
c.	Anti – Apt Solution	Set	1
d.	NIPS with 10 no virtual license	Set	1
e.	Web Application Firewall with 10 no of multiple instances	Nos	2
f.	DLP Solution	Nos	50
g.	Zero Trust Network (500 Users)	Set	1

#	IT Equipment + Software + Licenses	UOM	Quantity
6.	**Cyber Security Software**		
a.	Server Security solution (HIPS) Licences	Nos	200
b.	Endpoint Point Security Solution Licenses	Nos	50
7.	**On Premise Services (VM Based)**		
a.	**EMS, NMS & Helpdesk Management System (License Count)**	**Set**	**1**
	i. Network Operations Management	Nos	210
	ii. System Monitoring and Reporting for Fault, Performance & Consolidated event Dashboard	Nos	200 Servers and 12 DB
	iii. Server Automation	Nos	200
	iv. Service Management	Nos	10
	v. Asset Management	Nos	300
b.	Virtualisation & Management (core based)	Core	640
8.	**MGM Hardware/OS/DB**		
a.	Virtualization Software for MGM	Set	1
b.	Management Servers (Hardware) for MGM	Core	96
c.	Microsoft Operating System for MGM	Nos	12
d.	RedHat Operating System for MGM	Set	1
e.	Databases for MGM	Set	1
9.	**Software/License**		
a.	MS Windows Server Standard Latest Edition 2 Core License with required CAL Licenses	Nos	384
b.	Red Hat Linux Standard Latest Edition	Nos	20
10.	**Desktop / Printer**		
a.	Desktop with Keyboard & Mouse, without monitor	Nos	35
b.	Display Monitor	Nos	47
c.	Multifunctional Printer	Nos	2
d.	Laptop	Nos	6
11.	**MISCELLANEOUS**		
a.	ISO Certification (20000, 27001, 27017, 9001)	Set	1
12.	**Installation & Commissioning**		
a.	Installation, Configuration & Commissioning of all IT Equipment	Set	1
13.	**Integration**		
a.	Integration with OSDC 1.0, OSWAN, Sec-LAN, CSOC	Set	1

12.2. BOQ of Manpower

Sl No	IT Manpower	Qty	General Shift	1st Shift	2nd Shift	3rd Shift
1.	DC Project Manager	1	√	x	x	x
2.	Network Administrator	1	√	x	x	x
3.	SecurityAdministrator	1	√	x	x	x
4.	Cloud & Server Administrator	1	√	x	x	x
5.	EMS Specialist	1	√	x	x	x
6.	Database Administrator	2	√	x	√	x
7.	Storage Administrator	2	√	x	√	x
8.	Backup Administrator	1	√	x	x	x
9.	Cloud Network Engineer	4	√	√	√	√
10.	Cloud System Engineer	4	√	√	√	√
11.	Helpdesk Support	4	√	√	√	√
	Total	**22**	**11**	**3**	**5**	**3**

Note: Above manpower requirement table is indicative as minimum requirement for OSDC 2.0 and OSDC 1.0, bidder should have a clear prospective of the requirement of manpower to maintain the project and achieve the required SLA. Bidder should have their enough additional resource to meet the challenge of leave/replacement/changes and smooth delivery of services.

12.2.1. Resource Qualification and Experience

Sl No	IT Manpower	Minimum Qualification & Relevant Experience
1.	DC Project Manager	B.E. / B. Tech / MCA with 10+ Years' experience including minimum 5 years' experience in Data Centre project management with PMP / Prince2 / ITIL Certification.
2.	Network Administrator	B.E. / B. Tech / MCA or equivalent with 10+ Years' experience including minimum 4 year experience in Data Centre network management/WAN network management with OEM Certification like CCNP/CCSP/ CCNA Security/ CompTIA Security+ or equivalent.
3.	SecurityAdministrator	B.E. / B. Tech / MCA or equivalent with 10+ Years' experience including minimum 4 year experience in Data Centre Security management/WAN Security management with OEM Certification like CCNP/CCSP/ CCNA Security/

