

Revised-II-Technical Annexure-I

RFP for Supply, Installation, Commissioning and Maintenance of Hardware for LIC Private Cloud

Ref: LIC/CO/IT-BPR/HWDEV/CO-CLOUD/23-24/01 Dated: 14/03/2024

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
1	The bidder shall propose Plan & Design/Architecture and Health check services from the OEM. The OEM shall conduct a health-check of the deployed solution and submit a report indicating compliance to reference architecture and best practices		
2	The bidder shall propose direct back to back support and access to product updates/upgrades of OEM support 24x7x365 days for proposed products with unlimited number of incidents and dedicated support manager should be aligned giving highest level of support for LIC. The Bidder need to consider the support from the respective software OEM SKUs.		
3	Hardware Infrastructure OEM should have 24x7 support center in India and logistics center in Mumbai and Bengaluru		
4	The bidder shall propose Plan, Design and Validation Services from the software provider OEM (for Hypervisor, Software defined Storage, Private Cloud Software, Cloud security & Backup Software), Implementation should be carried out by OEM Certified Engineers provided by the Bidder. The OEM shall not subcontract the Design and Validation services to any third party. The OEM engineers Designing and Validating shall be on the payroll of the software OEM.		
5	The Bidder should propose Technical Account Manager (TAM) services from Software OEM throughout the contract to conduct Quarterly health check, suggest OEM best practice for the deployed solution and submit a report indicating compliance to reference architecture and OEM best practice. TAM should also be responsible for providing recommendation and available when required by LIC for upgrades and updates.		
6	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 (including any storage controller VM requirements on each host) should be called out explicitly (after considering de-duplication, compression, erasure coding) in solution document (with a public documentation providing the overhead calculation) & factored over and above the stated requirement in RFP for Cloud management & Operations, Automation & Orchestration, Hypervisor, Cloud Security.		
7	The bidder shall ensure that all the proposed software components as part of the solution shall have the ability to run on proposed HCI Solution based on the x86 architecture.		
8	The Bidder should propose Hypervisor, Cloud Management Layer, Software Defined Networking and Software Defined Storage from single OEM.		
9	Proposed Solution should be able to natively move VM along with its data across the DCs (DC and DR or other sites) with minimal downtime of VMs.		
10	The bidder has to ensure that proposed hardware & software infrastructure should be tightly integrated to deliver the use cases, functionality and capability required by LIC		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
11	The solution shall provide minimal downtime, zero-data loss continuous availability against physical host failures. This high availability should be offered without any dependency on the guest operating system.		
12	Integrated solution should have continuous secure enterprise visibility/dashboard of entire virtual infrastructure.		
13	The solution shall provide a framework to integrate with 3rd party endpoint security solutions.		
14	The solution shall provide a single web based management interface with end-to-end visibility of the data center platform delivering key functionality such as performance, capacity and configuration compliance.		
15	The solution shall provide explanations and recommended solutions to performance, capacity and configuration problems. It should also associate workflows with alerts to automatically initiate corrective measures at critical thresholds.		
16	The solution shall provide prebuilt & customizable operations dashboards & reports to provide real-time insight into infrastructure behavior, upcoming problems and opportunities for efficiency improvements.		
17	The solution shall provide guidance on right-sizing, resource consumption, risks and future issues that are unique to every data center environment. The solution should also provide capacity analytics which can identify over-provisioned resources so they can be right-sized for most efficient use of virtualized resources.		
18	The solution shall provide assistance in troubleshooting and operational management in the virtualized environment.		
19	The solution shall provide a software-defined and virtualized networking model that allows placement of virtual workloads on segments of networks that are isolated from each other without dependence on the underlying physical networking infrastructure configuration.		
20	The solution shall provide a virtual switching fabric that allows simplified GUI based configuration of switching capabilities such across the cluster with the ability to backup & restore network configuration (by restoring the management appliance)		
21	Traffic flow should be monitored and audit trails should be able to generate access information with all source information within the HCI environment.		
22	The solution shall provide stateful inspection for virtual workloads that can be applied at the virtual machine level.		
