CenturyLink®

SAP S/4HANA

Cross Comparison of Deployment Options

Impact on Costs & Business Operations

SAP S/4HANA Cross Comparison of Deployment Options:

Impact on Costs & Business Operations

	Private Cloud	Public Cloud	On-Premises
Total Cost of Ownership (TCO)	The total cost of ownership (TCO) is the sum of all direct and indirect costs associated with projects and services related to IT. The total cost of ownership (TCO) calculation for either on-premise or cloud (private or public) deployment needs to take into account the capital outlay, operating expenses such as ongoing maintenance costs, and indirect or hidden costs as a result of business downtime.		
Capex	• Aside from software license, the solution requires no other large capital outlay that could impact an organization's cash flow.	• Aside from software license, the solution requires no other large capital outlay that could impact an organization's cash flow.	• Capex costs – hardware and software, and all other startup costs related to facilities need to be accounted. • Other costs: –Time required to set up and configure hardware to meet SAP S/4HANA requirements. –Labor costs to include training – difficult to predict. • Large capital outlay with potential to impact organization's cash flow.
Opex	• Dedicated, single-tenant cloud computing model means more certainty over operating expenses • Shared-cost model –Enjoys economies of scale when purchasing hardware and software, shared facilities space, and other operating costs such as energy, internet, etc. Cost savings passed on to customers –Infrastructure (hardware, network and facility) security and certification costs are spread across all customers/ organizations, with savings passed on the customers.	• Operating expenses higher on a longer-term basis –Costs are incurred on pay-per-use basis when customer environment becomes increasingly complex. • Shared-cost model –Enjoys economies of scale when purchasing hardware and software, shared facilities space, and other operating costs such as energy, internet, etc. Cost savings passed on to customers. –Infrastructure (hardware, network and facility) security and certification costs are spread across all customers/ organizations, with savings passed on the customers.	• Ongoing operating costs difficult to manage due to changes in SAP HANA workloads –Variable costs can be difficult to determine due to various factors e.g., increases in energy and internet usage, upgrades and possible increases in IT headcount need to be determined. • No shared costs –No economies of scale; investments in infrastructure including facilities are considered fixed costs –Need to continually invest in security-related products, certifications and technologies to keep up with the ever-evolving security landscape.

Indirect costs:	• The key difference between cloud versus on-premises deployment is the overhead involved in managing on-premises installations.	• The key difference between cloud versus on-premises deployment is the overhead involved in managing on-premises installations.	• Need to take into account the management overheads as part of the TCO calculation.
Achieving IT Agility	IT agility is key to accelerating a company's digital transformation. Achieving IT agility enables faster time-to-market for new products and services, as well as faster time-to-value. The speed and efficiency with which IT can deliver on business demands is dependent on IT's alignment and collaboration with the lines-of-business (LOB) that they serve.		
Speed to provision	• Slower provisioning speed than public cloud as private cloud requires dedicated compute, hence more time to set up. –Dedicated servers and infrastructure with ability to scale fast without impacting performance	• Fastest for initial set up as it is based on leveraged compute environment.	• Slowest. –Resources need to be freed and sized up before any implementation can be conducted. –Need to install and configure hardware and software based on SAP S/4HANA's specifications. –Additional resources needed is dependent on organization's procurement budget and cycle.
Scalability and Customization	• Medium scalability, but combines the best of both the public and on-premises • Ability to support organizations with large instances. –Ability to manage large workload, but scalability dependent on how infrastructure and resources are set up and available. –IT infrastructure, architecture and software can be fully customized to meet business requirements.	• Scalability could be restricted –Limited by size of instances due to current limitation of cloud providers to support large HANA workloads –Inability to customize deployment especially in the areas of security and compliance to meet business requirements.	• Limited scalability due to fixed infrastructure; meeting SAP HANA workloads can be challenging. • Will need to purchase additional servers to scale; timing dependent on IT procurement cycle • Infrastructure, IT architecture and software can be fully customized to meet business requirements.
Security	Security is one of the top concerns of any organizations. As threats continuously evolve – both external and internal – there is no beginning and end to securing any organizations. Building a cyber-resilient organization is imperative. Finding cybersecurity expertise and talent has become the key challenge for many organizations.		

Responsibility	• 'Shared responsibility' framework available. –Private cloud provider and customer share responsibility for maintaining security, but roles and responsibilities need to be defined. –Organizations need to manage their data security and applications, including mission-critical ones.	• 'Shared responsibility' framework available. –Public cloud provider and customer share responsibility of maintaining security, but roles and responsibilities need to be defined. –Organizations need to manage their data security and applications, including mission-critical ones. Public cloud providers offer APIs for organization's developers to manage the applications and interact with their service. However, security and availability of cloud services depend on the security of the API. Weak APIs expose enterprises to security vulnerabilities.	• No 'Shared responsibility' framework available. –Organization is fully responsibility for securing the SAP S/4HANA deployment – hardware, software, data and applications including the physical facilities in which servers are hosted. • Challenge in recruiting and retaining top cybersecurity talent in-house.
Ability to secure SAP S/4HANA deployment	• Easiest to secure due to dedicated, single-tenanted model –Ability to customize security requirements to meet organization's needs –Constantly audited to meet security compliance industry standards –Provide customers with encryption keys to prevent insider threats Top cybersecurity talent employed by cloud providers	• Easier to secure than on-premises, less secure than private cloud due to multi-tenanted model –Constantly audited to meet security compliance industry standards –Provide customers with encryption keys to prevent insider threats –Top cybersecurity talent employed by cloud providers	• Hardest to secure • Difficult to staff IT with cybersecurity experts. –In-house IT personnel will need to keep pace with technological changes, cyber threats, and upgrades to applications – all increasingly challenging in a very dynamic cyber-threat environment.
Mandatory Requirements	Mandatory business requirements that can make or break the business are a set of "must haves" for organizations to function as a business. At the top of the list of conditions are compliance and regulatory considerations, and mitigation of business downtime.		
Compliance	The number of rules and regulations that an organization must adhere to has increased and will continue to grow. Compounded by this is the ever-changing nature of these regulations.		