Sl No	IT Manpower	Minimum Qualification & Relevant Experience
		CompTIA Security+ or equivalent.
4.	Cloud and Server Administrator	B.E. / B. Tech/ MCA or equivalent with 10+ Years' experience including minimum 5 year experience in Server management and 2 years in cloud management with OEM Certification like AWS architect/ RHCA/ VCP/ CCNA Cloud or equivalent.
5.	EMS Specialist	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2 year experience in Data Centre Operation management with any OEM Certifications like ITIL/ Application Performance Management, Infrastructure Management, Health Monitoring, automation, Service Management etc.
6.	Database Administrator	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2-year experience in Data Centre Operation management with OEM Certification like OCA/OCP / MS SQL / My SQL / Postgres / Mongodb or equivalent.
7.	Storage Administrator	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2-year experience in Data Centre Operation management with OEM Certification in storage administration & management and backup area.
8.	Backup Administrator	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2-year experience in Data Centre Operation management with OEM Certification in storage administration & management and backup area.
9.	Cloud Network Engineer	B.E. / B. Tech with 5 years of experience, having 2 years relevant experience in Network Virtualization Management (NSX) or equivalent with networking knowledge and experience in managing router, switches, firewall, load balancer and other network equipment's.
10.	Cloud system Engineer	B.E. / B. Tech with 05 years of experience, having 04 years relevant experience in Cloud/ Virtualization Management with OEM level (L2) certification on VMware / equivalent. Additionally, experience in System Management and Administration.
11.	Helpdesk Support	BCA / BSc.IT or any Graduate with 2+ Years' relevant experience. Preferable IT knowledge in LAN/WAN/Cloud etc.

12.3. Project Timelines and Liquidated Damages

The System Integrator (SI) is obligated to adhere to the project timelines outlined in this section, ensuring the timely delivery of all activities, milestones, and deliverables to the Client. Upon submission, OCAC or its authorized representative will be granted thirty (30) days for the review and commentary on all corresponding deliverables. The SI must incorporate any provided comments from OCAC within the final versions of the deliverables.

The tables below outline indicative deliverables, to be interpreted in conjunction with the detailed requirements in the Scope of Work section and Standard Form of Contract of the Request for Proposal (RFP). The Client or its authorized representative reserves the right to request additional information, documents, and deliverables as needed throughout the project.

T0: Represents the Project Start Date, corresponding to the agreement signoff or kick-off meeting date. **W:** Represents the timeline in weeks following the agreement signoff or kick-off meeting.

Week	Activity/ Milestones	OCAC	Consultant	Successful Bidder	Remarks
L0	Project Award	√	√	√	Issue of Letter of Intent (LOI). Letter of acceptance by successful bidder within 3 days of LOI. Draft MSA will be shared to successful bidder within 24 hours of acceptance by bidder.
L0+ 1 Weeks	Project Initiation	√	√	√	MSA to be signed within 1 Week from the date of issuance of LOI and PBG @ 10% of the TCV (Total Contract Value) to be submitted simultaneously.

Week	Activity/ Milestones	OCAC	Consultant	Successful Bidder	Remarks
T0	Project Kick-off & Mobilization	√	√	√	Kick-off meeting to happen within 10 days from the date of signing of MSA along with all the stake holders; Project plan to be submitted. T0 = Project Start Date
T0 + 75 Days	Commissioning & Testing of IT Systems, Cloud and Software solution, integration and migration of data & network from existing DC to new DC (PAT of IT System)	√	√	√	Bidder to carry out integrated system testing of all equipment and rectify all snags. Bidder needs to furnish weekly progress report and lay down integration plan, migration plan and User Acceptance Test Plan of IT Infrastructure.
T0 + 90 Days	Project Sign-Off & FAT (Go-Live of the Project)	√	√	√	Successful Final Acceptance Test of all commissioned IT and Non- IT systems and Issuance of Go-Live Certificate from OCAC.
T0+120 Days	ISO Certifications 27001:2013 or latest 9001:2015 20000 :2011 or latest 27017:2015	√	√	√	Submission of ISO Certifications.
T0+140 Days	Operations & Maintenance	√		√	Operation & Maintenance period shall be five years from the Go-Live of SDC 2.0

12.4. Liquidated Damages Table

In the event that the Bidder fails to fulfil the work within the stipulated time frame outlined in the Contract Agreement or any agreed-upon extensions, OCAC reserves the right to recover Liquidated Damages from the Bidder. The calculation details are specified in the table below. For the purpose of acknowledgment of completion, equipment/work is considered delivered/completed only when all its components, parts, and items of work are also delivered/completed. Should certain components/items of equipment/work not be delivered on time, their delay will persist until the missing or incomplete parts/items of work are duly delivered or completed.

Sr. No.	Milestone	Severity	Liquidated Damage	Remarks
1	T0+3 Months = M3	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If fail in completion of works and delivery for more than 5 week, letter of Default will be issue for Improvement.
2	T0 + 4 Months = M4	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If fail in delivery for more than 5 week, letter of Default will be issue for Improvement.
3	T0+ 5 Months = M5	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will be hold.
4	T0+6 Months =M6	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will be hold.

Sr. No.	Milestone	Severity	Liquidated Damage	Remarks
5	T0+7.5 Months =M7	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will be hold.
6	T0+8 Months =M8 (Project Sign-Off & FAT (Go-Live of the Project)	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 10 weeks then, OCAC is free to cancel the WO/contract. The remaining part of work will be completed by OCAC or any agency engaged by OCAC at the cost of selected vendor.

