

Primary Storage

In case the model (storage/size/any other spec) is different for different environments, compliance is to be provided for each make/model separately

Make of the Storage			
Model of the Storage			
S.No.	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents
1	The proposed array should be an all-NVMe array with active-active multi-controller/node scale-out architecture. The array should be scalable to at-least 4 active-active storage controllers/nodes, Proposed Storage should support non-disruptively upgrades, and proposed storage should support single/Dual drive capacity upgrade.The proposed array should support data in place upgrade to higher models of the same storage family.		
2	The proposed array should have multi-controller architecture with support of NVMe media for optimal storage performance.		
3	The proposed array should be an unified storage which support both SAN & NAS		
4	The proposed array should be configured using all NVMe drives on Industry standard RAID6 and should be able to deliver at least 1,50,000 IOPS (8K block size, 80% Read/20% Write) with minimal latency for both read & write IOs. Mentioned performance numbers should be achieved with data reduction techniques like Compression & deduplication and data Encryption turned ON. OEM should submit the document / official sizing tool output stating the above-mentioned performance metrics capability of the proposed system. These performance numbers should be delivered after considering the overheads of deduplication, compression and encryption. The capacity to be configured as a single/multiple storage pool which should be accessible to both the controllers simultaneously for Read & Write operations.		
5	Proposed storage solution should be offered with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage. The NVMe SSD capacity drives must not be used for any caching requirements of the storage. The caching requirements of storage must be factored separately		
6	The proposed array should be designed with full redundancy across all components at both the hardware and software level enabling the system to have 99.9999% availability or more		
7	The proposed array should support FC, iSCSI , (NFS v4.0 or above)/ (SMB 3.1 or above), NVMe/TCP, NVMe/FC from day one.		
8	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.		
9	The storage must be configured with proposed storage usable capacity after dedupe and compression. It should be scalable to at-least 2x usable flash NVMe capacity on the same storage Array. The storage should support volume movement within the cluster. Addition of controllers/nodes in the same cluster should not cause any downtime and the system should automatically detect and add new controllers/nodes to the cluster.		
10	The proposed array must support the latest industry standard (No proprietary) dual ported NVMe TLC / QLC drives.		
11	The proposed array should support enterprise class data services including - Thin Provisioning, Inline Compression & Deduplication, replication. Data reduction must be supported on block and vVol. The data reduction feature should have no performance impact on the storage due to DRR.		
12	Proposed storage array should support major Operating systems including Windows 2019, 2022, 2025 RedHat, SUSE, Ubuntu, Oracle, VMWare etc.		

13	The proposed array must have capability to create snapshots in the proposed storage array for block, Proposed storage solution should support snapshot creation using ROW/WORM algorithm. Storage arrays should have ability to use snapshot as writable volume. These snapshots should be secure and immutable.		
14	Proposed array should include LUN level priority based QoS engine which is easy to manage. Proposed solution should also have functionality so that a volume with a high-performance policy can be configured handle more IOPS than a volume with a medium-performance policy.		
15	The proposed array should be proposed with native IP ports for remote replication to DR site with appropriate licenses. If separate FCIP routers are required for replication, then the same should be included in the BOM (Min 2 Nos per site).Proposed storage system should be capable of native storage based asynchronous replication .		
16	The proposed array should be supplied with native Storage management software with Web based GUI capable of generating customized reports, real time monitoring, at least 1 year of historical performance data for analysis and trending, capacity utilization monitoring.		
17	The proposed Storage solution should support or integrate with software (either OEMprovided or third-party) capable of automating and orchestrating application/database-consistent copies for applications including, but not limited to, MSSQL, Oracle, Exchange, to support use cases such as data repurposing, off-host backup, Test/Dev, Reporting, etc.		
18	Proposed storage solution should support below integration options to enable DevOps and Infrastructure automation. All mentioned options should be officially supported by storage OEM. a) Support for REST API b) Support for Kubernetes Persistent Volumes using Container Storage Integration (CSI) c) Support for Ansible d) Support for PowerShell modules		
19	The proposed array must include SED (or hardware) based data at rest encryption solution to encrypt data on all drives (AES 256 bit) with embedded automated key management. Encryption should seamlessly work with all the storage features and without any performance penalty.		
20	Bank will not return the defective disk(s) in case of disk failure		
21	If the OEM proposes effective storage capacity, then DRR should be applicable for the entire contract period. Incase, the DRR is not achieved anytime during the contract period, the OEM is liable to supply the additional drives/capacity to meet the required performance and effective capacity at no additional cost to the bank.		
	EXPERIENCE		
22	The proposed make of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI		

