GSA White Paper

Best Practices for Effective Cloud Computing Services Procurement within the Federal Government

Basic Steps for Public Sector Organizations

General Services Administration

Federal Acquisition Services

Office of Integrated Technology Services

Cloud Computing Services Program Management Office
(GSA FAS ITS CCS PMO)

January 2016

Contents

Cloud Procurement in the Public Sector

This paper provides public sector organizations guidance on addressing common challenges with cloud computing services procurement and will reflect alignment with the Federal Government's "Cloud First" policy per the *Federal Cloud Computing Strategy.*[1] Guidance presented in this document is not intended to be prescriptive but to serve as supplemental, as use cases can be quite diverse in regards to purchasing cloud services. For the purpose of illustration this white paper considers a notional cloud acquisition lifecycle approach that reflects common acquisition practice.

Lessons learned from an introductory small but end-to-end implementation or pilot have been cited repeatedly by agencies such as NASA[2] for their usefulness. For example, system integration challenges and legal, security and regulatory compliance issues are important and might be reasonably anticipated; however, for an enterprise level program there are often cultural impacts relating to how cloud services will be consumed. Thus, lessons learned following an iterative cloud adoption approach can help shape a successful program.

While what constitutes a "cloud service" is subject for debate, especially among industry providers, the Federal government generally adopts the cloud computing definition provided by NIST in SP 800-145.[3] The essential characteristics in this definition are:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

To ensure the benefits of cloud computing are fully realized and to protect against vendor "cloud-washing" (i.e., overstating the application of cloud services) it is recommended that prospective buyers seek to ensure cloud services meet these five essential characteristics as defined. Typically, this is achieved by evaluating potential services for adherence to these characteristics in the resulting solicitation.

Proactive planning with all necessary organization stakeholders, including chief information officers (CIO), general counsels, privacy officers, records managers, e-discovery counsels, Freedom of Information Act (FOIA) officers, and of course procurement staff, will be essential when planning, evaluating and procuring cloud computing services. Planning and executing this stakeholder engagement will be very helpful throughout the procurement process.

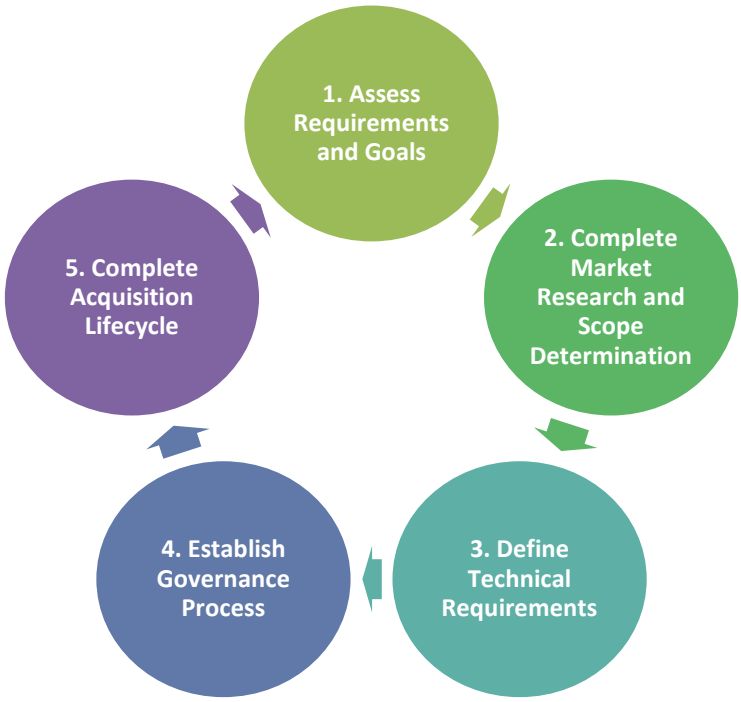
---

[1] Federal Cloud Computing Strategy (PDF)
[2] NASA presentation at NIST Cloud Computing Forum VIII (PDF)
[3] The NIST Definition of Cloud Computing, SP 800-145 (PDF)

Cloud Acquisition Lifecycle

The cloud acquisition lifecycle as depicted in figure 1 below is developed from the customer perspective and can be applied to both enterprise and project level acquisitions. This document aims to provide guidance for succeeding in each phase as further detailed throughout the document.

Figure 1: Notional Cloud Acquisition Lifecycle



1. Assess Requirements and Goals

A key opening step in any Information Technology (IT) service acquisition, and especially for cloud services, is defining the scope of the overall project. One factor that can impact scope and affect the value proposition is whether the service, system or program exists "on premise" and is migrating to the cloud or is being built new in the cloud. For existing on premise systems, customers should consider if the system should or can be moved as-is to the cloud and what level of application changes are either required or warranted when doing so.

Also important is documentation of the fundamental reasons for moving to the cloud. Ultimately, as with any project, it is important to clearly identify the desired outcomes and goals for the effort to ensure the scope is identified fully and accurately. Understanding these motives is essential to driving toward overall outcome and goal achievement.

To provide a succinct, comprehensive scope and high level requirements, the buying office should always consider the following elements:

- Alignment to the enterprise mission

- Size of the anticipated effort
- Specific need requiring cloud services
- Expected results/outcomes
- Summary of actions to be performed by project personnel versus contractor and/or cloud service provider (CSP)
- Stakeholders utilizing cloud services
- Security, regulatory, and legal requirements

Public sector organizations will benefit from engaging an appropriate procurement official such as an agency contracting officer (CO) early in the process to help the program office avoid any acquisition pitfalls that can occur later in the process. Establishing this relationship will help support scope determination and subsequent procurement.