Note:

- The recovery against aggregated liquidated damages shall not exceed 10% of the total contract value (TCV).
- If the bidder fails to complete all the specified Data Centre certifications in the RFP within 6 months, a penalty of 1% of the consolidated certificate cost will be charged per week after the expiration of the mentioned period.
- The T0 date of the Kick-off will be treated as the project start date. The total time for the completion of the project, OSDC 2.0, will be 10 months, including the certification of the Data Centre. 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 above.

12.5. Payment Schedule

Payment will be released to the successfully shortlisted bidder in phased manner as stated below:

Deliverables / Milestones	Timelines	Payment	Remarks
Supply of All servers. Storage and Network devices	T0 + 2.5 Months	20% of the Capex Amount Submission of as- build drawing, warranty documents, SOPs, Integration	Delivery acceptance by OCAC/CT Team
Supply of all hardware and Software (with Licenses) including their accessories besides Servers, Storage and Network devices	T0 + 3.5 Months	20% of the Capex Amount	Delivery acceptance by OCAC/CT Team
Installation of all Data center components.	T0 + 4 Months	40% of the Capex Amount	Installation certificates approved by OCAC consultant and Composite team
Configuration, Integration, Testing, commissioning and Go live.	T0 + 5 Months	20% of the Capex Amount	Go-Live certified by OCAC Consultant and Composite team
Operations and maintenance Management for 5 year payable quarterly		25% (per quarter) of the yearly quoted OPEX Amount.	Clearance from TPIA after due adjustment with SLA/Performance

Note:

- All payments to the successful bidder will be made in Indian Rupees only. Payments will be processed within thirty (30) days of receiving the invoice, subject to approval from the competent authority. Invoices must be issued in the name of OCAC.
- The Bidder is required to separately specify taxes in their invoices, and OCAC will pay the applicable taxes as per actuals after verification. Any tax savings will be deducted from the payable amount.
- If new taxes or changes in existing tax rates occur during the Agreement Period, OCAC will bear and pay these additional costs over and above the agreed price for each item, as per

the respective invoices raised by either Party/Member on OCAC. Similarly, any reduction in taxes will benefit OCAC. All invoices submitted to OCAC for payment should be tax invoices.

- The operational expenditure (OPEX) should not be less than 20% of the total quoted value.
- CAPEX includes the cost of IT equipment with Software, for OSDC 2.0 (Year 0 Cost).
- OPEX includes the operational expenditure such as manpower cost and annual maintenance cost of all equipment for 05 (Five) years (Year 1 + Year 2 + Year 3 + Year 4 + Year 5) to be incurred by the bidder for the operation and maintenance of OSDC 2.0 for 5 years after Go-Live.

12.6. Service Level Agreement (SLA)

- This SLA outlines the minimum service levels required based on contractual obligations, including performance indicators and measurements for OSDC. 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 the 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.

12.7. 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 Data Centre at the proposed site, as detailed in the RFP's Scope of Work:

- Onsite support for Data Centre Infrastructure Operations on a 247365 basis for five years to ensure 99.982% availability.

12.7.1. 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.

12.7.2. Category of SLA

- The SLA is logically segregated into the following categories:
- IT Infrastructure Related Service Level

Sr. No.	Definition	Measurement Interval	Target	Penalty
	Individual Server Availability (including the OS, database and the application running on it)		>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system

Sr. No.	Definition	Measurement Interval	Target	Penalty
1		Quarterly	>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
2	Storage Availability	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system
				[Record as Event of Default] Letter of warning may be issued to the bidder.
	Managed Backup Service Availability (with agreed retention period)		>=99.98%	No Penalty

Sr. No.	Definition	Measurement Interval	Target	Penalty
3	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		
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [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 for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system

Sr. No.	Definition	Measurement Interval	Target	Penalty
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
5	Preventive Maintenance DCO shall provide a detailed Preventive maintenance plan/Schedule on commencement of the Project.	Quarterly Reporting	100% Carried Out. PM Plan should be Approved from PM, OSDC/OCAC prior to be carried out in that quarter.	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.

- **Virtual Infrastructure /HCI Related Service Level**

Sr. No.	Definition	Measurement Interval	Target	Penalty
			Within 1 Hour after the approval of the request by the Customer/ User	0.5% of the QGR value for O&M of IT system for more 1 hours of delay beyond the target time. To the maximum capping of 5 hrs

Sr. No.	Definition	Measurement Interval	Target	Penalty
1	Provisioning and De-Provisioning of Virtual Machines	Quarterly		
				1.0 % of the QGR value for O&M of IT system for more 5 hours of delay on an incremental basis.
2	Overall Cloud Solution Availability (includes cloud network, cloud virtualization layer, cloud storage, virtual OS, cloud orchestration layer, cloud security layer and any other requisite component and services)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
			Up to 25	No Penalty

Sr. No.	Definition	Measurement Interval	Target	Penalty
3	Production Cloud or Cloud Dashboard is down, business operations severely impacted with no workaround; or a security issue	Every instance in the Quarter	minutes	
			>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 O&M of IT system for 1st time and 0.1 % of QGR value for O&M for IT system for every subsequent lapse.