NOTE	It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed primary storage offered as part of the solution.
------	---

x86 Servers

In case the model (Server/processor/memory/HDD/any other spec) is different for different application/deployment zone/environments, compliance is to be provided for each make/model separately

Make of the server				
Model of the server				
S.No.	Item	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents
1	Processors	Latest upto 64 cores dual processor model (Intel Xeon or AMD EPYC) with base clock speed of 2.2 GHz or better as per the requirement and proposition proposed by the bidder		
2	Chipset	Processor OEM Chipset compatible with the offered processors.		
3	Internal Storage	The server should Support minimum 8 hot-swappable NVMe drives or more		
4		Server should be supplied with 2x 1.92TB NVMe SSD or higher. Bank will not return the defective disk(s) in case of disk failure		
5		The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 4GB NV cache or higher		
6	Memory	Should be configured with 1TB memory or more Should have minimum 24 number of DIMM slots per server and support 6400MT/s or higher Dual Rank DDR5 memory or higher		
7	Operating System	Must be supplied with enterprise-level OEM supported Operating System and Virtualization solution, as required		
8	Network	2x Dual Port card with 25G SFP+ Ports with optics		
9	SAN Connectivity	2 x Dual Port 32 Gbps FC Card		
10	PCIe Slots	Should have minimum 4 or more PCIe Generation 5.0 slots or higher		
11	Security	Should have a cyber-resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks		
12		Should provide effective protection, reliable detection & rapid recovery using:		
13		Silicon-based Immutable Hardware Root of Trust		
14		Signed cryptographic firmware updates		
15		Dynamic USB Port Management		
16		Secure default passwords		
17		Shall provide dynamic system lock down server to prevent malicious attacks against embedded firmware and configuration drift in your datacenter without need to reboot the server.		
18		Persistent event logging including user activity		
19		Secure alerting		
20		Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted (either due to a malicious attack, or due to a power loss during the update process, or due to any other unforeseen event).		
21		Shall support boot from SAN and Rapid OS Recovery In the event of a corrupted OS image		

22		Support Secure System Erase to erase sensitive data and settings from the server storage devices and server non-volatile stores such as caches and logs so that no confidential information unintentionally leaks		
23		Configuration upgrades should be only with cryptographically signed firmware and software		
24		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware		
25		Intrusion alert in case chassis cover being opened		
26	Management	Real-time power meter, temperature monitoring, customized exhaust temperature and System Airflow Consumption		
27		Silicon root of trust, authenticated BIOS, signed firmware updates and BIOS Live Scanning for malicious firmware		
28		Telemetry Streaming		
29		Idle Server Detection		
30		Power control, Boot control		
31		The management software should collect system information (including impending component failure) from the device that generated the alert and should be able to send the information securely to OEM to Support to troubleshoot the issue and provide an appropriate solution.		
32		OEM's management software should be provided		
33		Firmware and configuration baselines for compliance monitoring and enable automated updates on schedule.		
34		Scope based access control to limit Users to specific group of devices		
35		Bare-metal server deployment and cloning		
36	Ports	Should have the following ports for server connectivity		
37		● 3 USB 2.0 ports or higher		
38		● 1 VGA port		
39	Others	Supports hot swappable redundant fans		
40		Supports hot swappable redundant power supplies		
41		Sliding Rail Kit to be provided along with the server		
	EXPERIENCE			
42		The proposed server make should have been successfully implemented in at least two BFSI clients, each with a minimum of 1,500 branches or offices		

