Ten Things to Consider Before Jumping into the Cloud

Keeping these ten steps in mind will help organizations deliver even greater outcomes when looking for an efficient cloud-centric procurement process

1

Understand Why Cloud Computing is Different
The standardized commercial delivery model of cloud computing is fundamentally different from the traditional model for on-premises IT purchases. Understanding this difference can help you structure a more effective procurement model. IaaS cloud services eliminate the customer's need to own physical assets.

2

Plan Early to Extract the Full Benefit of the Cloud
A key element of a successful cloud strategy is the involvement of all key stakeholders at an early stage. Promoting a culture of innovation and educating staff on the benefits of the cloud and how to use cloud technology helps those with institutional knowledge understand the cloud.

3

Avoid Overly Prescriptive Requirements
Public sector stakeholders involved in cloud procurements should ask the right questions to solicit the best solutions. Successful cloud procurement strategies focus on application-level, performance-based requirements that prioritize workloads and outcomes.

4

Separate Cloud Infrastructure from Managed Services
There is a difference between procuring cloud infrastructure (IaaS) and procuring labor to utilize cloud infrastructure or managed services, such as Software as a Service (SaaS) cloud. Successful cloud procurements separate cloud infrastructure from "hands-on keyboard" services and labor, or other managed services purchases.

5

Incorporate a Utility Pricing Model
To realize the benefits of cloud computing you need to think beyond the commonly accepted approach of fixed-price contracting. To contract for the cloud in a manner that accounts for fluctuating demand, you need a contract that lets you pay for services as they are consumed.

6

Leverage Third-Party Accreditations for Security, Privacy and Auditing
Leveraging industry best practices regarding security, privacy, and auditing provides assurance that effective physical and logical security controls are in place. This prevents overly burdensome processes and duplicative approval workflows that are often unjustified by real risk and compliance needs.

7

Understand That Security is a Shared Responsibility
As cloud computing customers are building systems on a cloud infrastructure, the security and compliance responsibilities are shared between service providers and cloud consumers.

8

Design and Implement Cloud Data Governance
Organizations should retain full control and ownership over their data and choose the geographic locations in which to store their data, with CSP identity and access controls available to restrict access to customer infrastructure and data.

9

Specify Commercial Item Terms
Cloud computing should be purchased as a commercial item, and organizations should consider which terms and conditions are appropriate (and not appropriate) in this context.

10

Define Cloud Evaluation Criteria
Cloud evaluation criteria should focus on system performance requirements. Select the appropriate CSP from an established resource pool to take advantage of the cloud's elasticity, cost efficiencies, and rapid scalability.