This version has been archived.

10 Considerations for a Cloud Procurement

March 2017

For the most recent version of this paper, see:

https://docs.aws.amazon.com/whitepapers/latest/considerations-for-cloud-procurement/considerations-for-cloud-procurement.html

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Purpose

Amazon Web Services (AWS) offers scalable, cost-efficient cloud services that public sector customers can use to meet mandates, reduce costs, drive efficiencies, and accelerate innovation.

The procurement of an infrastructure as a service (IaaS) cloud is unlike traditional technology purchasing. Traditional public sector procurement and contracting approaches that are designed to purchase products, such as hardware and related software, can be inconsistent with cloud services (like IaaS). A failure to modernize contracting and procurement approaches can reduce the pool of competitors and inhibit customer ability to adopt and leverage cloud technology.

Ten Procurement Considerations

Cloud procurement presents an opportunity to reevaluate existing procurement strategies so you can create a flexible acquisition process that enables your public sector organization to extract the full benefits of the cloud. The following procurement considerations are key components that can form the basis of a broader public sector cloud procurement strategy.

1. Understand Why Cloud Computing is Different

Hyper-scale Cloud Service Providers (CSPs) offer commercial cloud services at massive scale and in the same way to all customers. Customers tap into standardized commercial services on demand. They pay only for what they use.

The standardized commercial delivery model of cloud computing is fundamentally different from the traditional model for on-premises IT purchases (which has a high degree of customization and might not be a commercial item). Understanding this difference can help you structure a more effective procurement model. IaaS cloud services eliminate the customer's need to own physical assets. There is an ongoing shift away from physical asset ownership toward on-demand utility-style infrastructure services. Public sector entities should understand how standardized utility-style services are budgeted for, procured, and used and then build a cloud procurement strategy that is

intentionally different from traditional IT—designed to harness the benefits of the cloud delivery model.

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 (procurement, legal, budget/finance, security, IT, and business leadership) at an early stage. This involvement ensures that the stakeholders can understand how cloud adoption will influence existing practices. It provides an opportunity to reset expectations for budgeting for IT, risk management, security controls, and compliance. 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. It also helps to accelerate buy-in during the cloud adoption journey.

3. Avoid Overly Prescriptive Requirements

Public sector stakeholders involved in cloud procurements should ask the right questions in order to solicit the best solutions. In a cloud model, physical assets are not purchased, so traditional data center procurement requirements are no longer relevant. Continuing to recycle data center questions will inevitably lead to data center solutions, which might result in CSPs being unable to bid, or worse, lead to poorly designed contracts that hinder public sector customers from leveraging the capabilities and benefits of the cloud.

Successful cloud procurement strategies focus on application-level, performance-based requirements that prioritize workloads and outcomes, rather than dictating the underlying methods, infrastructure, or hardware used to achieve performance requirements. Customers can leverage a CSP's established best practices for data center operations because the CSP has the depth of expertise and experience in offering secure, hyper-scale, IaaS cloud services. It is not necessary to dictate customized specifications for equipment, operations, and procedures (e.g., racks, server types, and distances between data centers). By leveraging commercial cloud industry standards and best practices (including industry-recognized accreditations and certifications), customers avoid placing unnecessary restrictions on the services they can use and ensure access to innovative and cost-effective cloud solutions.

4. Separate Cloud Infrastructure (Unmanaged Services) 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. Cloud infrastructure and services, such as labor for planning, developing, executing, and maintaining cloud migrations and workloads, can be provided by CSP partners (or other third parties) as one comprehensive solution. However, cloud infrastructure should be regarded as a separate "service" with distinct roles and responsibilities, service level agreements (SLAs), and terms and conditions.

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.

CSP pricing should be:

- Offered using 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 pay-as-you-go pricing or flexible pay-per-use pricing gives customers the opportunity to evaluate what the cost of the usage will be instead of having to guess their future needs and over procure. CSPs should provide publicly available, up-to-date pricing and tools that allow customers to evaluate their pricing, such as the AWS 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 business and compliance needs.

CSPs should also provide features that enable customers to analyze cloud usage and spending so that customers can build in alerts to notify them when they approach their usage thresholds and projected/budgeted spend. Such alerts enable organizations to determine whether to reduce usage to avoid overages or prepare additional funding to cover costs that exceed their projected budget.

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. There are many security frameworks, best practices, audit standards, and standardized controls that cloud solicitations can cite, such as the following:

- Federal Risk and Authorization Management Program (FedRAMP)
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 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 27017, ISO 27108, ISO 9001
- Department of Defense (DoD) Security Requirements Guide (SRG)
- Federal Information Security Management Act (FISMA)
- International Traffic in Arms Regulations (ITAR)
- Family Educational Rights and Privacy Act (FERPA)
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)
- Federal Information Processing Standard (FIPS) 140-2

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. In an IaaS model, customers control both how they architect and secure their applications and the data they put on the infrastructure. CSPs are responsible for providing services through a highly secure and controlled infrastructure 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 that is used, either IaaS, SaaS, or Platform as a Service (PaaS).Customers should clearly understand their security responsibilities in each cloud model.

8. Design and Implement Cloud Data Governance

Organizations should retain full control and ownership over their data and have the ability to 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. Customers should clearly understand their responsibilities regarding how they store, manage, protect, and encrypt their data. A major benefit of cloud computing as compared to traditional IT infrastructure is that customers have the flexibility to avoid traditional vendor lock-in. Cloud customers are not buying physical assets, and CSPs provide the ability to move up and down the IT stack as needed, with greater portability and interoperability than the old IT paradigm. Public sector entities should require that CSPs: 1) provide access to cloud portability tools and services that enable customers to move data on and off their cloud infrastructure as needed, and 2) have no required minimum commitments or required long-term contracts.

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. A commercial item is recognized as an item that is of a type that has been sold, leased, licensed, or otherwise offered for sale to the general public and generally performs the same for all users/customers, both commercial and government. IaaS CSP terms and conditions are designed to reflect how a cloud services model functions (i.e., physical assets are not being

purchased, and CSPs operate at massive scale to offer standardized commercial services). It is critical that a CSP's terms and conditions are incorporated and utilized to the fullest extent.

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. This approach ensures that you get the best cloud services to meet your needs, the best value in these services, and the ability to take advantage of market-driven innovation. The National Institute of Standards and Technology (NIST) definitions of cloud benefits are an excellent starting point to use for determining cloud evaluation criteria: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf.

Conclusion

Thousands of public sector customers use AWS to quickly launch services using an efficient cloud-centric procurement process. Keeping these ten steps in mind will help organizations deliver even greater citizen-, student-, and mission-focused outcomes.