x86 Servers				
In case the model (Server/processor/memory/HDD/any other spec) is different for different application/deployment zone/environments, compliance is to be provided for each make/model separately				
Make of the server				
Model of the server				
S.No.	Item	Minimum Technical Specification	Compliance (YES/NO)	Remarks/Datasheet Referece
1	Form Factor	1U/2U rack mounted with sliding rails		
2	Configured CPU	At least Dual 64 Cores Latest Intel Xeon Gold Series or latest AMD EPYC series with base clock speed of minimum 2.2Ghz		
3	Memory slots	Minimum 24 DDR5 DIMM slots		
4	Memory configured	1 TB populated with 6400MT/s Dual Rank modules		
5	Disks supported	Scalable Upto 8 NVMe drives		
6	Disks configured	Drives 2 x 1.92TB NVMe for OS in RAID1, Hot Plug or higher. Bank will not return the defective disk(s) in case of disk failure		
7	Operating System	Must be supplied with Windows Datacenter license		
8	GPU Memory	94 Gb or higher		
9	RAID Controller	HW RAID Card with minimum 4GB NV cache, supporting RAID 1, 5, 6, 10		
10	I/O slots	Server should support minimum four PCI-Express 5.0 slots.		
11	Ethernet ports	8x 25G SFP+ ports (card level redundancy required)		
12	Fibre Channel Ports	2x Dual Port 32 Gbps FC Card		
13	Power Supply	Redundant Hot plug Power Supplies, platinum grade or higher		
14	Fans	Hot plug fans as per OEM server requirement		
15	Power & temperature	Should support real-time power graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing		
16	Pre-failure alert	Should provide agent-free predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, HDD		
17	Server Management	1. Real-time power meter, temperature monitoring, customized exhaust temperature and System Airflow Consumption		
18		2. Silicon root of trust, authenticated BIOS, signed firmware updates and BIOS Live Scanning for malicious firmware		
19		3. Telemetry Streaming		
20		4. Idle Server Detection		
21		5. Power control, Boot control		
22		6. The management software should collect system information (including impending component failure) from the device that generated the alert and should be able to send the information securely to OEM to Support to troubleshoot the issue and provide an appropriate solution.		
23		7. OEM's management software should be provided		
24		8. Firmware and configuration baselines for compliance monitoring and enable automated updates on schedule.		
25		9. Scope based access control to limit Users to specific group of devices		
26		10. Bare-metal server deployment		
27	Server security	Should have a cyber-resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks		
28		Should provide effective protection, reliable detection & rapid recovery using:		
29		Silicon-based Immutable Hardware Root of Trust		
30		Signed cryptographic firmware updates		
31		Dynamic USB Port Management		
32		Secure default passwords		
33		Shall provide dynamic system lock down server to prevent malicious attacks against embedded firmware and configuration drift in your datacenter without need to reboot the server.		

34		Persistent event logging including user activity		
35		Secure alerting		
36		Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted (either due to a malicious attack, or due to a power loss during the update process,or due to any other unforeseen event).		
37		Shall support boot from SAN and OS Recovery In the event of a corrupted OS image		
38		Support Secure System Erase to erase sensitive data and settings from the server storage devices and server non-volatile stores such as caches and logs so that no confidential information unintentionally leaks		
39		Configuration upgrades should be only with cryptographically signed firmware and software		
40		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware		
41	Intrusion alert	Intrusion alert in case chassis cover being opened		
42	Warranty and Support	5 Years, 24*7 support with 4 Hour On-site response with 6 Hr CTR support"		

NOTE	It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed GPU server offered as part of the solution.
------	--

