Bidders are required to indicate their compliance **(Yes or No)** commitment to the items listed in the tables below. Failure to commit to these items will lead to bid disqualification. Bidders are required to **initial all pages** and **sign the last page** in the spaces provided.

Primary site - Capacity

Requirement	Minimum	Expected outcome	Compliance Yes/No
Compute CPU Cores	984 cores	The cores should be usable	
Memory	7TB		
Software Defined Storage	500TB	All Flash disks – usable capacity	
	1PB	HDD disks storage – usable capacity	
Hosts Networking (East-West inter cluster traffic)	10GB interfaces	Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Applicable for East-West traffic (layer-2 boundary)	
Hosts Networking (North-South traffic to physical network or ToR switches)		Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Crosses a Layer-3 boundary to communicate with the rest of the network. Should be enough to connect all the hosts to our network	

Secondary site

Requirement	Minimum	Expected outcome	Compliance Yes/No
Compute CPU Cores	984 cores	The cores should be usable	
Memory	7TB		
Software Defined Storage	500TB	All Flash disks – usable capacity	
	1PB	HDD disks storage – usable capacity	

Hosts Networking (East-West inter cluster traffic)	10GB interfaces	Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Applicable for East-West traffic (layer-2 boundary)	
Hosts Networking (North-South traffic to physical network or ToR switches)		Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Crosses a Layer-3 boundary to communicate with the rest of the network. Should be enough to connect all the hosts to our network	

Third Site WC

Requirement	Minimum	Expected outcome	Compliance Yes/No
Compute CPU Cores	64 Cores	The cores should be usable	
Memory	128 GB		
Software Defined Storage	200GB	SSD disks storage – usable capacity	
	500 GB	HDD disks storage – usable capacity	
Hosts Networking (East-West inter cluster traffic)	10GB interfaces	Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Applicable for East-West traffic (layer-2 boundary)	
Hosts Networking (North-South traffic to physical network or ToR switches)		Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Crosses a Layer-3 boundary to communicate with the rest of the network.	

		Should be enough to connect all the hosts to our network	

Fourth Site EC

Requirement	Minimum	Expected outcome	Compliance Yes/No
Compute CPU Cores	64 Cores	The cores should be usable	
Memory	128 GB		
Software Defined Storage	200GB	SSD disks storage – usable capacity	
	500 GB	HDD disks storage – usable capacity	
Hosts Networking (East-West inter cluster traffic)	10GB interfaces	Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Applicable for East-West traffic (layer-2 boundary)	
Hosts Networking (North-South traffic to physical network or ToR switches)		Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Crosses a Layer-3 boundary to communicate with the rest of the network. Should be enough to connect all the hosts to our network	

GNC Site

Requirement	Minimum	Expected outcome	Compliance Yes/No
Compute CPU Cores	64 Cores	The cores should be usable	
Memory	128 GB		
Software Defined Storage	200GB	SSD disks storage – usable capacity	
	500 GB	HDD disks storage – usable capacity	

Hosts Networking (East-West inter cluster traffic)	10GB interfaces	Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Applicable for East-West traffic (layer-2 boundary)	
Hosts Networking (North-South traffic to physical network or ToR switches)		Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Crosses a Layer-3 boundary to communicate with the rest of the network. Should be enough to connect all the hosts to our network	

DMZ Site

Requirement	Minimum	Expected outcome	Compliance Yes/No
Compute CPU Cores	64 Cores	The cores should be usable	
Memory	128 GB		
Software Defined Storage	200GB	SSD disks storage – usable capacity	
	500 GB	HDD disks storage – usable capacity	
Hosts Networking (East-West inter cluster traffic)	10GB interfaces	Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Applicable for East-West traffic (layer-2 boundary)	
Hosts Networking (North-South traffic to physical network or ToR switches)		Interfaces should support minimum 10Gbps with redundancy and be scalable to 40Gbps connectivity when needed Crosses a Layer-3 boundary to	

		communicate with the rest of the network. Should be enough to connect all the hosts to our network	