- **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 within 2 hrs from the time of attack.	Every instance in the Quarter	Beyond 2 hrs	Rs.5,00,000.00 per DoS attack
	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ OSDC 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.			

Sl. No.	Definition	Measurement Interval	Target	Penalty
3		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 hour 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

- **Helpdesk Support Services**

Priority	Response Time	Resolution Time		MAT (Maximum Allowable Time) After Resolution Time.	
	PWH or EWH	**PWH**	**EWH**	**PWH**	**EWH**
1	10 minutes	Within 6 Hours	Within 6 Hours	4 Hours	4 hours
2	20 Minutes	Within 8 hours	Within 12 hours	4 hours	4 hours
3	30 Minutes	Within 12 hours	Within 24 hours	12 hours	12 hours

S NO	Definition	Measurement Interval	Target	Penalty
1	**"Resolution Time**", means time taken by the Bidder staff to troubleshoot and fix the problem from the time the call has been logged at the Helpdesk till the time the problem has been fixed.	Quarterly	100% calls to be resolved within 30 minutes	No Penalty
			Calls resolved after 30 minutes of OR Unresolved call	0.01% of the Total QGR value for every call (with the delay of 30 minute) on an incremental basis.

- **Manpower Related Service Level**

Sr. No.	Definition	Measurement Interval	Target	Penalty
1	Resource availability for all services agreed for Operation and Maintenance purpose of the project. DCO manpower should be available 24x7x365 days.	Quarterly	Single absence of a single resource	**No Penalty** (if replaced by equivalent skilled resource within 1 day) Replacement should be subject to prior approval of Project Manager OSDC/ OCAC.
				Double of the cost of the absent resource for the period of absence.

- **Compliance & Reporting Procedure**

Sr. No.	Measurement	Definition	Measurement	Target	Penalty
1	Submission of MIS Reports and QGR reports	The Bidder shall submit the MIS reports and QGR reports Quarterly and as and when required to OCAC/ OSDC, Odisha	Quarterly	Report for the previous quarter shall be submitted within the first week of next quarter.	No Penalty
				Delay beyond the date of submission	0.01% of the QGR value for every week time delay
2	Incident Reporting	Any failure/ incident on any part of the Data Centre infrastructure or its facilities shall be communicated immediately to Customer as an exceptional report giving details of downtime, if any.	Quarterly	100% Critical incidents to be reported to Customer within 1 hour with the cause, action and remedy for the incident.	No Penalty
				Delay beyond an hour	1% of the QGR Payment for every hour's delay on an incremental basis.
3	Change Management	Measurement of quality and timeliness of changes to the Data Centre facilities	Quarterly	100% of changes should follow formal change control procedures. All changes need to be approved by Customer. It should be implemented on time and as per schedule & without any disruption to business	0.1% of the QGR value for every non-compliance of Change request on an incremental basis.

Sr. No.	Measurement	Definition	Measurement	Target	Penalty
4	Scheduled Maintenance	Measures timely maintenance of the equipment installed at the Data Centre. The Bidder shall provide a detailed equipment maintenance plan on the commencement of the project.	Quarterly	100 % of scheduled maintenance should be carried out as per maintenance plan submitted by the Bidder. Any scheduled maintenance needs to be planned and intimated to Customer at least 2 working days in advance	0.1% of the QGR Payment for every non-compliance on an incremental basis
5	Implementation of Audit Recommendations	Implementation of audit recommendations by OCAC/OSDC or its auditor which have been agreed by Bidder & Customer to be implemented.	Half- yearly	100% on time to be implemented as per timelines agreed upon with Customer	0.5 % of the QGR Payment for every non compliance
6	Maintenance of Inventory	The Bidder should maintain an inventory of items that will be required on an ongoing basis for maintenance	Quarterly	100% as per the inventory log committed and maintained by Bidder.	0.1% of the QGR Payment for every non compliance

12.8. 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 Consultant/PMU and Customer 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 Customer and Bidder on performance targets.

12.8.1. IT Infrastructure Service Level

The IT Infrastructure service level applies to devices specified in the Bill of Materials (BOM) as per Proforma 22

Servers and Systems: As detailed in the Table of Proforma 22

Storage Devices: As outlined in the Table of Proforma 22

Network Devices: As specified in the Table of Proforma 22

Safety, Security, and IT Support Equipment: As identified in the Table of Proforma 22.

12.8.2. 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.