SAN Switch

In case the model (Switch/Port Count/Port speed) is different for different environments, compliance is to be provided for each make/model separately

Make of the SAN Switch				
Model of the SAN Switch				
S.No.	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Vendor's Remarks
1	The switch should have non-blocking architecture with all ports active with 32 G SFP+ modules , switch should also support 64G transceiver for future upgrades.			
2	The switch should be configured with base 24 port (minimum) and can be upgraded to 48 ports with port-on - demand licenses activation			
3	The switch should support auto-sensing 64,32,16, 8 Gbit/sec FC capabilities.			
4	The switch shall support different port types such as D_Port (ClearLink Diagnostic Port), E_Port, EX_Port, F_Port, optional port-type control Brocade Access Gateway mode: F_Port and NPIV-enabled N_Port			
5	The switch must provide a maximum Aggregate bandwidth of 4Tbps (data rate) end to end or more			
6	Non disruptive Microcode/ firmware Upgrades and hot code activation.			
7	The Switch must provide autonomous Congestion control mechanisms without user intervention			
8	The Switch must be able to automatically quarantine and unquarantine slow-devices			
9	The Switch must provide Virtual Machine (VMID) support for end-to-end SAN telemetry			
10	The switch should support Frame-based trunking with up to eight SFP+ ports per ISL trunk; up to 512Gb/s per ISL trunk			
11	The Switch must support POST and online/offline diagnostics, including RASttrace logging, environmental monitoring, non-disruptive daemon restart, FCping andPathinfo (FC traceroute), port mirroring (SPAN port).			
12	The Switch must support web based management and also support CLI.			
13	The switch must support 24K frame buffers			
14	The Switch must support SAN Analytics with parallel SCSI and NVMe-FC analytics			
15	Should provide redundant and hot pluggable components.			
16	The switch should support Front to back and back to Front airflow			
17	The switch should be 1U form factor and rack mountable in a standard Rack			
	EXPERIENCE			
18	The proposed make of the SAN Switch should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI			

Backup Solution
In case the model (Switch/Port Count/Port speed) is different for different environments, compliance is to be provided for each make/model separately

Make of the Backup solution				
Model of the Backup solution				
S.No.	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
1	Proposed backup software must support backup, recovery, Long term archival and restoration from single GUI / console/unified management.			
2	The backup soolution must provide MFA integration to ensure additional security measure against compromise for local admin and AD users.			
3	The proposed backup solution must support efficient, source-side deduplicated data movement. The backup master servers and the media servers must be provided in high availability configuration ensuring no single point of failure.			
4	The data protection platform must provide online, application-consistent protection for databases (Oracle, SAP HANA, Microsoft SQL Server, MongoDB, etc.) using native or online agents to enable fast, granular restores across a broad range of supported Windows, Linux, and Unix OS. It should also deliver image-level protection for virtualized environments including VMware, Microsoft Hyper-V, Nutanix AHV, OpenShift, and additionally offer Kubernetes backup and recovery – all managed through a single, unified UI console.			
5	Proposed backup software must support Multi-Tenancy feature.			
6	Should be able to integrate with native backup interfaces of Hyper Converged Solutions in future agentless and/or image level backup of VMs			
7	Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NFS/S3 protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1.			
8	The proposed backup solution must support provide Data protection, Replication, Encryption, Immutability, MFA (Multi-factor authentication) and archival to external NFS/S3 based storage from day 1 and all these licenses must be included.			

