CORRIGENDUM-5

Ref: CO/IT-DT/BACKUP_UPGRADE_RFP_Corrigendum_5   **Date: 23.04.2025**
Request for Proposal for the procurement of Backup solution for ODS project
Reference: LIC/CO/IT-DT/ODS/Backup solution/2025/01 dated: 21.03.2025.

The following corrections are made in Annexure –XII
Backup Appliance/Storage technical specifications
 Software Features and Backup Services requirements
 Point 12 – "The storage system must support Object protocol, Open Stack Swift– compatible object ingest over HTTP or HTTPS" has been deleted. Please refer to corrigendum – 3 Point 12
 The requirement - **The storage system must support block level protocol like iSCSI, FC.** – is retained (under Backup Appliance/Storage technical specifications d) (Software Features and Backup Services requirements Point-12)

The final revised Annexure-XII is appended below:

1. **Revised Annexure-XII (to be submitted along with Eligibility & Technical Bid)**

Annexure – XII: Technical Requirements for RFP for procurement of Backup solution for ODS project of LIC of India

RFP Ref: LIC/CO/IT-DT/ODS/Backup solution/2025/01 dated: 21.03.2025

1. **Backup Appliance/Storage technical specifications**
        a) **General Features:**

S. No.	Technical Specification	Whether complied (Y/N)
1	The proposed Backup Appliance/Storage for each site should be capable of being directly mounted (at each sites) as a partition on Exadata server by directly connecting Backup Appliance/Storage to Exadata Primary Database servers (Exadata X7-2servers) and Standby Database Servers(Exadata X9M-2 HC servers) **through point-to-point optical fiber network" Or**	

"QSFP28 Copper cables without connecting thru current Dell unified switch (Please see proposed network connection diagram under schedule-3) **Alternatively**, the bidder may propose connectivity through a **dedicated high-speed compatible LAN switch between Exadata servers and Backup Appliance/Storage** , provided the following additional conditions are met: • Backup speed of 10 TB /hour is achieved. • All the proposed backup solution hardware components including proposed switches fits within less than 24U Rack space and within the power requirements specified in Corrigendum-1 page-17 clause-9	
2	It should be possible for other Databases on Exadata server X5-2 server VMs at primary site (like UAT Database servers and SMS database) and other independent databases like catalog databases at both sites, to be backed up through RMAN interfaced with proposed Backup software to Backup/storage appliance**(Please see proposed network connection diagram under schedule-3)**	
3	Proposed backup appliance/storage should have redundant components/HA mechanism in place to avoid single point of failure .	
4	Proposed backup appliance/storage should have scalability with respect capacity expansion and proportional cache in future.	
5	It should be possible to configure and schedule backups of backup sets from Backup Appliance to LTO tapes	
6	It should be possible to configure and schedule flat file backups from Staging servers to Backup Appliance to LTO tapes as well as directly from Staging servers to LTO tapes	
7	The storage system should be based on industry standard components.	
8	The storage system must have an easy-to-use web-based graphical interface (GUI), command line interface (CLI) as well as Restful cloud API to simplify administration.	
9	The storage system should provide hybrid storage architecture - combining Read and/or Write	

	Flash Accelerators (SSDs) with SAS-3 HDD.	
10	The storage system should provide auto-tiering to optimize workloads effectively and cost-efficiently.	
11	The storage system must be able to provide optimized storage caching hierarchy with hybrid storage pools containing DRAM, SSD and SAS-3 hard disk drives.	
12	The storage system should transparently execute writes to a pool of low latency SSD media so that writes can be quickly acknowledged and automatically flush the data to SAS-3 drives as a background task.	
13	The underlying disk storage manager should automatically recognize different I/O patterns and place data in the best storage media for optimal performance.	
14	The storage system can fully utilize the entire DRAM for IO activity by using technologies Adaptive I/O Staging.	
15	The storage system should have a hybrid storage capacity scaling capabilities to add SSD or combination of SSD and HDDs with 24 disk drive enclosures.	
16	The storage system should be available as both an on-premises appliance and a cloud image that can be installed on a compute instance to provide storage in cloud environment with up to 1PB of Automated capacity.	
17	The storage system should be able to provide read and write cache for I/O enhancement with the help of built in software, without any additional costs.	
18	The proposed Storage system should be compatible with Oracle Exadata systems	