12.8.3. Service Window:

- **PWH (Prime Working Hours):** 8 AM to 8 PM (Monday to Saturday)
- **EWH (Extended Working Hours):** 8 PM to 8 AM (Monday to Saturday), Sunday, and all state Government Holidays.

12.8.4. Setting Priority Levels

The OSDC 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

OSDC. 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 SDC. 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 Data Centre without disrupting any services and failure/delay in undertaking and completing activities such as:

- Adding new device to Fabric.
- OS – Installation, Uninstallation
- Patch – Update, Remove,
- ... (and more)

This is an indicative list and not exhaustive.

12.8.5. 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/OSDC.
2. When the bidder withdraws the resource in accordance with its organizational policy due to non-performance or non-cooperation, aligning with OSDC 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/OSDC 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 table provided above serves as an indicative minimum requirement for OSDC 2.0 and the existing 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 a surplus of additional resources to effectively address challenges related to leave, replacement, and any necessary changes, ensuring the seamless delivery of services.

The general shift for manpower considerations is defined as 10:00 AM to 06:00 PM, excluding all state government holidays and national holidays.

Note:

- This Bill of Quantities (BOQ) is presented as an indicative document, and any additional items necessary to ensure the completeness of the solution must be quoted as separate line items, including their respective quantities and prices.
- Bidders are required to submit a comprehensive, unpriced BOQ aligned with their proposed solution as part of the technical bid.

12.8.6. 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, encompasses round-the-clock monitoring, maintenance, and management of the complete Data Centre infrastructure. This includes the provision of Helpdesk services, ensuring a minimum uptime efficiency of 99.982% for Odisha State Data Centre 2.0 (OSDC 2.0) and other managed facilities. The objective is to assure the operations team, service providers, 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 Data Centre (OSDC).

- **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**

12.8.7. Commissioning of System

i. The bidder should predefine 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 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.

12.8.8. Human Resource and Planning

Adequate staffing, with the right qualifications, is crucial for OSDC 2.0 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 Data Centre without impacting its functionality.

Requirements:

- **Organizational Structure:** Clearly outlines the DC department structure and defines team responsibilities related to Data Centre operations.
- **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 Data Centre is qualified, trained,

and experienced in managing its operations.

- **RACI Matrix:** Clearly assigns responsibilities, accountability, consultation, or notification for specific tasks as per defined requirements.

Note:

The manpower requirement table above serves as an indication of the minimum personnel needed for OSDC 2.0 and the existing DC. However, bidders are expected to possess a comprehensive understanding of the manpower requirements essential for project maintenance and meeting the stipulated SLA. It is imperative for the bidder to anticipate challenges related to leave, replacements, changes, and ensure the seamless delivery of services. Additionally, it is mandated that key resources and IT manpower (excluding Helpdesk Executives) outlined in the resource table must be employees on the payroll of the successful bidder's company.

Note:

1. All qualifications and certifications of the mentioned employees will undergo verification by OCAC/Composite Team post the contract award. Consultant/PMU (assigned) will conduct periodic verifications during the Operation and Maintenance phase.
2. In the event of any deficiency found in the profile parameters, OCAC reserves the right to reject the manpower. The bidder must replace the resource within 15 days from the date of rejection.

12.8.9. Policies and Procedures

An effective OSDC 2.0 management strategy necessitates documented and enforced policies and procedures. These guidelines prevent inconsistencies, reducing the risk of service interruptions or downtime.

Requirements:

- Data Centre User Manual
- Data Centre Instructions
- Emergency/Crisis Management Plan
- SOPs (Standard Operating Procedures)
- Health & Safety Procedures
- Change Management Procedures
- Access Procedures
- Maintenance Procedures

12.8.10. 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

12.8.11. 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

12.8.12. Access Management

This guideline outlines the criteria for granting access to OSDC 2.0, 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.

12.8.13. 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:

- Data Centre Induction
- Data Centre Trainings

Bidder shall provide all necessary training to OCAC officials and authorized team members for the successful functioning of the Data Centre operation and management.

12.8.14. 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

12.8.15. Reporting

Accurate, objective, and complete reporting is crucial for referencing. Reports include Data Centre Activity, Preventive Maintenance, Incident, KPI, and Service-related metrics.

12.8.16. Monthly Reports

Consolidated monthly reports include ICT infrastructure availability, SLA/non-conformance, issues/complaints, systems rebooted, backup and restoration log, changes in the Data Centre, 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 Data Centre uptime.
4. Summary of changes in the Data Centre.
5. Log of preventive/scheduled maintenance undertaken.
6. Log of break-fix maintenance undertaken.
7. Details of manpower availability at the Data Centre.

12.8.17. Half-Yearly Reports

Consolidated component-wise reports on ICT infrastructure availability and resource utilization should be submitted in softcopy. Additionally, a Data Centre Security Audit Report, IT infrastructure Upgrade/Obsolescence Report, and another consolidated component-wise ICT infrastructure availability and resource utilization report should be submitted in hardcopy.