9	The Proposed solution should ensure Data Protection & Archival: a) Backup and Recovery: Protects data by creating secure backups and enables fast recovery in case of failures or cyber incidents. b) Data Immutability & Encryption: Ensures that sensitive data is protected both in transit and at rest using strong encryption methods. (Backup software managed but applies on Backup Storage - WORM capability). The proposed solution and its backup appliance must provide immutable backup storage via WORM (Write Once, Read Many) or a retention-lock capability. Immutability must be backup-software-aware and integrated with the storage layer through a secure protocol and/or native API. It must be enforced automatically at the policy level — not manually configured — and propagated down to storage. The backup software and storage must operate as a single integrated system, not in silos. c) Data Integrity and Availability: Ensures that data remains intact and available for recovery in case of an outage, system failure, or cyberattack. d) Archival: Reduces the cost of storing inactive or less frequently accessed data. e) Compliance and Legal Hold: Ensures that data is retained for the necessary period as required by regulatory bodies and the organization's internal policies. f) Search and Retrieval: Enables fast and efficient retrieval of archived data, ensuring that critical information can be accessed quickly when needed. g) Long Term Retention/Forever Retention: Covers a "No Loss of Data" policy using long-term retention. h) The proposed solution should have the ability to protect all mount paths associated with disk libraries configured from a Backup/Media Server against ransomware attacks, or provide equivalent ransomware protection for backup architectures that do not use conventional mount paths or Backup/Media Servers.			
10	The proposed backup software must be deployed in a high-availability (HA) configuration, encompassing all critical components — including media/proxy servers and the master/control server — to eliminate any single point of failure across the backup core infrastructure.			
11	The Backup software must be able to compress and encrypt data and should also suport de-duplication.			
12	Proposed backup solution should support archiving the long term retention copies of ALL the workloads like VMs, DB, Files, etc on <i>Long term Storage</i> using NFS/S3 protocols and required software licenses must be provided on day 1.			
13	Solution should provide historic backup & retrieval reports for success & failure Daily, Monthly & Quarterly or as per Bank requirement.			
14	The backup software should provide centralized management / Single interface for management of all backup and archival across applications and workloads deployed in on-premises and cloud environments			

15	The following backup and retention policy to ensure data protection, recoverability, and compliance with long-term retention needs is complied: • Daily Incremental Backup – retained for 2 weeks in disk-based appliance/backup storage • Weekly Full Backup for all data types – Retained for 4 weeks in disk-based appliance/backup storage • Monthly Full Backups – Retained for 2 Months in the same appliance/backup storage *After the 2-month period, Monthly Full backups must be migrated to long-term backup storage, where they shall be retained for the entire duration of the contract. Backup Appliance / Backup Storage Requirements * Online Backup Storage/Appliance must retain backups for a minimum period of 2 months, with each Monthly backup being preserved during this duration. * All monthly backups taken during the contract period must also be stored on long-term storage for the entire duration of the contract. *All the data, logs, information & others must be backed up using the proposed backup and retrieval solution, in accordance with the defined backup policy and retention requirements. *Regularly test and verify the integrity of backed-up data and information by performing retrieval exercises. This process should be completed prior to overwriting or replacing any previously taken backups, to ensure that the data is recoverable, intact, and usable when required.			
16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to-disk (D2D) connection.			
17	Proposed backup solution must support software based de-duplication and shall be capable of taking backup of data and workloads (irrespective of the underlying storage OEM) and the solution shall support deduplicated backup copies for long-term retention. Based on policy backup software should be able to move deduplicated backup copy to a Long term storage automatically. The proposed backup solution shall support deduplicated backup targets across leading OEM storage systems and shall not be restricted on any specific OEM/vendor.			
18	Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power , fans etc. and Backup Appliance - Power , fans etc.) , HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.			
19	Proposed Disk Based backup appliance should have the ability to perform different backup, restore, replication jobs simultaneously and must support communications and data transfers through 10/25 Gb ethernet LAN over SFP+. The proposed backup appliance should be offered with minimum 4 x 10/25 Gbps NIC SFP+ or Proposed Disk Based backup storage should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 32 GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The Proposed Backup Storage should have should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity.			