23	If data caching layer is required in proposed solution, the solution shall provide a data caching tier that supports SSD/PCIe/UltraDIMM/NVMe.		
24	The solution shall provide the ability to scale-up (by adding more disks to existing nodes) or scale-out (by adding more nodes to the cluster) in terms of storage and compute.		
25	The solution shall be able to use hypervisor/ VM based replication to asynchronously replicate VMs across sites based on configurable schedules of RPO (Replication) of 5 minutes or less and RTO (For VM Recovery) of 15 minutes or less.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
26	The solution should provide orchestration layer to have automated disaster recovery. The recovery plan should be granular enough to enable individual VM level recovery at the DR site. (for license calculation initial requirement: 2500 VMs)		
27	The solution shall have the ability to change storage policies applied on VMs on the fly without having to restart workloads		
28	The solution shall also support storage space efficiency features like de-duplication, compression and RAID 5/6 with erasure coding i.e. protection against single drive or single host failure. [All overheads should be taken care of separately]		
29	Proposed solution should be able to integrate Internal Network at speed of 10/25G and External Network at speed of 40/100G. Internal and External network connectivity will be provided through SDN solution already available with LIC. Vendor needs to provide required cables. Management Switches needs to be provided by vendor.		
30	The solution shall provide an orchestration engine with ready workflows and ability to create custom workflows like provisioning VMs across clusters. (for license calculation, initial requirement: 1000 VMs)		
31	The solution shall provide SELF-SERVICE portal to end users for virtual machine provisioning & support automated delivery of data-center services. (for license calculation, initial requirement: 1000 VMs)		
32	The proposed solution should have built-in replication capability which will enable efficient hypervisor replication of virtual machine data over the LAN or WAN with an RPO of 5 minutes or less. In case additional licenses are required for VM replication and Disaster Recovery Orchestration, license should be quoted for 2500 VMs.		
33	The proposed solution should be capable of working as a hybrid cloud in future, with single management platform for managing workloads of private and public cloud. In case additional licenses are required for Public Cloud VM management, license should be quoted for 100 VMs		
34	Solution should support VM provisioning across DC/DR/Public Cloud/Hybrid Cloud		
35	Bidders must propose the HCI solution with 5 year comprehensive onsite warranty and AMC for 6th & 7th year.		
36	Solution should provide a centralized console to perform single click upgrade/update of Hypervisor, Cloud Management, Container platform, Software Defined Storage and Software Defined Networking layers		
37	The solution should have capability for remote log collection and proactive support for predictive hardware component failure.		
38	Power available per RACK is 12 KVA at DC site and 12 KVA at DR site . RACK calculation needs to be done accordingly.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
39	The proposed Virtualization & Private Cloud software usage licenses in the solution should be Perpetual/Subscription in nature and core based. If any bidder doesn't have core based licensing then they must provide unlimited VM licenses to LIC and should NOT have any dependency on particular hardware make and model. All the Cloud management capabilities should be provided by a Single Software OEM. In case of subscription based licenses, subscription period should be considered as 7 years with an option to extend by one more year with rate quoted for 7th Year.		
	Functional Specifications		
40	The proposed Hyper converged Infrastructure (HCI) hardware should be certified for the proposed Virtualization software.		
41	The usable resource requirement(exclusive of management and system overheads as mentioned in Sl. No. 6) in each site (DC and DR) is as follows, Cluster-1: 1) 1024 physical cores 2) 16 TB RAM 3) 200 TB Usable Space before de-duplication, compression and erasure coding, with All Flash NVME storage (Enterprise Class), Note: This cluster can be used to host Windows VMs. Cost of licensing cluster for hosting Windows VMs with Windows Server 2022 Data Centre Edition should be quoted in commercial bid. LIC will decide at the time of placing order based on actual requirement. Cluster-2: 1) 1024 physical cores 2) 16 TB RAM 3) 400 TB Usable Space before de-duplication, compression and erasure coding, with All Flash NVME storage (Enterprise Class) Cluster-3: 1) 1024 physical cores 2) 16 TB RAM 3) 400 TB Usable Space before de-duplication, compression and erasure coding, with All Flash NVME storage (Enterprise Class), *Minimum IOPS required is 1,00,000 (expected Read Write Ratio of 60:40) for a mix work load. Physical to virtual CPU ratio considered is 1:4 Above usable resources are required even after one Node and one drive failure in a cluster.		
