10 Considerations for a Cloud Procurement

Anthony Kelly

Erick Trombley

David DeBrandt

Carina Veksler

January 2015

Purpose:

Cloud computing provides public sector organizations with rapid access to flexible and low-cost IT resources. Organizations can provision the right type and size of computing resources they need to power their newest bright ideas or operate their IT departments, removing the need for large investments in hardware. As part of this effort, cloud computing presents an opportunity to reevaluate existing procurement strategies in order to create a fast, flexible acquisition process that capitalizes on the full scale and flexibility of the cloud. The acquisition of cloud services is unlike most traditional technology acquisitions in the public sector, and procurement considerations should be a key element of the cloud acquisition process in order to reap the benefits of decreasing cloud costs, increasing performance through improved infrastructure, and enhanced functionality through system-wide innovation.

Below are ten procurement considerations that are key components of a broader public sector cloud strategy. These considerations are based on AWS's many years of experience in delivering large-scale, global infrastructure in a reliable and secure fashion.

1. 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 (procurement, legal, budget/finance, security, IT, and business leadership). This ensures that there is a clear understanding of how cloud adoption will influence existing practices. Organizations that have built successful cloud procurement strategies focus early on facilitating the rapid procurement of services, and on removing needless procurement complexity or irrelevant processes, which may serve as unnecessary barriers to fully realizing the benefits of the cloud. These barriers are discussed in more detail in the points below. Many traditional, commodity-based requirements, approaches, and terms are not relevant to a commercial item service such as cloud computing, and organizations should consider the unique nature of cloud computing when developing their procurement strategies.

2. Avoid Overly Prescriptive Requirements

Successful cloud procurement strategies focus on overall application-level, performance-based requirements. They do not dictate the specific methods, hardware, and equipment used to fulfill these requirements. Recognizing that cloud is procured as a commercial item (discussed below), acquisitions should leverage a Cloud Service Provider's (CSP's) established commercial best practices for data center operations. The procurement should not dictate the use of specific equipment or procedures (e.g., racks, server types, etc.). By stating requirements in commercial cloud industry-standard terminology and by permitting the use of commercial practices, customers will have access to the most innovative and cost-effective solution options.

3. Specify Commercial Item Terms

Cloud computing should be purchased as a commercial item. A CSP's unique terms and conditions are integral to realizing the benefits of the cloud, as utility-type cloud services

have value in operating at a massive scale, driving innovation and cost efficiencies. Customers should allow for evolving terms and conditions in order to benefit from dynamic service enhancements. Unnecessary restrictions or change consent requirements can limit the ability to both scale and take advantage of frequent innovative service changes. Consider whether each term and condition is relevant to procuring a commercial item, and remove unnecessary requirements that could potentially impede the ability to take advantage of the cloud's scalability and on-demand delivery.

4. Understand Different Cloud Models

There are different cloud service models available, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), and there are different approaches to procuring, managing, pricing, and securing each of them. It is imperative that organizations take into account these different cloud models and create acquisition approaches for each model. Information and internationally accepted standards on these and other cloud service types can be found on the National Institutes of Standards and Technology (NIST) website: http://www.nist.gov/itl/cloud/.

5. Separate Cloud Infrastructure (i.e., Unmanaged Services) from Managed Services

Successful cloud acquisitions separate the purchase of cloud infrastructure from the purchase of related services and labor for planning, developing, executing, and maintaining cloud migrations and workloads. This separation promotes maximum pricing efficiencies.

6. Incorporate a Utility Pricing Model

Realizing the benefits of cloud computing requires thinking beyond the commonly accepted approach of fixed-price contracting, and building an acquisition model for the on-demand, utility-style, pay-as-you-go nature of cloud computing. To contract for the cloud in a manner that accounts for fluctuating demand, customers need a contract that lets them pay for services as they are consumed. CSP pricing should be:

- Offered via a pay-as-you-go utility model, where at the end of each month customers simply pay for their usage.
- Allowed the flexibility to fluctuate based on market pricing so that customers can take advantage of the dynamic and competitive nature of cloud pricing.

Allowing CSPs to offer different pricing models enables customers to evaluate each pricing model against the requirements of their solicitations, as opposed to an "apples to apples" pricing comparison through arbitrary compute or storage units. CSPs should provide transparent, publicly available, up-to-date pricing, and tools that allow customers to evaluate their pricing, such as AWS's Simple Monthly Calculator: http://aws.amazon.com/calculator. Additionally, CSPs should provide customers with the tools to generate detailed and customizable billing reports to meet customer business and compliance needs.

7. 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, preventing overly burdensome processes or approval workflows that are not justified by real risk and compliance needs. There are many security frameworks, best practices, audit standards, and standardized controls that cloud solicitations can cite, such as: Federal Risk and Authorization Management Program (FedRAMP), Service Organization Controls (SOC) 1/Statement on Standards for Attestation Engagements (SSAE) 16/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70), SOC 2, SOC 3, Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization (ISO) 27001, ISO 9001, Department of Defense Risk Management Framework (DoD RMF, Cloud Security Model), Federal Information Security Management Act (FISMA), International Traffic in Arms Regulations (ITAR), and Federal Information Processing Standard (FIPS) 140-2.

8. Understand That Security is a Shared Responsibility

As cloud computing customers are building systems on top of cloud infrastructure, the security and compliance responsibilities are shared between service providers and cloud consumers. In an IaaS model, customers control how they architect and secure their applications and data put on the infrastructure, while CSPs are responsible for providing services on a highly secure and controlled platform and for providing a wide array of additional security features. The respective responsibilities of the CSP and the customer depend on the cloud deployment model (discussed in point 4 above), and customers should be clear as to their responsibilities in each model.

9. Design and Implement Cloud Data Governance

Cloud customers should retain full control and ownership over their data and have the ability to choose the geographic location(s) in which to store their data, with CSP identity and access controls available to restrict access to customer infrastructure and data. CSPs should provide customers with a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity. A major benefit of cloud computing as compared to traditional IT infrastructure is that customers have the flexibility to avoid traditional vendor lock-in, and CSPs should allow customers to move data on and off of their cloud platforms as needed.

10. Define Cloud Evaluation Criteria

Cloud evaluation criteria should focus on system performance requirements, with the appropriate CSP selected from an established resource pool in order to take advantage of the cloud's elasticity, cost efficiencies, and rapid scalability. This approach ensures that customers are getting the best cloud services to meet their needs, the best value in these services, and the ability to take advantage of market-driven innovation. The NIST definitions of cloud benefits are an excellent starting point

when determining cloud evaluation criteria: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.

When working with AWS, you can quickly launch services using an efficient procurement process. Keeping these ten steps in mind will help deliver more mission for the money.