12.8.18. 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 hardcopies may be required upon OCAC's request.

12.8.19. Incident Reporting

A. Software License Violations:

1. OCAC will annually audit the IT infrastructure solution by a third-party, ensuring proper software versions and compliance.
2. The audit report will offer recommendations on infrastructure issues and obsolescence.
3. The audit covers IT infrastructure obsolescence, providing recommendations for upgrades and disposal plans.
4. A half-yearly security audit will assess security practices and vulnerability, rating them as Satisfactory, Requires Improvement, or Unsatisfactory.
5. Bidder support and cooperation are essential for these audits.
6. Bidder must implement audit recommendations within defined service levels.

B. 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 reports, and more.
3. All documents will be owned by OCAC.

C. 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.

12.8.20. 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.

12.8.21. 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.

12.8.22. O & M Roles and Responsibilities

12.8.22.1. 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.

12.8.22.2. Responsibilities of OCAC:

1. Provide timely approvals and sign-offs for deliverables.
2. Direct and monitor Bidder activities as per RFP and validate service levels as per SLA.

13.8.10 Certification

Various operational standards must be followed, and the Data Centre should adhere to international standards provided by ISO. The following certifications are required:

- ISO 9001
- ISO 20000
- ISO 27001
- ISO 27017

13.8.11 Automation of Services

OSDC 2.0 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 of all DC alerts related to critical equipment through SMS or Email to all concerned.

12.1 Handing Over Taking Over (HOTO) Plan

The selected SI will conduct a comprehensive analysis of the existing SDC (AS-IS basis) in collaboration with the current DCO, Project Consultants, Composite Team, OCAC, and other stakeholders. The HOTO plan involves a seamless transition of SDC 1.0 from the current 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 DCO, 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 DCO 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 DCO will provide shadow support for 10 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. Proforma and Schedules

13.1. Proforma 1: Proposal Covering Letter

(Bidder's Letter Head)

To

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 " IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar.

Ref: RFP Enq. No. – XXXXXXXXXXXXXXX, Dtd. XX/XX/2024

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 for the Selection of System Integrator IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY).

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.

Dated this Day of 2023

(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.

13.2. Proforma 2: Declaration of Acceptance of Terms & Conditions of RFP

(Bidder's Letter Head)

To
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

Ref: RFP Enq. No. – XXXXXXXXXXXXXXX, Dtd. XX/XX/2024

Sir/Madam,

I have meticulously reviewed the Terms & Conditions stipulated in the RFP Document [OCAC/ /] concerning the RFP for the Selection of System Integrator " IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar.

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 System Integrator)

Name:
Designation:
Place:
Date:

13.3. Proforma 3: Format of Technical Proposal Document

(Bidder's Letter Head)

RFP Ref. No.: OCAC/ / Date:

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 Technical Proposal for " IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar

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 aforementioned reasons.

We acknowledge that OCAC is not obligated to accept any Proposal received.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Designation:

Place:

Date:

13.4. Proforma 4: Forwarding Letter for Earnest Money Deposit

(Bidder’s Letter Head)

From (Name & complete address of the bidder)

Bidder’s Name

Bidder’s Address

To
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 for "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)” at OCAC Tower, Bhubaneswar.

Reference: RFP number <OCAC/__/Dated __/__>

We, M/s <*Bidder's Name*>, having carefully read and examined in detail the RFP document for " selection of System Integrator (SI) for IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)” at OCAC Tower, Bhubaneswar, 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.
Thanking you, Yours sincerely,
(Seal & Signature of the Authorized signatory of the System Integrator)
Name:
Place:
Designation:
Date:
Encl: - Copy of Earnest Money Deposit

13.5. **Proforma 5:** Format for Furnishing Earnest Money Deposit

Whereas (hereinafter called the "tenderer") has submitted their offer dated for Selection of System Integrator for "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY) 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 tenderer 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 from the last date of RFP submission date/ RFP validity date, and any demand in respect thereof should reach the Bank not 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. Proforma 6: Company Profile of Bidder

(Bidder's Letter Head)

Reference: RFP number <OCAC/__/Dated __/__>

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:	
Web-Site & -mail ID for any grievance		

(Seal & Signature of the Authorized signatory of the System Integrator)Name:
Place:

13.7. Proforma 7: Declaration regarding Clean Track Record

(Bidder's Letter Head)

DECLARATION REGARDING CLEAN TRACK RECORD

Reference: RFP number <OCAC/__/Dated __/__>

To

General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013
Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [OCAC/ /_] regarding RFP for Selection of System Integrator for "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar.