42	Per Node/Server(Enterprise Class) specifications - For Cluster-1: Latest Generation (Certified by Proposed Virtualization software OEM) x86 64 Bit architecture-based, 2x32 core Intel Platinum Processor with minimum 2.5 GHz Clock speed or higher and 60 MB Cache or higher		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
	For Cluster-2 and Cluster-3: Latest Generation (Certified by Proposed Virtualization software OEM) x86 64 Bit architecture-based, 2x32 core Intel/AMD Processor with 2.4 GHz Clock speed or higher and 60 MB Cache or higher For Cluster-1, Cluster-2 and Cluster-3: Processor with more than 32 cores can be provided subject to maximum of 64 cores i.e. maximum 128 cores per node. Minimum of 1 TB DDR5 RAM with true runtime memory speed of 4800 MHz or higher , expandable upto 2 TB If more than 1 TB RAM provided then true runtime memory speed can be 4400 MHz or higher. Two number of quad port (Or Four number of Dual port) 10/25GbE Cards populated with 8 quantity of 25G SFP for connectivity to the existing Leaf Switch from day one. All SFP provided in the solution should be OEM make. Cables required for network connectivity should be provided. N+1 hot swappable Power Supply. [Overheads of management and system setup to be taken care of separately]		
	Hypervisor Related		
43	The solution shall provide a purpose-built hypervisor 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.		
44	Support for heterogeneous guest OS - Window and Linux (Redhat, Cent os, SuSE, Ubuntu, Debian). Respective windows and Linux guest OS must certify the underlying hypervisor and should be available publicly.		
45	Proposed hypervisor should support standard features like VM Migration, High Availability, & Distributed Resource Scheduler.		
46	Hypervisor shall provide the ability to hot add CPU and memory , hot-plug disks and NICs (provided the same is supported by guest OS)		
47	Hypervisor should support container and open source integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		
48	Virtualization Management software should be deployed in clustered mode across nodes & racks so that failure of host, OS, virtualization management software component should have zero downtime impact on the availability of Virtualization management.		
49	Hypervisor / Proposed HCI should support Import of Other Disk Styles VMDK, VHD, QCOW2, OVF natively without any external 3rd party tool.		
50	Hypervisor must have capability for OS Catalogue/ template and OS provisioning with role based access to virtual machine.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
51	Proposed hypervisor should support standard features like non-disruptive migration of workload across hosts, High Availability and Distributed resource scheduling during resource constraints.		
52	Hypervisor shall provide automated live migration for initial placement and balancing of available resources with the rules to define affinity and / or anti-affinity of workloads		
53	Hypervisor should provide ability to grant / ensure resources to virtual machines as they need for hosting critical workloads. Also the initial placement of workloads should consider CPU, Memory and Storage contentions / hotspots.		
54	Hypervisor shall provide zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.		
55	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		
56	Virtualization Manager must support Directory based/Open LDAP and SAML based authorization for management.		
57	Virtualization software should provide network traffic-management controls to allow flexible allocation of physical NIC to different network- traffic types enabling segregation of different Network-traffics and should support 802.1Q for multi VLAN traffic.		
58	Hypervisor should support Rest API and Command line management along with GUI interface.		
59	Required Hypervisor License and Hypervisor Management licenses should be highest level of license edition included into the solution.		
60	Hypervisor shall provide centralized interface from which virtual machine access switching for the entire data center can be configured, monitored and administered.		
61	Virtual Machine performance reports for performance and utilization of virtual machines should be available.		
62	High availability capability should be available that utilizes server health information and migrates VMs from failed hosts if host failure occurs.		
63	The solution shall provide configurations at VM level that can be tuned to help reduce latency by reserving Storage or defining Storage QoS at IOPs & Throughput level.		