Item	Focus Area	Requirement	Compliance Yes/No
1.	Compute	The solution should be scalable in a non-disruptive manner by adding additional nodes to the cluster at a later point of time without having to power down any nodes	
2.		Computes should be implemented with HA in the event of node failure and virtual machines should migrate to another node automatically	
3.		The solution should provide the ability to scale-up (by adding more nodes to the cluster), and or more compute resources to a node.	
4.		The solution should provide the ability to create rapidly on-board new hosts to the platform by automatically deploying reference configurations including networking settings	
5.		Scale node (compute + storage), compute-intensive or storage-intensive independent of each other should be supported	
6.	Storage	Solution should be software defined with Flash Storage disks(SSD) and non-flash (HDD) disks	
7.		The solution should support storage space efficiency features such as de-duplication and compression	
8.		Should have automated self-rebalancing capabilities to align with defined Storage service levels based on best practice	
9.		The storage solution should have in-built software defined storage capability integrated within the Hypervisor kernel.	
10.		The proposed solution should have built-in replication capability which will enable efficient array-agnostic replication of virtual machine data over the LAN and WAN	

11.		Solution should provide QoS capabilities for storage I/O that are enforced across all virtual machines accessing a storage, regardless of which host they are running on either automated or configurable	
12.		Virtualization software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues	
13.	Disaster Recovery	The solution should offer automated orchestration of site failover and failback with a single-click to reduce recovery times.	
14.		The solution should offer frequent, non-disruptive testing of recovery plans to ensure highly predictable recovery objectives.	
15.		The solution should offer Centralized management of recovery plans from the virtualization manager console replacing the manual runbooks	
16.		The solution should offer VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on storage	
17.		The solution should offer application-agnostic protection to eliminate the need for app-specific point solutions	
	Technical account manager	Provide at least one dedicated technical account manager for full project deployment to cover all sites.	
	SAP Workloads	In ensuring that the environment is adequately provisioned in line with SAP technology best practice, it is important that the Private cloud adhere to SAP as an OEM required standards of provisioning the machines.	
	Oracle Workloads	In ensuring that the environment is adequately provisioned in line with Oracle technology best practice, it is important that the Private cloud adhere to Oracle as an OEM required standards of provisioning the machines.	
	Microsoft Workloads	In ensuring that the environment is adequately provisioned in line with Microsoft technology best practice, it is important that the Private cloud adhere to Microsoft as an OEM required standards of provisioning the machines.	

	SLA	The Bidder should provide support response time on service requests. This will form part of the SLA.	

Item	Focus Area	Requirement	Compliance Yes/No
	Hypervisor	**High Availability** Hypervisor layer should support live migration of running virtual machines from one physical node to another with zero downtime, continuous service availability, and complete transaction integrity transparent to users	
		Maintenance The solution should 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.	
		Dynamic Resource Allocation Allocates and balances computing capacity dynamically across collections of hardware resources for virtual machines	
		Virtual Network It should provide virtual switch that can span multiple hosts, enabling significant reduction of on-going network maintenance activities and increasing network capacity	
		Inter-Operability The proposed solution should be able to inter-operate with another existing ecosystem in the datacenter. It should be able to inter-operate with traditional FC/ISCSI or even Physical Server storage on other clusters	
		Replication The solution should offer VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on only storage replication	
		Single and Multi Storage migration Migration of all virtual machine related files or data from one datastore to another without service interruption either in the same storage or across to another storage array	
		Reliability Virtualization software shall provide a virtualization layer that sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability	