b) **Reliability, Availability and Serviceability**

S. No.	Technical Specification	Whether complied (Y/N)
1	The storage system must provide predictive self-healing and diagnosis of all system FRUs: CPUs, DRAM, I/O cards, disks, fans and power supplies.	
2	The storage system should also support a two-node active-active cluster configuration, with no single point of failure.	
3	The storage systems clustering feature should have the ability to synchronize administrative configuration and also the ability to fail over storage and network resources.	
4	The storage system must help administrators to quickly diagnose and resolve performance issues in production systems, using revolutionary business analytics functionality that delivers real-time Visibility throughout the data path.	
5	The storage system should support Link Aggregation Control Protocol (LACP), to bundle multiple network devices to behave as one.	
6	The storage system must make provisioning and management, that is dramatically simplified for system installation, configuration and tuning.	
7	The storage system should possess self-healing capabilities to automatically and silently detect and diagnose underlying system problems and automatically respond by taking faulty components	

S. No.	Technical Specification	
	offline.	
8	The storage system must not have battery to reduce maintenance task and increase system reliability.	
9	The system should be able to upgrade important components firmware to maintain high reliability.	

c) **Scalability and Connectivity**

S. No.	Technical Specification	Whether complied (Y/N)
1	The storage system must be highly scalable to support rapid growth in storage capacity.	
2	The storage system must support scalability in multiple dimensions with ability to scale I/O throughput with multiple network type support, read and write optimization and total storage capacity to meet Application needs.	
3	The storage system should provide at least 24 CPU cores and 1 TB DRAM per controller	
4	The storage system should be able to support scaling by adding enclosures or disk trays.	

5	The storage system must support 22 TB or higher capacity SAS-3 hard disk drive. or The bidder can propose a Backup appliance/storage using <u>only latest technology high-performance SSD drives that delivers:</u> • At least 340 TB usable capacity under **RAID 1+0**. • Fit all SSD disks within a maximum of 2 enclosures (due to Rack space constraint). • Fit the entire Backup solution hardware components in a Rack space of less than 24U and within power requirements specified (as already mentioned in Corrigendum-1, Page-17 Clause -9) • And is offered at a comparable and competitive price point.	
6	The storage system should support 7.68 TB or higher SSD.	
7	The storage system should be mountable on existing non-Exadata racks at Primary site and at DR site. The entire backup solution hardware including Backup Appliance, Media servers, Tape Library should fit in within available rack space of 24 U.	
8	The storage system should support at least 20 10Gb/25Gb/40Gb/100Gb Ethernet (twinax/optical) ports	
9	The storage system should be able to seamlessly connect to Exadata X5 and X7 with 10Gb/40Gb Ethernet (twinax/optical) ports.	
10	The storage system should be able to seamlessly connect to Exadata X9	

	with 25Gb/100Gb Ethernet (twinax/optical) ports.	
11	The storage system must have redundant HBA cards for tape backup (each 16Gb/32Gb dual-port FC HBA).	

d) Software Features and Backup Services requirements

S. No.	Technical Specification	Whether complied(Y/N)
1	The storage system should be able to backup Transparent Data Encrypted enabled database's backup of Oracle Databases using Oracle RMAN backup.	
2	The storage system should be able to fully restore backup without any corruption or inconvenience.	
3	The storage system should be able send TDE enabled and Hybrid Columnar compressed database backups to tape library.	
4	All required backup software's required for backup to storage system and sending it to tape library to be included. Tape library with at least 9 disk drives to be considered.	
5	All basic software features, for example file / block protocols and data services such as thin provisioning, de-duplication, compression, snapshot should be included free of charge.	