Ability to meet compliance	• Shared-cost model available –More cost- and resource-effective for organizations –Easier to meet compliance as public cloud provider needs to meet compliance as well • Single-tenant model: Private cloud provider can customize audit –Compliance audits aligned to customer's needs –Organization have access to data center	• Shared-cost model available –More cost and resource effective for organizations –Easier to meet compliance as public cloud provider needs to meet compliance as well • Unable to customize audit –No access to data centers	• Organization solely responsible for compliance certification and costs • More difficult to meet compliance due to the resources needed to meet various industry and government related compliance • If organization operates in more than one country, organization needs to meet compliance imposed by other jurisdictions
Business Downtime	Businesses today, especially those born-in-the-cloud, demand an "always-on" seamless IT experience. Maintaining this experience is challenging due to software upgrades, data overloads, hardware and software issues and so forth.		
Service Level Agreements (SLAs)	• SLAs function to guarantee a higher level of performance and uptime. –Single-tenanted environment are typically used to support large complex environments without much impact on performance.	• SLAs function to guaranteed connectivity versus performance of the deployment –Multi-tenanted cloud environment can only provide a certain level of uptime. Public cloud emphasizes scalability at the expense of configurability –SAP S/4HANA workloads that require extremely high memory and throughput without experiencing performance issues can be challenging.	• Organizations can define SLAs with in-house IT, but SLAs are not implemented as stringently as compared to cloud providers.

Redundancies	• Cloud architecture enables continual uptime by mitigating downtime risks through complex network of international data centers with physical redundancy at the disk level within the servers of each center. –Redundancies are built in during their maintenance cycles as well. –Ability to build in redundancy with adoption of the N+1 redundancy model • Shared-resource model means that cloud providers can provision redundancies cheaper than on-premises • Private cloud single-tenanted architecture allows for customized configurations –Can provide dedicated resources that can be assigned for failover in the event of an outage.	• Cloud architecture enables continual uptime by mitigating downtime risks through complex network of international data centers with physical redundancy at the disk level within the servers of each center. –Redundancies are built in during their maintenance cycles as well. –Ability to build in redundancy with adoption of the N+1 redundancy model • Shared-resource model means that cloud providers can provision redundancies cheaper than on-premises.	• Difficult to compete with cloud providers in developing redundancy. • Expensive to purchase infrastructure to build the N+1 model; low ROI.
Managed Service Provider Engagement	The success of any business transformation is also highly dependent on post-migration support. To fully harness SAP S/4HANA's potential, organizations need the right IT skills and support structure to run their operations. Hence, it is important to evaluate current skill sets within the organization to determine if they meet the day-to-day needs of supporting the new environment. If not, and depending on your business priorities, work with a managed service provider (MSP). Engagement of MSPs differ across different cloud deployment options; MSPs also need to HANA-certified by SAP.		
One SLA Versus Multiple SLAs	• Only One SLA Needed: Working with a private cloud provider with SAP HANA operations support capabilities streamlines management and minimizes complexities. This is the most ideal scenario. **Note:** Not all private cloud providers are SAP HANA-certified.	Multiple SLAs: Need to manage public cloud provider and managed service provider(s)	• Multiple SLAs: Need to manage multiple vendors and managed service provider(s) • Infrastructure contract with customer, not with managed service provider, leads to issues with longer turnaround time. Customer needs to be more actively involved in incidence resolutions.

Expertise	• Single SLA for managed hosting services; cloud provider needs to be HANA-certified by SAP. –Managed hosting cloud provider owns both hardware infrastructure. –Less coordination between managed service provider and customer –Reliable and readily available expertise in managing day-to-day issues related to cloud computing, hardware infrastructure and networking, SAP S/4HANA deployment and other software configuration complexities.	• Need to use third-party managed service providers that are HANA-certified by SAP. • More coordination between public cloud provider and managed service provider. • Organization will need to dedicate IT staff to manage outsourced team.	• Need to reassign IT staff from day-to-day IT operations to implement and provide support for SAP S/4HANA 24/7 –Potentially affecting other parts of the company's business and IT operations. • Limited staff knowledge –Might not have the experience of implementing SAP S/4HANA and maintaining the system and various applications.

About CenturyLink

CenturyLink (NYSE: CTL) is the second largest U.S. communications provider to global enterprise customers. With customers in more than 60 countries and an intense focus on the customer experience, CenturyLink strives to be the world's best networking company by solving customers' increased demand for reliable and secure connections. The company also serves as its customers' trusted partner, helping them manage increased network and IT complexity and providing managed network and cyber security solutions that help protect their business.

Call +65 6768 8098 | **Click** centurylink.com | **Email** info@centurylink.com

CenturyLink®