64	Proposed Solution should support Memory overprovisioning using advanced memory management techniques such as “Memory Ballooning” or “Memory Swapping” or “Transparent page sharing” or “Memory Compression”.		
65	The solution should be able to Migrate VM with data from existing hypervisor (Vmware in existing private cloud) to proposed hypervisor (In this new private cloud). Existing private cloud will be in use for some time and after that this migration will be required. Existing backup copies created using Veeam Backup software needs to be migrated to new private cloud backup repository. Bidder needs to include this migration cost in BOQ considering 400 VMs with total VM data size as 250 TB and backup data size as 130 TB		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
66	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.		
67	It should support affinity and anti-affinity rules to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated using GUI/CLI.		
68	Virtualization software should provide Cluster level encryption which protects unauthorized data access at-rest without any performance overhead natively.		
69	Should provide abstraction of GPU pool to allocate to VMs for GPU intensive workloads.		
	Software Defined Storage		
70	Support for real-time data storage tiering between cache and capacity disks to maintain optimal performance, should be a part of the solution and any licenses for the same should be incorporated as part of the proposal.		
71	The solution must have De-duplication and Compression features licensed and Compression implemented from day one (Should not have dependency on any proprietary hardware device). Storage Efficiency Features should be available across any type of nodes.		
72	The solution should deliver zero data loss in case of disk, host or network failure. The HCI Platform should have Disaster Recovery Orchestration to create Recovery Plans for the Virtual Machines		
73	The proposed solution should provide hyper-converged software that allows delivery of enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network & associated components such as SAN Switches & HBAs.		
74	The proposed HCI solution should be 100% software defined and should not leverage any specialized hardware (proprietary) other than x86 Hardware to run virtualization layer with Software Defined Storage.		
75	The proposed solution should provide framework to set storage and data policies like mirroring, fault tolerance, capacity reservation, cache reservation, IOPs on a per-VM & per virtual disk basis and should also allow changes to these policies on the fly without restart of virtual machines.		
76	HCI solution should support for hosting their SDS (Software Defined Storage) component with choice of servers hardware available from leading OEM's. LIC should be able to run SDS solution on any compatible x86 hardware of choice and Licenses proposed for Software Defined Storage (SDS) Platform should be perpetual/ subscription based in nature (end user License name must be in the name of LIC). Bidder/OEM need to provide the Hardware Validation on the proposed HCI Solution. The SDS license should not be tied with any specific hardware and must be transferable to any supported x86 hardware, in case LIC wants to deploy it on new supported x86 hardware.		
77	HCI solution should support data integrity and consistency check against stored checksums, in the event of advert issue, data should automatically start rebuilding immediately in cluster for data resiliency without any manual admin intervention in case of Disk or Node failure.		
78	Proposed solution should support 1 Node failure per cluster at both DC and DR location.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
79	The Solution should be able to work on latest supported x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor /make /model.		
80	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.		
	Cloud Management Platform		
81	The solution should have catalogue of private as well as public cloud services (When Procured), and should support self-service provisioning capabilities for the new Proposed Hybrid Cloud Solution.		
82	Central administrator must be able to manage/control the self-service portal view for the tenants and enable multi tenancy. Any authorized user must be able to deploy the application using the published blueprint in his self-service portal.		
83	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting, capacity, cost optimization etc.		
84	Ability to integrate with industry standard authentication like AD and it should have inbuilt identity services to provide seamless single sign on experience across cloud management components.		
85	Service Catalog Integration, and support for show-back and resource usage.		
86	Dashboards must be available to allow different customers to control the behavior and consumption of the services		
87	The model should include at least three user levels for the Platform (Admin/User/Monitor)		
88	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network, storage, applications and custom services through a unified multi-tenant IT service catalog.		
89	The solution shall allow authorized administrators, developers or business users to request new IT services, manage specific cloud and IT resources, while ensuring compliance with business policies.		