I hereby declare that to the best of my knowledge and based on the documents available my company has not been debarred / blacklisted by Central Govt./ any State Govt. I further certify thatI am competent authority in my company has authorized me to make this declaration.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System

Integrator)Name:

Pla

ce:

Designation: Date:

13.8. Proforma 8: Undertaking on litigation

(Bidder's Letter Head)

Reference: RFP number <OCAC/__/Dated __/__>

Undertaking on litigation(s)

This is to certify that << COMPANY NAME >> is not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP.

Company Secretary / Authorized

SignatoryName of Signatory:

Bidder Company

Name:Date:

Place:

13.9. Proforma 9: Undertaking on Not Being Black-Listed

(Bidder's Letter Head)

Reference: RFP number <OCAC/__/Dated __/__>

Undertaking on Not Being Black-Listed

This is to certify that to the best of my knowledge and based on the documents available << COMPANY NAME >> is not blacklisted by the Government of Odisha or any of its agencies for any reasons whatsoever and not blacklisted by Central / any other State/UT Government or its agencies for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices andnot backed out from executing the work after award of the work as on the RFP submission date.

Company Secretary / Authorized
SignatoryName of Signatory:

Bidder Company
Name:Date:
Place:

13.10. Proforma 10: Undertaking of Service Level Compliance

(On the Bidder's Letterhead)

RFP Ref. No.: OCAC/_____/___ Date:

To

General Manager (Admin)

Odisha Computer Application Centre,

N1/ 7D, Acharya Vihar Square, Near Planetarium,

P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Dear Sir/Madam,

Sub: Undertaking on Service Level Compliance

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 tobe insufficient in meeting the RFP and/or the service level requirements given by OCAC, thenwe will augment the same without any additional cost to OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)Name:

Place:

Designation: Date:

13.11. Proforma 11: Authorization Letters from all OEMs

(OEM's Letter Head)

RFP Ref. No.: OCAC/_____/___ Date:

To,

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 "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar.

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 :

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

13.12. Proforma 12: OEM’s Support Form

(OEM’s Letter Head)

RFP Ref. No.: OCAC/____/___ Date:

To,

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 “IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)” at OCAC Tower, Bhubaneswar

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 freely upgrade them for a period of Five years of Operations and Maintenance, from the date of go-live of the project, by M/s___(name and address of the Bidder) who has proposed to use for the project “IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)” at OCAC Tower, Bhubaneswar or his successor. We would also adhere to the timelines for maintenance as indicated in this RFP by closely working with the Bidder or his successor for a period of five years from the date of supply of the equipment. 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 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 :

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

13.13. Proforma 13: Warranty Certificate Undertaking

(OEM's Letter Head)

RFP Ref. No.: OCAC/ / Date:

To

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 "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar.

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 shallbe 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 conformto the specifications and for which notice is promptly given by OCAC to us (Bidder). We shall provideon-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 serviceperiod for services).

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation: Date:

13.14. Proforma 14: Declaration by OEM

(OEM's Letter Head)

RFP Ref. No.: OCAC/ / Date:

To
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 "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar

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 Enq. No. XXXXXXXXXXXX, Date XX/XX/2024.

We here by declare that, the MAF is bind with the bidder and can not be revoked by <OEM Name) at any point of time during the Bid Process Management 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. It should be included by the bidder in its Pre-qualification bid.

13.15. Proforma 15: Technical specification compliance by OEM.

(OEM’s Letter Head)

RFP Ref. No.: OCAC/ / Date:

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 System Integrator)

Name:

Place:

Designation: Date:

13.16. Proforma 16: Statement of No Deviation from Requirement Specifications

(Bidders's Letter Head)

RFP Ref. No.: OCAC/ / Date:
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.

Thanking you, Yours sincerely,
(Seal & Signature of the Authorized signatory of the System Integrator)

Name: Place:
Designation: Date:

13.17. Proforma 17: Bidder’s Annual Turnover

(On the Applicant Statutory Auditors Letterhead)

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	2017-18	2018-19	2019-20
1	Total Sales as per the P/L A/c (A)			
2	Less: Custom and/or Excise Duty if included intotal 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 perP/L A/c (C)			
4	Less: Any other statutory taxes if included intotal 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

/CAName of Signatory:

Bidder Company Name:

Date: Place:

13.18. Proforma 18: Bidder's Net worth

Net Worth calculation

(On Applicant's Statutory Auditor's letterhead)

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	2017-18	2018-19	2019-20
1	Paid up Share Capital as per B/S (A)			
2	Add: Free Reserves as per B/S (B)			
3	Less: Deferred Payment if any as per B/S (C)			
4	Amount of probable impact on reserves due to audit qualification (D)			
5	Net Worth (F) =(A)+(B)(C)-(D)			
6	Annual Turnover (F) ==(A)-(B)-(C)-(D)-(E)			

Note: Please attach audited Balance Sheets and IT return statements to confirming the figures mentioned in columns.