6	The storage system should support metadata device or DDT SSD to store the data de-duplication table for maximum de-duplication performance.	
7	The storage system must support Hybrid Columnar Compression technology which enables end-to-end data reduction for Oracle Database.	
8	The storage system much support data reduction technology with minimal performance impact at storage level such as data compression and inline data de-duplication.	
9	The storage system must support Oracle Intelligent Storage Protocol which enables better integration to Oracle DB (automatic tuning).	
10	Must provide seamless multi-protocol integration and secure data sharing between Microsoft Windows and UNIX/LINUX clients.	
11	The storage system must support file level protocols, like NFSv2, NFSv3, NFSv4, NFSv4.1, SMB1/2/2.1/3, HTTP, FTP, SFTP, FTPS.	
12	The storage system must support block level protocol like iSCSI, FC	
13	The storage system must support directory services like NIS, AD and LDAP.	
14	The storage system must support network services NTP, DHCP and SMTP.	
15	The storage system support replication on-disk compressed data as is over the write, node compression/recompression when doing replication.	

16	The storage system must have QOS feature such as File System & LUN I/O throttling.	
17	The storage system should support mix of resource pool such as flash pool, disk pool.	
18	The storage system should support direct communication between storage system and Oracle database by reducing latency and improves I/O performance for Oracle workload.	
19	The storage system should support a minimum of 10x compression of static Database data, resulting in a minimum of 3x reduction in storage footprint for data warehousing and long-term storage of information in Oracle Database.	
20	The storage should support data retention policy on Oracle Cloud Infrastructure object, snapshot, and share/file retention policies for legal hold, data governance, or regulatory compliance.	

e) Monitoring, Notification and Management

S. No.	Technical Specification	Whether complied (Y/N)
1	The storage system must provide real-time analysis and monitoring functionality, at almost no performance impact to the running production applications.	

2	The storage system must provide monitoring storage analytics and dashboard monitoring for key system performance metrics	
3	The storage system should provide automated serviceability using Call Home feature.	
4	The storage system should support front-accessible and hot-swappable disk drives.	
5	The storage system should support iSNS or an equivalent capability, such as an integrated management interface and APIs designed for modern data protection workflows.	
6	The storage system must support remote management via HTTPS, SSH, SNMP v1/v2c/v3, IPMI, S3, RESTful API, Open Stack Cinder.	
7	The storage system should support Role-Based Access Control (RBAC) and end-to-end integrity measures to enforces granular control over access privileges.	
8	The storage system must provide or support a single management console to manage both cloud and on-prem environments that allows administrators to manage their Storage resources in the cloud along with their on-premises resources, providing a unified management platform for distributed cloud environments.	

f) Data Protection Features

S. No.	Technical Specification	Whether complied (Y/N)
1	The storage system must provide data security through checksum data and metadata.	
2	The storage system must support RAID0 (Striping), RAID1 (2 and 3 ways mirroring), Single parity RAID, Double parity RAID and Triple parity RAID.	
3	The storage system must support mix RAID level/pools in the same system.	
4	The proposed storage system must support both IP-level and I/O-level multipathing for high availability and fault tolerance. Network Multipathing: The storage system must provide IP-level redundancy using industrystandard techniques such as IPMP (for Solarisbased systems), NIC bonding, teaming, or LACP (IEEE 802.3ad) for non-Solaris platforms. This ensures continued network availability in the event of a network interface or path failure. I/O Multipathing to Disk Arrays: The storage system must support multipathing for storage I/O connectivity to ensure failover and load balancing across multiple data paths. Support for standard multipathing frameworks (e.g., Linux DM-Multipath, Windows MPIO, or equivalent) is required where applicable.	
5	The storage system should support all the types of replication of data	

	for disaster recovery,1-to-1, 1 to many, many to 1 and bi-directional.	
6	The storage system should support duplicated replication, to only send unique data blocks over in order to reduce the data sent over the wire.	
7	The storage system should support resumable replication. In case of network or other failure, replication should resume at the point it left off, when failure happened.	
8	The storage system should support independent retention policies for auto-generated snapshots on