90	The solution must allow the use of the company default public cloud credential to provision and manage the resources.		
91	The solution must support provisioning on Private and Public Cloud.		
92	The solution should have capability for mixed deployment in a blueprint. eg. Provision database like Oracle, MSSQL in private cloud & Provision Application & Web Server in different cloud provider. eg. Web of Cloud and DB on Premise with L2 Extension.		
93	The solution must allow restriction of vCPU, Memory and Disk resources to each project or group of users and also have restriction on other controls such as naming and tagging		
94	The solution must provide full audit governance on who launch the blueprint, output log of each action and script used to run the action.		
95	The solution must allow/support disk image of Windows, Windows Server and all variant of Linux.		
96	The solution must allow single management console to view the capacity, performance of the infrastructure and the blueprint designer without logging in		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
	to different URL.		
97	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		
98	The vendor must provide pre-defined set of blueprints available in the self-service portal.		
99	The software must allow the designer to design the automation.		
100	The software must support multiple application profiles for private cloud as well as public cloud service providers.		
101	The software must allow the designer to create custom action for the team to use. Eg. Scale out or Scale Up. Bidder needs to deploy scale up and scale out as a requirement stated in scope of work.		
102	The software must allow the designer to use shell script, PowerShell script to code the automation.		
103	The software must allow infrastructure as code to allow the developer to create, delete and launch the cloud agnostic blueprint in case LIC requires that capability in future so that same blueprints so created can be deployed LIC private clouds and public clouds.		
104	The software must allow the designer to define variable which can be used during the execution.		
105	The software must allow the dynamic addition and modification to the variable.		
106	The designer Blueprint can define the vCPU & memory for each virtual machine.		
107	The software must allow the designer to design multiple VMs blueprint.		
108	The software must allow the designer to create multiple replicas of the VMs providing min and max no. LIC wants to create simultaneous VMs across DC and DR to have sync in configuration and wants this to be enabled from Day-1. Data replication in case of Active-Active VMs at DC-DR sites, will be taken care by application team.		
109	The operator will be able to power on, power off, restart, scale up and down, delete and perform any other custom VM action through the UI.		
110	The solution should be able to give a complete cost governance across the Private Cloud.		
111	The solution shall support creation of services such as 'Single VM' and a 'Multi-tier application infrastructure (including software based constructs such as load balancers)' as part of a standard template.		
112	The solution shall support native (without using any 3rd party component) approval policies integrated with email notifications such that approvals/rejections can be done.		
113	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 through APIs.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
114	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		
115	The solution shall provide an orchestration engine with ready workflows and ability to create custom workflows based on SOAP/ REST operations and PowerShell scripts.		
116	The solution should be able to define multiple tenants which would enable the administrators to create a secure multitenant infrastructure wherein a tenant can have resources, service levels and automation processes that uniquely meet that tenant's needs.		
117	The proposed Private Cloud solution must be ready for containers, Kubernetes and dockers deployment.		
118	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 analyze unstructured data from 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.		
119	The solution shall provide automated provisioning of infrastructure through a unified, web-based, multi-tenant self-service IT service catalog.		
120	The Solution should do 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.		
121	self-healing services monitoring such that identified services should be running and should restart automatically if stopped as desired state and vice versa within the scope of HCI infrastructure only		
122	Solution should continuously monitors for compliance and should report any deviations through automated alerts to ensure consistent adherence to policies		
123	Solution should continuously evaluates environments and should notify through automated alerts in case any issue is identified		
124	The Solutions should support event-driven configuration management, remote execution, and orchestration for enforcing configuration across VMs and infrastructure.		
125	Solution should have capability to automate Software deployment and updates in VM's OS and Should have capability to enforce Operating systems hardening and compliance.		
	Cloud Security		
126	The solution shall provide visibility of network traffic between the VMs.		
127	The solution shall provide a software defined security & security virtualization layer that allows faithful delivery of network services in software without dependence on specific make/model of networking devices/appliances.		
128	The solution should provide a stateful distributed firewall such that the firewall for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
129	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.		
130	The solution should provide embedded/virtual machine distributed firewall and should provide near line rate performance.		
131	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.		
