Description	Compliance (Y/N)	Comments
Solution Features		
100% software-defined system with no dependencies on proprietary hardware		
Able to pool all direct attached storage resources of all nodes in the cluster and make it accessible to all hosts		
Provide high performance storage access to the guest VMs on the same physical host as the guest VMs making the request		
Redundant components with no single point of failure in the system		
Fully support all mainstream hypervisors		
Provide an integrated hypervisor that is built into the HCI stack and does not require a separate management interface or appliance to run		
Support multiple server hardware vendors to provide choice and lowest possible costs now and in the future		
Support Enterprise virtualization features including VMware vMotion, HA, and DRS and Hyper-V live migration and failover clustering		
Include a single management interface, even for multiple hypervisor deployments		
Ability to natively mix different hypervisors between primary and DR datacenters (i.e. use an alternate hypervisor as a DR target)		
Include native File Services (CIFS/SMB/NFS) without bolt-on or added hardware or software and managed in the same interface as the rest of the system		
Must not depend on RAID technology or Disk Groups but be fully distributed		
Scalability		
Provide a flexible pay-as-you-grow deployment model that enables expansion of cluster resources to meet real-time business demands		
Ability to add nodes non-disruptively		
Ability to remove nodes non-disruptively		
Ability to scale-out one or more nodes at a time		
Ability to mix and match different models and generations of the same server hardware manufacturer (in same cluster)		
Ability to mix and match manufacturers and generations between HCI clusters with no bearing on software support, licensing or management		
Ability to expand cluster resources in a scale-out model with predicable, linear performance		
Ability to scale storage capacity independent of compute		
Networking		
Includes network visualization capability		
Disaster Recovery/Business Continuity		
Includes native, VM-level replication that includes Disaster Recovery Orchestration and requires no add-on or separately licensed software regardless of number of VMs protected		
Option to extend the on-premise infrastructure to a cloud-managed DR site that runs the same HCI software		
Management		
Provides non-disruptive, single-click upgrade process for the entire infrastructure, including the hypervisor		
Provides automated, single-click, rolling upgrades of hypervisor and compute/storage layers with no VM down time, all from a single graphical user interface		
Includes system-wide data analytics to analyze resource usage over time and provide tools to monitor resource consumption, identify abnormal behavior, and guide resource planning		
HTML5 management tool/graphical user interface (GUI)		
All core management tasks must be able to be completed in the single management tool		
Provides a native, single management tool supporting ESXi, Hyper-V, KVM-based hypervisors and manage mixed hypervisor environments		
Interactive network topology diagram within the native HTML5 based management console		
Management tool deployment architecture must be highly available by design		
Management tool must be built into the distributed system, scales with the cluster, and does not require separate hardware infrastructure		
Management tool must provide Predictive Analysis and Capacity Optimization		
Cloud		
Ability to run the same hyper-converged software in the public cloud		
Includes Disaster Recovery replication between on-premise and public cloud systems using the native replication technology of the HCI software in the same single interface		

Ability to natively use AWS or AZURE as a target for long term data retention for backup, disaster recovery, and archival without relying on a separate backup software		
Security		
Provides a centralized security and auditing capability to easily assess the overall security posture by improving visibility, managing policy, validating compliance between data centers and cloud instances		
Able to perform platform security hardening by default, in code, instead of manually hardened after deployment		
Automatically and constantly keep infrastructure secure (STIG compliant) via automated checks and self-healing and logs all corrective changes for audit		
Supports multifactor authentication for management interface		
Able to perform logging and auditing of all administrative actions with a native mechanism to ensure log integrity		
Able to encrypt management traffic by default		
Support for Self Encrypting Drives		
Support software-based data at rest encryption		

NOTE: Please include all plan options available on additional tabs and insert any additional costs where applicable

Description	Quantity	Unit Price	Total Price	Comments
				(List hardware)
Hardware Subtotal			0	
				(List software)
Software Subtotal			0	
Licensing				
Subscription				(Note length of contract)
Licensing and subscription Subtotal			0	
Installation/Labour/Delivery etc.				(List any install/labour/delivery costs)
Installation/Labour Subtotal			0	
Travel and lodging				(List any T&L costs)
T&L Subtotal			0	
Project Management				(List any associated project management costs)
Training				(List any associated training costs)
Project Management and training Subtotal			0	
Other costs….				(List any other costs ie. Delivery, insurance, other overhead etc.)
Other Subtotal			0	
Total System Cost (CAD)			0	