Source and target. | |
9	The storage system should support ability to control the replication bandwidth.	
10	The storage system must support to track and monitor individual-file level activities, ensuring compliance with data security and privacy regulations.	
11	The storage system must support provide a point-in-time view of the file system. These snapshots cannot be modified.	
12	The storage system must support and enables seamless integration between the on-premises storage and cloud object storage. It allows users to interact with and manage objects stored in cloud object storage directly from the on-premises storage environment, facilitating data movement and synchronization between on-premises and cloud storage.	

g) **Other Features**

S. No.	Technical Specification	Whether complied (Y/N)
1	The storage system should support virus scanning and quarantine capabilities. At least should support popular anti-virus software like Symantec, McAfee, CA etc.	
2	The storage system should support backup software integration, like Veritas Net Backup,Commvault.	
3	Storage Capacity 340 TB Usable RAID(1/0) Or Mirror	

2. **Backup software specifications**

Generic Mandatory Specifications	Compliance (Yes/No)
1.Analyst Rating	
The Backup software proposed should be in Gartner's leader quadrant of Magic Quadrant report of any last 5 years for Data protection/Backup software.	
2. Backup and Recovery for Oracle Database and Flat Files:	
Backup software should support disk to disk and disk to tape backups at the same time	

Proposed appliance should have the ability to perform different backups, restore simultaneously	
The backup software must support Oracle RMAN for all Oracle database backups.(disk to appliance). Backup Software should be interfaced with oracle RMAN to take backups of UAT, PRSMS, Catalog database, OEM database at each sites	
The backup software should be capable of performing the backup of backup sets from Disk/Appliance to LTO tapes backups.	
The backup software should allow seamless integration with RMAN scripts. Proposed backup software should support seamless interfacing with Oracle RMAN utility backup features for RMAN Backups and backup restoration	
The backup software must support backup for flat files from staging servers at both locations.	
3. Primary and Standby Database Architecture:	
The backup software must support Oracle Data Guard replication for primary and standby databases.	
Backup should be executed through direct Optical Fiber connections between Exadata servers and storage appliances (disk-to-disk).	
4. Backup Server and Storage Architecture:	
Backup software must support backup from staging servers (disk-to-disk) and server-to-tape backup.	

The backup software should be able to move backup data from backup appliance to tape storage devices.	
5. Retention Policies and Backup Management:	
RMAN retention policies should take precedence over backup software policies.	
The backup software should support configuration for RMAN retention policies (e.g., recovery window, redundancy) to override the retention policies of backup software	
RMAN maintenance commands such as cross-check and delete obsolete must work seamlessly with the backup software.	
Maintenance tasks like cross-check and delete obsolete should be scheduled and configured within the backup software.	
6. System Compatibility and Resource Efficiency:	
The backup software must be compatible with Oracle Exadata (X5-2, X7-2, X9M-2). Proposed Backup software shall be compatible and certified to work on Exadata X5-2, X9-2 and X9M-2 systems. The software should be certified by respective Backup software OEMs to work on Oracle Exadata systems	
The backup software must not introduce performance issues (e.g., excessive CPU or memory usage) on Exadata systems.	
The backup software must be compatible with Oracle Enterprise Linux 8 and above	

The backup software must support Oracle Exadata RAC configurations and ensure RMAN backups are distributed across RAC nodes.	
The Backup software /agents/plugins should be compatible with latest version of Operating system Oracle Enterprise Linux.	
The Backup software /agents/plugins should be compatible with Oracle database version 19C and above.	
7. Performance and Efficiency:	
A backup speed of 10 TB / hour should be achieved . (Please refer to Section B, Clause 6 – SLA requirements on Backup performance requirements	
The Media Management Layer (MML) of the backup software should be optimized to minimize CPU and memory usage, avoiding database waits/MML waits.	
Proposed backup software should be able to de-duplicate data across backup and backup data sets to reduce storage footprint (using software based de-duplication)	
The backup software must provide efficient deduplication and compression to optimize storage and minimize backup window.	
8. Data Encryption and Security:	
The backup software must support Transparent Data Encryption (TDE) for Oracle databases.	

