Compliance matrix

Parameter	Specification	Compliance(Yes/NO)
Capacity	The system should be configured with 60 TB usable capacity or more using NL-SAS 7.2K or better RPM Drives with Triple drive failure protection.	
Storage Controller1	The Storage system offered must be a true unified and scale-out system offering NAS (file) , SAN (block) and object workloads. The Storage supplied should be an appliance with a Single Microcode offering all protocols and should not be based on server based General Purpose Filesystems or Operating systems such as Linux, Windows etc.	
Storage Controller2	Storage system must be offered in a No-Single-Point of Failure offering upto six 9s of availability with minimum 2 Nodes/Controllers and Scale-Out to minimum 12 Nodes/Controllers.	
Cache/Memory Support1	The system should be offered with minimum 128 GB or more Distributed/Global/Federated DRAM cache across dual controllers. The cache should be scalable to 384 GB or more in a scale-out architecture with minimum 12 Controllers or better. System should offer capability to protect the write cache in case of a controller failure. Also, a failure of controller should not lead to write-through mode for cache.	
Cache/Memory Support2	The system should be configured with minimum 2TB or more of SSD/Flash/NVMe in addition to the above and same should be scalable to 12TB or more.	
Number of Concurrent connection support	512 or more.	
Raid Level Support	Raid 6 or equiavalent or better and the usable capacity should be config with dual drive failure	
Drive Support	The system must support intermixing of SSD, SAS, and NL-SAS drives , each of 12Gbps or more interface speed to meet the capacity and performance requirements for the applications. The system must support a minimum of 144 disks or more for scalability purpose.	
Disk Drive Protection	The proposed system should offer minimum dual drive failure protection, however for high density drives it should also support triple drive failure protection for better resiliency and performance.	
Protocols	The storage should be configured natively with FC, iSCSI, NFS (NFSv3, NFSv4, NFSv4.1 supporting RFC5661), CIFS/SMB protocols for use with different applications. In addition to the above, Object (S3 compatible) protocol should also be supported either natively or through any additional appliance.	
Front-End and Backend connectivity	The proposed storage system should have minimum 4x12Gb SAS ports and 8 x 16Gbps FC front end ports available across dual controllers.	
Storage General Features1	Capability of moving the hot data to high-performance drives and cold data to low performance drives in real time. The system should provide capabillity to tier data to high density drives on premise and off premise to an object storage or equivalent plarform preserving data efficiencies .	
Storage General Features2	The proposed system should offer centralized, application-consistent data protection supported for various applications.	
Data Protection1	The proposed system/solution should offer incremental replication capabilities in both fan-out and cascading topologies. The WAN replication should be secured by end-to-end encryption and bandwidth optmization supported natively. All the necessary licenses should be available on day 1.	
Data Protection2	The system offered should provide the ability to recover files, databases, and complete volumes instantaneously from the snapshot copies.	
Data Protection3	The proposed system should be offered with the necessary licenses/software that simplify backup, restore and clone management by allowing moutable snapshots and clones without disruption to production.	

Data Protection4	The Proposed Storage system should have native GUI to monitor & perform operations on data protection jobs	
Data Protection5	Proposed storage should offer capabilities to create backup copies across sites and also allow replication of data across backup targets. Any license required should be configured.	
Security and Encryption1	Storage shall provide the capability to santize disk to ensure that data can be made un-readable while replacing the Disk Drives in the array.	
Security and Encryption2	The storage system should support the functionality to enable administrators in limiting or restricting users' administrative access granted for their defined role.	
Security and Encryption3	The Storage system should support (UEFI) secure boot to ensure that only signed and verified images are used to boot the system. Storage array should provide security feature while booting by ensuring that Key Manager manages keys to lock/unlock drives and associated volumes.	
Security and Encryption4	The storage system should offer capability towards visibility, detection and remediation of ransomware attacks. The storage system should provide a file blocking methodology that allows organizations to filter or block traffic based on file extensions and file metadata	
Security and Encryption5	Storage system must use TLS for secure communication and administration functions such as secure log forwarding.	
Security and Encryption6	Storage management software should support MFA to ensure secure access of Management Software. The Storage array should support SHA-2 level security for manging user credentials	
Security and Administration	Multi admin authentication facility for critical operation.	
Security and auditing	Audit Trail Capability – The Storage solution shall offer suitable solution to retain detailed of NFS Transaction Log to record every file access on the shared file system. The audit log shall include access time stamp, client node IP, mode of access (read or write) and user information. This log shall be retained at least for last 72 hours and shall be in searchable format. Vendor shall offer required resources for capturing this information.	
Security and Encryption7	Proposed storage should support block level data de-duplication , compression for all kinds of data (structured & unstructured), compaction and Thin provisioning .	
Data Reduction Technology / Storage Efficiency	The Storage Management Software should offer operational simplicity and rich data management functionalities for Unified Storage. It should provide a single dashboard to monitor health, availability, capacity usage, performance, and data protection status of various platforms along with resource planning.	
Mangement1	The management tool should display system alerts and notifications for proactive management on the dashboard for users to quickly access them and it should provide information about support cases raised on the cluster.	
Mangement2	The management tool should offer global search bar for all storage objects and also action based searching.	
Mangement3	The offered system should offer capability to find and fix security vulnerabilities and automate risk remediation.	
Management4	Suitable methodologies need to be provided for uploading and downloading files securely.	
Mangement5	The offered system should support ransomware and insider threat detection to protect data with early detection and actionable intelligence on ransomware and other malware incursions. It should detect malicious activity and protect the data by automatically taking a snapshot.	
Rack Mountable	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided and installed by the vendor.	
Service Center or Support	Vendor should have service or support center at Bengaluru .	
OEM Certification	The bidder must provide authorization letter from the OEM for their participation in this tender.	
Storage Quality Certification	OEM should have delivered more than 100 TB capacity storage solution to any Central Government agency/PSU's in last two years & document proof to be provided	
ISO certification	The bidder should have a valid ISO certification	

Warranty	The Hardware and software quoted should have 5 years support along with upgrade and updates periodically. Faulty disk will not be returned to OEM or vendor.Warranty support should including the above policy.	
Power Supply	Dual Redundant Power Supply	