132	The solution shall lend itself to network monitoring by supporting standards protocols (for remote network analysis).		
133	The solution shall provide ready integration with the proposed platform to automate delivery of networking & security services such as switching, routing and firewalling.		
134	The solution should be capable to provide agentless or Light weight agent guest and network introspection services. Agentless preferred.		
135	The solution should have capability to provide stateful micro-segmentation for virtual machines from a single console.		
136	The solution should have capabilities to integrate with industry-leading Solutions for antivirus, malware, intrusion prevention, and next-gen security services.		
137	The solution should provide a stateful firewall with capability of defining security policies on constructs such as IP address, VM names, objects and tags and Security tags		
138	The Security policies must follow the VM in the event of migration (i.e. vMotion) within the data center.		
139	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.		
140	The proposed solution should be a purely software based solution and should not be dependent on any hardware make and model.		
141	The bidder shall ensure that all proposed components shall have the ability to run on standard compatible server infrastructure based on the x86 architecture without having any dependence on specific make/model of infrastructure components.		
142	The 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.		
143	The solution should provide overlay network & security virtualization and should work on any underlay physical network devices make and topology.		
144	The solution should support virtual Distributed Switch which is a generic software defined switch platform that is supported on proposed hypervisor.		
145	The solution should support the ability to create a cluster of managers of Network & Security virtualization for high availability of the user interface and API.		
146	The solution should offer to deploy virtualized network functions (like vswitching, firewalling), administrators can build virtual networks for Virtual		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
	Machines or Virtual Desktop Infrastructure without the need for complex VLANs, ACLs or hardware configuration syntax on underlay physical network.		
147	The solution should support micro-segmentation for east- west traffic of virtual machines, offering security policy on VNIC of the virtual machines.		
148	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.		
149	The solution should support Secure VPN between two data centers or between on-premise to public cloud.		
150	The solution should support traceflow/process level details of individual VMs and workload.		
151	The 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.		
152	The solution should support network & security virtualization operations and troubleshooting.		
153	The solution should be certified and integrate with proposed private cloud solution.		
154	Proposed solution should support IPV4 & IPV6.		
155	Proposed solution should be certified and integrate with existing network underlay infrastructure which the LIC has already invested into. Please provide Design and integration document.		
156	The proposed solution should provide uniform micro segmentation capabilities Across Private and Public Cloud		
157	For License calculation, All Clusters should be covered.		
	Load Balancer		
158	The solution shall provide a basic virtual load balancer to scale application delivery. In case of License calculation, license for 100 instances should be included in BOQ for this functionality.		
	Backup Solution (Backup Software + Purpose-Built-Backup Appliance/ Distributed Storage)		
159	Proposed Backup solution at DC and DR should be offered with minimum 1 PB of usable storage capacity before Compression, Deduplication and Erasure Coding and it should be upgradable up to 2 PB		
160	Proposed Backup solution should be based on 'Disk-To-Disk-To-Disk' Technology and the proposed backup software should be in the Leaders quadrant in the latest available Gartner Magic Quadrant for Backup and Recovery Solutions .		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
161	Backup schedule to be supported by offered product: Daily, Weekly, Monthly, Yearly. Backup retention policy for DC and DR: Daily Backup-24 copies, Weekly Full Backup-4 copies, Monthly Full Backup-12 copies, Yearly Full Backup-3 copies		
162	The proposed software should have inbuilt calendar-based scheduling system, Proposed back up software should support various level of backup e.g. Full, incremental/differential/ synthetic full.		
163	Should be able to provide backup window of 10 hours		
164	Proposed backup hardware should support throughput of 25 TB/hour for native backup without considering deduplication, compression.		
165	Backup software should be with Perpetual / Subscription based licensing and Enterprise grade software (all features should be enabled from day one without any rider).		
166	The proposed Backup software must offer capacity, socket or instance based licenses with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary and DR site. If bidder is quoting capacity based licenses, bidder should quote for 1PB capacity. if bidder is quoting instance based licenses , bidder to quote licenses for 2500 VMs		
167	Backup software should be Hardware Agnostic software and it should support snapshot integration with any virtualization system like VMWare, AHV, Hyper-V and RHEV etc. and support de-duplication on any storage target. It should be able to backup data to discs for long term retention.		