The backup software must support Hybrid Columnar Compression (HCC) technology for Exadata, ensuring high deduplication and compression ratios.	
The backup software should support **role-based access control (RBAC)** with audit logging to track all administrative activities.	
The solution must support **integration with multi-factor authentication (MFA)** for administrator access.	
The backup software should support **secure API integrations** with existing security monitoring solutions (SIEM, SOC).	
9. Backup to Virtual Tape Library (VTL):	
The backup software must support Virtual Tape Libraries (VTL) for both disk-to-disk backups and restorations.	
Proposed Backup software shall support Virtual Tape Library for backups to disk as well as for restorations.	
10. Vendor Support and Compliance:	
The bidder shall have back-to-back arrangement with Oracle for configuring direct point-to-point connections / connections through LAN switch from Exadata servers to the backup appliance.	
11. Ease of Use and Management:	

The backup software must provide a centralized management interface to schedule, monitor, and report on backup activities.	
The software should allow scheduling of backups using RMAN scripts and provide detailed reports on backup success/failure.	
12. Scalability and Future Proofing:	
The backup software should be scalable to accommodate future data growth and additional Exadata hardware.	
The solution should be flexible enough to accommodate future versions of Exadata hardware and features.	
13. Backup Software- Other Specifications	
24x7 OEM support should be included. This should include upgrades, updates, patches, bug-fixes etc.	
The proposed Integrated solution (Backup Software and De-Dupe Appliance) must be provided by a single Bidder to ensure ownership of design and support. It must be with the respective OEM support and must be implemented by Single Bidder.	
The bidder must include all the necessary hardware including servers, backup software, De-Dupe Storage etc as a part of the proposed solution. The Hardware must be sized to be able to handle the backup/restore operations mentioned in the RFP.	

Must be provided with perpetual licenses for unlimited number of hosts and must be configured with 75 TB of Front End capacity based license at both sites with 5 years AMC support.	
Proposed backup software must have backup server compatible to run on both Windows and Linux OS platforms. It should offer a single Console to manage entire backup operations across the platforms from single window across sites (DC and DR)	
Must have Agent/Modules for online backup of applications and databases such as Oracle Exadata DB. It should support online backup of databases such MSSQL, Exchange, DB2, Informix, Sybase, SharePoint, and SAP, SAP HANA etc.	
Proposed Backup Software should use the Auto discover applications option to automatically find Oracle databases in the environment and install software to back up the Oracle database.	
The Proposed Backup Software should protect Oracle Data Guard instances. Role-based backups are executed on the primary and standby sites for data and log files.	

The Proposed backup software should protect databases that have Hybrid Columnar Compression (HCC) enabled.	
The proposed backup software should backup and restore Oracle databases that uses Transparent Data Encryption (TDE) or Tablespace Encryption (TSE)	
The backup solution must support online LAN free (SAN based) backup of all physical servers and databases through appropriate agents. The backup data must flow directly from client to backup appliance for both LAN & SAN connected clients	
Proposed Backup Software must support Data based Backup and restore including the parameters which are supported on the RMAN command line to back up or restore files such as control files, parameter files (SP files), and individual data files.	
The Proposed backup software must support backup and restore operations in an Oracle Data Guard environment, for both single-instance Oracle databases and Oracle RAC databases.	

The proposed software should support block-level and flat-file backup with incremental/synthetic full backup cycles, full VM recovery, bare metal recovery for Windows/Linux, granular file-level restore, DB restore, and Instant VM recovery.	
The proposed backup solution should provide a mechanism to validate the consistency of the backup image before restoring the data to ensure only consistent data is getting restored.	
The proposed software should have a security dashboard with cyber security solution that includes: (a) Machine-learning-based prevention mechanism to prevent against cyber threats. (b) Behaviour analysis for ransomware detection and protection with encryption rollback. (c) Ransomware protection and Malware detection functionality (d) Alert mechanism in the event of detection of any anomaly	
Proposed solution should have Cyber Resilience capabilities to protect data from ransomware, malware or any other threat discovered from time to time. Solution should provide capability to scan backup data for any file anomalies or malware infection.	