20	The proposed appliance/backup storage must ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and required documentation from the OEM is to be submitted along with the proposal.			
21	Proposed Appliance/Backup Storage should support different retentions for primary and DR backup storage and should support instant copy creation on remote site for better DR readiness with support for transmitting only deduplicated unique data in encrypted format to remote sites.			
22	The proposed backup Solution must support immutability, retention lock or equivalent feature which ensures that no data is deleted accidentally.			
23	Proposed Appliance/Backup Storage should support bi-directional, many-to-one, one-to-many, and one-to-one replication.			
24	Proposed Appliance/Backup Storage should support 256 bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption.			
25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism			
26	All file system data and Metadata must be verified continuously even if parts of the file system are never accessed for reads (Automated Data Scrubbing Process)			
27	Any modification or new data must not modify existing data blocks to prevent possibility of corruption. Any new or modified content must be written to new blocks			
28	The appliance/storage should be configured with all the licenses backup and replication necessary for the sought functionalities.			
29	The proposed solution shall ensure that backup expiry/immutability cannot be bypassed by any internal or external change to system time, whether by restricting time changes or by an immutability mechanism that is independent of the system clock.			
30	Proposed Appliance/Backup Storage must offer with feasibility to protect data from accidental deletion			
31	Regular Maintenance activities like Systems Housekeeping/Garbage Cleaning etc should be able to happen simultaneously along with regular backup and restore operations without having the need for a dedicated window			
32	Proposed backup appliance/storage should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user.			
33	The solution should provide data validation features to ensure data integrity by validating data integrity during backup, when data is at rest and during data copy operations.			
34	Backup is to be performed at both DC and DR. The Proposed solution must have Disk to Disk to Long term Storage (D-D-LTS) Backup solution with backup data to be kept on disk for easy retrieval.			
35	Backup & retrieval software, Backup Appliance or Integrated appliance is to be proposed at both DC & DR with all requisite licenses for both the sites separately.			
36	Product should offered with 24x7- 5 years (Contract period, whichever is later) onsite warranty support.			
37	Backup software should be able to replicate backed up data in de-duplicated format (for bandwidth optimization) to another site for compliance purposes, without the need of external replication tools. All necessary licenses for achieving consistent replication of backup data should be quoted.			

38	The proposed backup solution must natively support a LAN-Free architecture for all image-level VM backups to prevent performance degradation on production networks. All raw backup data payloads must stream directly from production storage to the backup appliance/storage over a dedicated Storage Area Network (SAN/Fibre Channel/iSCSI) or dedicated storage fabric. Production Ethernet/LAN infrastructure must be completely bypassed, restricting its use strictly to minor control traffic and metadata orchestration.			
39	The proposed backup software must have the capability to integrate with snapshot based backup for data residing on popular storage devices from NetApp / Dell-EMC / Pure etc.			
40	Backup storage/Appliance capacity expansion - whether by adding disks, adding an enclosure, or adding scale-out nodes - must be non-disruptive, and no additional storage-side licence shall be required to consume the expanded capacity where the backup software"s protected-capacity licence already covers the data being protected.'			
41	The proposed solution should provide the High Availability with failover/failback capabilities for the Backup Management server without the need of clustering at OS level and any additional license requirements.			
42	Comprehensive reporting of media, backup server, jobs, analytics should be offered as part of the functionality in the supplied software either natively or through additional reporting software.			
	EXPERIENCE			
43	The proposed make and category of the backup solution & appliance should have been implemented in at least 2 scheduled commercial bank with 1500 branches.			

NOTE	It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed Backup Solution and Backup Appliance/Storage offered as part of the solution.
------	--

Long Term Storage

In case the model is different for different environments, compliance is to be provided for each make/model separately