Company Secretary / Statutory Auditor /CA Name of Signatory:

Bidder Company Name: Date:

13.19. Proforma 19: Project Credentials Format

(Bidder's Letter Head)

RFP Ref. No.: OCAC/ / Date:

Sl. No.	Item	Detail
General Information		
1.	Customer Name/ Government Department	
2.	Details of Contact Person • Name: • Designation: • Email: • Phone: & Fax: • Mailing Address:	
Project Details		
3.	Name of the project	
4.	Government/Non-government	
5.	Start Date/End Date	
6.	Current Status	(work in Progress (PAT/FAT/Go-Live) OR completed)
7.	Contract Tenure	
8.	Area of the Data Centre	
9.	Effort involved in Payroll person-months in the complete project	
10	Order Value of the project (in Crores)	
11.	Please provide copies of Work Order or Certificate of Completion for completed projects from the customer	
More than one same table content may be provided for more than one project detail.		

I do hereby acknowledge that the details provided above are true to best of my knowledge.
Yours sincerely,
(Seal & Signature of the Authorized signatory of the System Integrator)

Name: Place:
Designation:Date:

13.20. Proforma 20: Format for providing CV of Key Personnel

(Bidders's Letter Head)

RFP Ref. No.: OCAC/ / Date:

Curriculum Vitae of Key Personnel's

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 Resources	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	YES/N	

Sl. No.	Particulars	Details	Supporting document
	firmin its own payrolls	O	
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.

*Starting with present position, list in reverse order every employment held by the staff membersince graduation

**Among the assignments in which the staff has been involved, indicate brief details of the projectin which this responsibility was assigned (including nature and duration of duty)

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name: Place:

Designation: Date:

13.21. Proforma 21: Detailed Timelines and Work Plan with proposed Manpower Strength

(Bidders's Letter Head)

RFP Ref. No.: OCAC/ / Date:

The Bidder is supposed to specify a detailed work plan for all activities that will be carried out during the project implementation phase and proposed engagement of manpower strength on monthly basis. Provided below is an indicative work plan.

#	Activities	Months												
		1	2	3	4	5	6	7	8	9	10	11	12	
1	Design Validation													
2	Design and OEM Approval by Customer / Consultant													
3	Statutory Approvals (if Any)													
4	Commissioning and Testing of all systems													
5	Handing Over to customer for ICT Installation													
6	SITC of ICT infrastructure													

Indicate all main activities of the assignment, including delivery of reports (e.g. inception, interim and final reports) and other benchmarks such as Customer approvals. Duration of activities shall be indicated in the form of a bar chart. Please specify other activity (Addition or Deletion), if not listed in the form.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator) Name: Place:
Designation: Date:

13.22. Proforma 22: Format for Unpriced Bill of Material

(Bidders's Letter Head)

RFP Ref. No.: OCAC/ / Date:

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 System Integrator) Name: Place:
Designation:Date:

13.23. Proforma 23: Format for Performance for Bank Guarantee (PBG)

RFP Ref. No.: OCAC/ / Date:

To,

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 office 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

13.24. Proforma 24: Format of Commercial Proposal Document

(Bidders's Letter Head)

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 for IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar.

Reference: RFP No: **OCAC/_______/_____** Dated:**___/_____/________**

We, the undersigned Bidder, having read and examined in detail the RFP documents for **"**RFP for Selection of System Integrator for "IT Infrastructure expansion of Odisha State Data Centre (ODYSSEY)" at OCAC Tower, Bhubaneswar. I / we do hereby propose to provide services as specifiedin the RFP documents number **OCAC/____/__ Dated __/__/_____**

1. PRICE PROPOSAL AND VALIDITY

All the prices mentioned in our RFP are in accordance with the terms as 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 on account 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 shall 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 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.

7. PERFORMANCE BANK GUARANTEE BOND

We hereby declare that in case the contract is awarded to us, we shall submit the PBG bond in the form prescribed in Proforma of Bank Guarantee towards PBG and as per General Conditions of Contract. We hereby declare that our RFP is made in good faith, without collusion or fraud and the information contained in the RFP is true and correct to the best of our knowledge and belief. We understand that our RFP is binding on us and that you are not bound to accept a RFP you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)
Name:
Designation:
Place:
Date:

13.25. Proforma 25: Undertaking on Exit Management and Transition

(On the Bidder's Letterhead)

RFP Ref. No: OCAC/____/_____ Date:

To
General Manager (Admin)
Odisha Computer Application Centre,
N1/ 7D, Acharya Vihar Square, Near Planetarium,
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Dear Sir/Madam,

Sub: Undertaking on Exit Management and Transition

1. 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 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.

2. I/We also understand that the Exit management and transition will be considered complete on the basis of approval from OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator) Name: Place:

Designation:Date

END OF DOCUMENT