Proposed Integrated Solution must support backup and restore of physical as well as virtual environments such as HyperV, VMware, AHV, Citrix XEN, KVM, Oracle VM, Kubernates etc. with agentless / image backup	
The propose integrated solution must protect Oracle Linux virtual machines at the image level and support CBT (Change Block Tracking) based backups and CBT restores. The solution must not require dedicated physical proxy servers to perform image level backup.	
Must provide support to restore a single VM, single file from a virtualized environment. It must provide restore from the backup server management console for ease of use and centralzied administration	
Must not need a physical proxy to perform backup and recovery of vmware virutal environment. A single proxy must be able to perform minimum 20 concurrent streams with source deduplication	
The Proposed backup solution must support the Client side data de-duplication for the File System, Applications and Databases.	
Must be able to dynamically break up large backup sets to be backed up in parallel to allow backups to complete faster for Windows, Unix and Linux	

clients.	
Proposed disk based backup appliance should be able to interface with various industry leading server platforms operating systems and Must support LAN/SAN based D2D backup simultaneously via NFS v3, CIFS, FC , OST and NDMP protocols.	
The backup software must have in-built calendar based scheduling system and must support the ability to configure retries of client in case of backup failure	
It must support various level of backups including full, incremental, differential, synthetic and virtual synthetic backup methodology.	
Must support NAS and storage array based snapshot backup for off host zero downtime and zero load on the primary backup client.	
The integrated solution must allow setting up of different retention policies for backed up data at primary site and the replicated site.	

The integrated solution must provide single Graphical User Interface for backup, restore and management. The single GUI interface must provide management of backup software, disk based backup appliance	
Must have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Integrated Backup Solution /Clients, Virtual Environment, Replication etc.	
The solution must be able to recreate backup catalog from data on existing volumes. Additionally in case of disaster or server crash, the backup solution must be able to restore the complete backup server configuration and catalog in timely manner	
Must be capable of integration with active directory infrastructure for ease of user rights management along with role based access control to regulate the level of management	

3.   Media Server specifications

Description of Requirement	Compliance (Yes/No)

Chassis	
2U Rack Mountable	
CPU	
2 x Intel Xeon 4th or 5th Generation Silver/Gold/Platinum processor with 16 core, 2.5Ghz, 37.5Mb cache	
Chipset	
Latest Chipset	
Memory	
1TB RAM and expandable up to 2TB	
HDD Bay	
4 x 7.68TB NVMe drive	
Controller	
Embedded / PCIe based RAID controller with 8GB Flash backed write cache supporting RAID 0, 1, 5, 6, 10, 50, 60 Must support mix-and-match SAS, SATA, and NVMe drives to the same controller.	
PCIe Ports	
Supporting 8xPCIe5.0 slots	

Network Ports	
2 x Dual Port 10Gig Network Adapter with 10Gig Transceivers 2 x Dual Port 32Gig FC HBA Card	
Interfaces	
USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port	
Power Supply	
Hot plug redundant Power Supply with minimum 1600W	
Fans	
Redundant hot-plug system fans	
Industry Standard Compliance	
ACPI 6.3 Compliant	
PCIe 5.0 Compliant	
WOL Support	
Microsoft® Logo certifications	
PXE Support	
Energy Star	
SMBIOS 3.2	

UEFI 2.7	
Redfish API	
IPMI 2.0	
Secure Digital 4.0	
Advanced Encryption Standard (AES)	
Triple Data Encrytion Standard (3DES)	
SNMP v3	
TLS 1.2	
DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP)	
Active Directory v1.0	
ASHRAE A3/A4	
System Security	
UEFI Secure Boot and Secure Start support	
Tamper-free updates - components digitally signed and verified	
Immutable Silicon Root of Trust	
Ability to rollback firmware	
FIPS 140-2 validation	