168	Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied.		
169	The offered product to have web based Graphical User Interface (GUI) so that all backup can be managed centrally, regardless of locations, GUI to be same across heterogeneous platform to ensure easy administration.		
170	Proposed solution should have security and compliance dashboard inbuilt with the product.		
171	Software should be able to restore VMs to a cloud service provider like AWS, Azure or Google directly from the backup copy.		
172	The software should have the capability to backup on-prem data directly into cloud repositories such as AWS S3 or Microsoft Blob.		
173	Proposed backup software should be able to leverage Immutable Cloud based storage like S3-Immutable service to prevent backup copies of data from any corruption or ransomware attacks.		
174	The backup software must Pinpoint identified ransomware strains and prevent reintroduction of malware into your environment using YARA (or equivalent) content analysis.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
175	The proposed solution should have on demand scans available for malware attacks.		
176	The backup software must have built in Malware Detection Engine performs low impact, real time data and file extensions/via guest indexing analysis during backup for immediate malware detection.		
177	Proposed solution should support options for immutability, WORM, Air-Gap and data isolation for backup data.		
178	Proposed backup solution must be offered to protect the backup from any malware & ransomware attacks and provide guaranteed recovery		
179	The backup software must instantly reports backup inconsistencies into SIEM tools so we can act fast and reduce further risk to data.		
180	The backup software must prevent the accidental or malicious deletion or encryption of backups by employing a zero trust architecture, "Four eyes" (or equivalent) admin protection and immutable backups.		
181	The proposed backup software should provide Instant recoveries for any backup.		
182	Backup software should support file level recovery from any backup of any VM		
183	The Proposed backup Software should support Syslog and SIEM Tool integration.		
184	Backup software should support instant database recoveries of MySQL, MS SQL from the backup files.		
185	Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.		
186	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability.		
187	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.		
188	Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities.		
189	Proposed backup software should be able to harden the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks.		
190	Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten" regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.		
191	The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation
192	Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site. The above feature should be achieved either by the Backup Software or by the proposed hypervisor solution.		
193	Backup software should be able to replicate Backup data to another site for compliance / Disaster Recovery purposes, with or without the need of external replication tools on Backup array. All necessary hardware and licenses for achieving consistent replication of backup data should be quoted.		
194	Backup software should have the ability to backing up a Public Cloud VM like VMs running in AWS or Azure and restore it as a valid VM workload back onto a hypervisor based server farm.		
	Object Storage		
195	Proposed object storage at DC and DR should be offered with minimum 500 TB of usable storage capacity before Compression, Deduplication and Erasure Coding and it should be upgradable up to 1 PB Proposed Object Storage should give minimum throughput of 1500 MB / second considering below minimum parameters, Get / Read Throughput - 10% Put / Write Throughput - 90% Object Size - 7 MB Note: This Object storage will be used primarily for storing video KYC files and it will not be used as a backup storage. Backup of these video files is not required.		
196	Proposed Object storage should be configured with WORM capability		
197	Erasure coding algorithm provided must support data protection against 2 drive failure across same storage node or failure of 1 storage node		
198	There should be replication between Object Storage at DC and DR.		
199	Object Storage must be managed and monitored via integrated UI, CLI & RESTful APIs, shall support multi-tenant architecture including ability to apply quota limits on specific sections within the object store. Object storage should allow different administrative rights over different tenants, and logical containers/buckets inside individual tenants.		
200	Object Storage must protect all objects with Erasure Coding without the dependencies of RAID storage.		
	RACK		
201	42U rack with 4 power strips with sufficient sockets compatible with proposed hardware.		
202	Sufficient Cable Managers, Fans & Castor Wheels.		
203	Make- OEM/ VALRACK/ President/ HCL		
	Deviations(if any)		

SL No.	General Specifications	Compliance (Yes/No)	Link to documentation

Date:

Signature of Vendor/Vendor's Representative