Make of the Long Term Storage				
Model of Long Term Storage				
S.No.	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
1	Proposed storage would be proposed for long retention of Backup data (Protocol- NAS/CIFS/SMB/S3/SAN storage (Protocol- iSCSI)			
2	Bank is looking for Long term storage for the duration of the Contract. Bidder to design and propose the solution for storing the backups for the druation of the contract with adequate interfaces for perofmring the backup & retrieval within the defined period and as per the terms of the RFP. Interface should be design to ensure that Data / logs/Informations are in the proposed storage after the duration mentioned in the RFP. The Backed up data / logs need to be restored in the respective technology for forensic and other requiriement of the bank etc.			
3	Bank is looking for Long term storage for the duration of the Contract. Bidder to design and propose the solution for storing the backups for the druation of the contract with adequate RAID. Proposed Sizing should be proposed on RAID 6			
4	• Bidder is required to propose the long-term backup storage at both the Data Centre (DC) and Disaster Recovery (DR) sites and must adequately sized the storage to retain backup data for the entire duration of the contract. • The sizing should account for data growth, retention policies, and restore requirements, ensuring reliable and compliant backup management throughout the contract period.			
EXPERIENCE				
5	The proposed make and category of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches			

NOTE

It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed Long Term Storage offered as part of the solution.

Load Balancer			
In case the model is different for different environments, compliance is to be provided for each make/model separately			

Make of the Load Balancer			
Model of the Load Balancer			

S.No.	Minimum Technical Specification	Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
1	The proposed solution should be a dedicated appliance as ADC not as add on license Feature on NGFW and WAF.			
2	The Appliance should have dedicated 1x1GbE port for management and 4x10GbE SFP+ ports and multicore CPU, minimum 4 TB HDD and dual power supply.			
3	The SLB OEM should support 7K SSL TPS for RSA 2K key, 10K SSL TPS for ECDSA P25			
4	The appliance should have dedicated SSL Acceleration hardware card for handling SSL Traffic. The SSL traffic should not be process by CPU of the appliance			
5	The solution should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.			
6	The solution should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie or equivalent, shortest response, proximity, SNMP, SIP session ID etc.			
7	The solution should support Multi-level virtual service policy routing ,-Static, default and backup policies for intelligent traffic distribution to backend servers			
8	The solution should support for policy nesting at layer 7 and layer 4. it should able to combine layer4 and layer7 policies to address the complex application integration.			
9	The solution should have script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. It should support ePolicies or equivalent to customize new features/rules to re-direct the traffic on specific parameters.			
10	The solution using e-policy or equivalent then should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash IP and snmp			
11	The solution should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.			
12	The Solution should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.			
13	The solution should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers			
14	The solution should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..			
15	The proposed load balancing solution should support a license upgrade mechanism that allows for the enablement of additional features on the same physical or virtual appliance, without requiring hardware replacement. Where applicable, the solution should be capable of integrating with or supporting secure machine-based authentication mechanisms for access to corporate resources.			
16	The solution should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048,4096 bit keys for encrypted application access.			
17	The solution must support Single Sign-On (SSO) for web based applications and web based file server access. It should also supports SAML secure application access			
18	The solution should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed TCP optimization option configuration should be defined on per virtual service basis not globally.			

19	The solution should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. It should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".			
20	The solution should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.			
21	The solution should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.			
22	The solution should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.			
23	Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application.			
24	The solution should support site selection feature to provide global load balancing features for disaster recovery and site redundancy.			
25	It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.			
26	The solution should provide comprehensive and reliable support for high availability and N+1 clustering based standard VRRP RFC 2338 or equivalent on Per VIP based Active-active & active standby unit redundancy mode.			
27	the solution should support Stateful session failover with N+1 clustering support when deployed in HA mode.			
28	The solution should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speedup the failover. It should support for secondary communication link for backup purpose			
29	The solution should support floating IP address and group for stateful failover support. It should support built in failover decision/health check conditions including, CPU overheated, system memory, process health check, unit failover, group failover and reboot			
30	The solution should also have option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway			
31	The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.			
32	The solution should support XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should provide detailed logs and graphs for real time and time based statistics			
33	The appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback. The system should support led warning and system log alert for failure of any of the power and CPU issues			
34	OEM should have TAC & R&D facility in INDIA. The proposed solution should be up and running in PSU/PSE/Govt. Organization within the last 5 years			