Secure erase of NAND/User data	
Configurable for PCI DSS compliance	
TPM (Trusted Platform Module) 2.0 option	
Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser	
Bezel	
Bezel Locking Kit option	
Support for Commercial National Security Algorithms (CNSA)	
Chassis Intrusion detection kit	
Secure Recovery - recover critical firmware to known good state on detection of compromised firmware	
Operating Systems and Virtualization Software Support	
Windows Server. Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Oracle Linux and Oracle VM	
Provisioning	
1. Should support tool to provision server using RESTful API to discover and deploy servers at scale	

2. Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
Firmware security	
For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable	
Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	
Embedded Remote Management and firmware security	
System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication	
Server should have dedicated 1Gbps remote management port	
Server should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware	
Server should support agentless management using the out-of-band remote management port	

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	
Two factor Authentication	
Local or Directory-based user accounts with Role based access control	
Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support.Should provide support for AES and 3DES on browser.Should provide remote firmware update functionality.Should provide support for Java free graphical remote console.	
Should **support managing multiple servers as one via** • Group Firmware Update • Group Configuration • Group Virtual Media and Encrypted Virtual Media	
Should support RESTful API integration	
Server should have security dashboard, displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features.	
Server Management	
Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	

The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts	
The Systems Management software should provide Role-based access control	
Zero Touch Provisioning (ZTP) using SSDP with remote access	
Management software should support integration with popular virtualization platform management software like Vmware vCenter & vRealize Operations, and Microsoft System Center & Admin Center	
Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD and auto-creation of case ID	
Should provide an online portal that can be accesible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	

Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline	
The Server Management Software should be of the same brand as of the server supplier.	
Warranty	
5 Years 4 hr CTR 24x7 Support	

4. Tape Library specifications

Functionality	
Capacity	**Complied (Yes/No)**
1. Offered Tape Library shall support Native data capacity of 11PB (uncompressed) using LTO-9 Technology.	
2. Shall be offered with Minimum of nine LTO-9 FC tape drive. Drive shall support encryption	
3. Shall be offered with 40 Cartridge slots and shall be scalable to 640 slots.	
Tape Drive Architecture	
1. Offered LTO-9 drives in the Library shall conform to the Data rate matching technique for higher reliability.	

2. Tape Drive Architecture in the Library shall conform to the INCITS T10 standard ADI Protocol or newer standards.	
Scalability	
Tape Library shall be scalable to minimum of 48 number of LTO-9 drives	
Speed	
Offered LTO-9 drive shall support 400MB/sec in Native mode.	
Connectivity	
Offered Tape Library shall provide native FC connectivity to SAN switches. Maximum FC speed per drive should be 16Gbps FC to SAN Switches	
Partitioning	
Offered tape library shall have flexibility to configure each offered drive into a separate partition. Offered tape libray shall have support for 21 partition when fully populated. Vendor shall provide the license for same.	
Encryption device	
Offered Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the encrypted keys in a redundant fashion.	
Management	
Tape Library shall provide web based remote management.	
Barcode Reader and Mail slots	
Tape library shall support Barcode reader and mail slot.	

Tape Library shall be offered with 5 mail slots within the 40 cartridge slots.	
Every additional 40 Cartridge slots shall provide the flexibility to use 5 slots as mail slots.	
Other Features	
Tape Library shall have GUI Panel	
Shall be rack mountable.	
Shall have option for redundant power supply	
Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.	
Offered drives in the tape library shall optionally support both data path and control path failover.	
Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved.	

I hereby certify that the Backup solution proposed fulfills all Technical requirements

Dated at _____   this   day of _____   2025

Authorized Signatory (Name: Contact Person, Phone No., Fax, E-mail)

(This letter should be on the letterhead of the of the company by the Bidder and OEM duly signed by an authorized signatory)

These Corrigendum/Modifications/Additions to Request for Proposal for the procurement of Backup solution for ODS project of Life Insurance Corporation of India are issued with the approval of Secretary (IT/DT).

Secretary (IT/DT)