		and security	
		On-demand self Service Solution should provide consumer of cloud computing solution to be able to automatically acquire and release resources without requiring any action from ICT engineers whenever the need for such resources increases or decreases. Should supports multi-level approval process settings for cloud resources and approval notification so that users can specify a maximum of five levels of approvals and are notified to approve resource requests.	
		Resource pooling The solution should offer resource pooling where the available computing resources, physical or virtual, are pooled together and are dynamically assigned and reassigned based on consumer demand. i.e. through tenants & multi-tenant model.	
		Rapid elasticity Provide provisioning and releasing of the resources, instantly and elastically, in an automatic way in order to enable a consumer to quick scale out and in based on customer's demand	
		Measured Service and Charge back Provide cloud computing solution with the ability to measure the consumption of resources, and to automatically control and optimize the resources and use quotas as mechanism to control and charge back business units	
	Cloud Services of Cloud Controller	**Dedicated Physical Machines** Provide dedicated physical machines for SAP applications. The orchestration must be capable to manage the dedicated physical machines for SAP applications as part of the cluster	
		Object Storage Service (OBS) Provide solution that support S3, POSIX, NFS, and SFTP protocols in the same cluster, so that user's data can be accessed by a variety of clients.	
		Unified Management of Hybrid Cloud Supports hybrid cloud artificial intelligence (AI) so that users can call AI services such as image recognition and facial recognition on the hybrid cloud management platform.	
		Domain Name Service (DNS) Should supports the DNS service. A domain name that map private IP addresses to	

		provide the DNS service for cloud resources in the clusters. Domain names can be created without the need to purchase and license. Should allow users to create, modify, and delete domain names on the management console.	
		Cluster management Support the lifecycle management of multiple clusters, including cluster creation, scale-out, scale-in, upgrade, and deletion.	
		Operations Management The solution should support Online Analytics on Health of the storage and provide predictive alerts	
		Operations Management One Click non-disruptive rolling upgrades of system software and system firmware from the same management GUI console	
		Operations Management Single dashboard to manage and provision virtual machines, network, storage, monitor performance and manage events & alerts	
		Operations Management The solution should provide prebuilt & customizable operations dashboards & reports to provide real-time insight into infrastructure behaviour, upcoming problems and opportunities for efficiency improvements	
		Operations Management The solution should provide a log analytical tool which will collect data from various data Sources limited to proposed solution	
		Operations Management The solution should provide unified management of performance and capacity for the proposed platform via a role-based web interface	
		Operations Management The solution should provide the ability to identify and report on over-sized, under-sized, idle and powered-off virtual machine such that the environment can be right-sized and resources can be reclaimed The solution should provide predictive analytics capabilities to understand baselines and model capacity and demand for accurate forecasting of infrastructure requirements	
		Operation Management	

		The solution should provide configuration compliance reports/alerts/dashboards for the underlying hypervisor platform	
		Interoperability The Bidder should ensure that the private cloud is Interoperable with other cloud providers. I.e. connector to third parties, hosted services at other cloud providers	

Security Solution - Micro Segmentation

Focus Area	Requirement	Compliance Yes/No
Breadth of products	Bare Metal Hypervisors Windows Operating systems Linux Multi-clouds capabilities	
Discovery and Visibility	Agent based micro segmentation platform at host level	
	In-built full traffic visibility of applications at process level for full applications visibility	
	Identifying and discovering sensitive data (‘crown jewels’)	
	View only alerting mode (no blocking to allow phased project implementation as part of discovery and visibility	
	Provide a detect only mode allowing granular safe implementation (one application at a time approach)	
	Should enhance application owner visibility of application which can be integrated with Active directory and various data sources to provide application identity	
Policy enforcement	Provide East-West security	
	Rule based micro segmentation	
	Provide deep granularity to provide isolation between hosts in the same segment	
	Provide deep granularity to provide isolation between hosts in the same segment closest to the application its protecting	
	Provide self-learning and automatic policy generation capabilities	
	Should provide Identity based segmentation (identity centric) to allow enforcement down to	

	user identity (AD Integration) and, multi factor authentication.	
	IoT Devices Provide secure, granular control based on pre-set segments on how, when and where devices connect to the network	
	Provide comprehensive Zero Trust network security solution that extends to IoT devices (Cameras, printers, and field devices)	
	Unified solution as a single platform that enforces access control policies across users, servers, and IoT devices	
Policy enforcement	**Remote and third-party Access to the network resources** • Solution should allow to grant access based on identity with business and risk awareness. • Should secure encrypted 1:1 connection between user and approved system only. • Unauthorized resources should be completely invisible to users. • Eliminates lateral movement on internal networks. • Enforce identity-centric policies and remove over-privileged access. • Grant timely and precise access for these users. **Remote live entitlement to resources** • Should support dynamic and context sensitive posture: Have real-time understanding of policy to create individualized micro-perimeters for each user based on location, type of resources. i.e., user leaves the office, context will be dynamically adjusted, forcing a tighter access policy. And when at even more insecure location, such as an airport or other public Wi-Fi, additional adjustments can be made, further restricting ability to access sensitive company data.	
	Security operations automation • Should have reporting and alerting • Should support the automation and orchestration of workflows, processes, policy execution and reporting.	

Reporting and incident management	**Threat and vulnerability management** • The solution should have vulnerability management capabilities. • Should support the remediation of vulnerabilities with formalised workflow, reporting and collaboration capabilities **Security incident response** • The technology should be able to help PRASA plan, manage, track and coordinate the response to a security incident.	
AI Capabilities	Continuous security monitoring and intelligent analysis Unified	
General	Should present lower total cost of ownership	
	Easy to deploy with no major change to the applications and systems.	
	Should utilise minimal footprint on hosts	
	Should exhibit a low implementation time to avoid complex approach that can delay and result in project implementation failure	
	Should not require significant change to user experience	
	Should eliminates “default trust” that leads to attacks from within the network thus will address internal and external threats.	
	Should have capabilities to cloud Scale and have resilience - Provide hybrid ready/native and cloud agnostic capabilities which can work across heterogenous cloud environments.	
	Should be resilient and highly available.	

Datacenter Facility

Focus Area	Requirement	Compliance Yes/No
Datacentre Support	Support services to be available 24x7x365 with 2 HR respond time. The maintenance and support agreement should cater full service, preventative & unscheduled maintenance on list of equipment inclusive of labour and the replacement of parts. It is therefore required that the bidder should provide full maintenance as managed service	

Parts	Bidder to replace parts for the equipment's under support agreement and to adhere to the SLA when incident arise. Original factory parts should be used for replacement. Bidder is required to provide parts replacements for all the components of the DC, and it should be included in the cost for 36 months contract duration. Issues such as availability of stock, supply of tested and certified parts, contingency planning in the event of defective parts, and the removal and disposal of old parts should be addressed as part of deliverables.	
Management Software	Bidder is required to decommission existing software in Hatfield to assign them to the primary, secondary and GNC sites. Bidder is required to install and configure the software in primary, secondary and GNC sites.	
Preventative Maintenance	Bidders to provide preventative maintenance service schedules **quarterly** (4 service schedule per year over 36 months) on list of equipment to be maintained. Key components to be covered: • Air conditioner • Fire detectors • Fire extinguishers • UPS and Batteries • Cameras • Access Control System • Rack based PDU's • Power & data cable physical inspection • Raised floor • (DCIM) - Datacentre software configuration, enhancement, and optimization to streamline datacentre monitoring and management	
Unscheduled Maintenance	Bidders to provide unscheduled maintenance service on the list of	

	equipment to be maintained for 36 months period. Key components to be covered: • Air conditioner • Fire detectors • Fire extinguishers • UPS and Batteries • Access Control System • Rack based PDU's • Power & data cable physical inspection • (DCIM) - Datacentre software configuration, enhancement, and optimization to streamline datacentre monitoring and management	
Monitoring	Facility Devices Monitoring, Performance Management, Report Management, Energy Efficiency Management, Asset Management and Capacity Management should all be included as part maintenance.	
Reporting	Bidders to provide examples of reports to be submitted for listed maintenance schedules	
OHS	Bidders to adhere to OHS	

This is to certify that the Bidder has / have acquainted himself / themselves with the General Compliance Requirements in the table above for private cloud infrastructure Tender and accepts/commits to the requirements.

THUS DONE and SIGNED at _____

Signature: _____

on this _____ day of _____
DULY AUTHORISED SIGNATORY(IES) WITNESSES

1. _____ 2. _____

Signature: _____