2. Complete Market Research and Scope Determination

Market research is performed to identify potential cloud solutions and vendors that may meet the enterprise or project's needs. Commercial Cloud Service Providers (CSPs) have generally standardized their own service offerings and buyer requirements may require "layered services" - additional support or customization. These layered services can be provided by professional services built on top of the native CSP offering by a systems integrator, thus in effect becoming a managed service.

For a Federal agency, the General Services Administration's (GSA's) *IT Schedule 70*[4] features a Cloud Special Item Number (SIN) 132-40 that identifies vendors and their cloud services that are available for use by Federal Government as well as state, local and tribal authorities. These services are provided by vendors that have gone through a compliance review against NIST cloud characteristics and have agreed to a common definition of cloud services, service models, and deployment models. GSA IT Schedule 70 pricing and the associated terms and conditions that are publicly available via GSA Advantage[5], and GSA e-Library[6] can be valuable aids to market research efforts beyond commercial vendor websites.

The agency may also want to engage with vendors directly and early in the market research process. Speaking to vendors can help clarify scope and guide discussions to support cost benefit tradeoffs and better understand the approaches of other agencies facing similar challenges. This outreach can also help ensure vendor engagement and interest when an agency decides to issue a Request For Information (RFI). RFI's are issued by customers to gain additional information based on interest from the enterprise and can serve a useful purpose in

[4] http://www.gsa.gov/portal/content/104506
[5] https://www.gsaadvantage.gov/
[6] http://www.gsaelibrary.gsa.gov/

larger procurements, providing advanced advertising to vendors of the pending procurement. Some examples of RFI's include gathering additional technical specifications on cloud solutions, cloud technical implementation approaches, and contracting strategies.

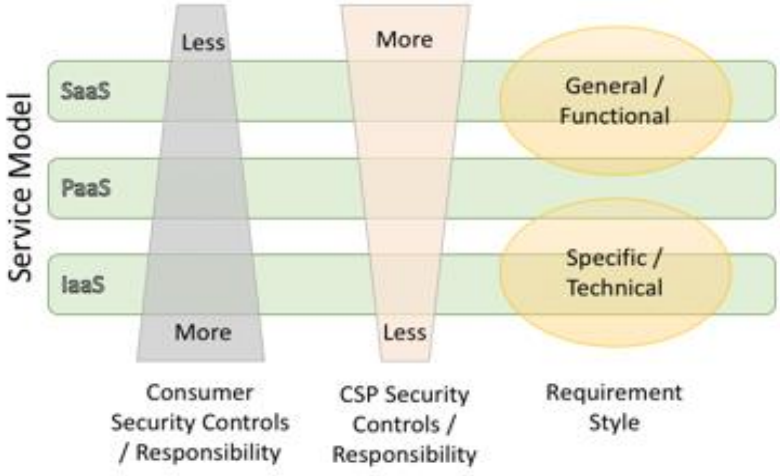
Depending on the jurisdiction and scope of the project there can be opportunities to leverage economies of scale through a joint procurement consolidating needs from multiple sources, either within a single agency or across entities.

Lastly, in supporting market research for cloud services it is often possible to obtain free trials from vendors or even purchase a modest scale of services for a nominal investment, allowing technical teams to test various products and positively inform scope determination and requirement development.

3. Define Technical Requirements

Cloud solutions can be complex but some generalizations can be described based on the cloud service model applicable for the circumstances. As described in Figure 2 below, each cloud service model presents unique functionality with agency security controls and responsibilities decreasing as you move from infrastructure to platform to software. Similarly, the specificity and style of some types of requirements will change from very specific and technical to more general and functional in nature. Additional information and detail on the entities and functional roles in a cloud environment can be found within the NIST Cloud Computing Reference Architecture.[7]

Figure 2: Cloud Service Models and Trends



In order to ensure vendors bidding on the solicitation fully understand the procurement, careful attention needs to be paid to defining the roles and responsibilities for activities within scope of the contract. IT systems often involve multiple stakeholders and the interface of work between

[7] NIST Cloud Computing Reference Architecture (PDF)

parties needs to be well defined so the activities performed by the soliciting agency are differentiated from those to be performed by the contractor. The boundaries of responsibility should be clearly documented to minimize the number of questions received from contractors when responding to the solicitation and more importantly ensure the vendors are bidding on the desired scope of work so the solicitation is successful.

A clear advantage of cloud computing is scalability. Cloud elasticity—the ability to scale resource delivery up and down rapidly—is an important feature and contractors need to fully understand customer operating conditions and expectations to provide realistic proposals. Requirements should include consideration for normal and surge operating conditions. When specifying as-is and to-be estimates of operating conditions and capacity estimates, the following types of metrics should be considered for specification when applicable:

- Total utilization
- Average utilization
- Peak utilization
- Frequency of peak utilization occurrence
- Duration in time for an increase from average to peak utilization

Security Requirements

The security of the system is always of concern. Any program should refer to its internal security polices and controls as well as the overarching state, local or federal security requirements for information systems. This may require working with the staff of the Chief Information Security Officer (CISO) or equivalent component to perform a security assessment and issue an authority to operate the cloud system.

In the Federal sector, IT security requirements for systems are governed by the Federal Information Security Management Act[8] (FISMA). While NIST publications provide standards and guidance for FISMA, they do not specifically address cloud computing. GSA launched FedRAMP[9] (Federal Risk and Authorization Management Program) to provide a standardized approach to cloud security featuring a "do once and reuse many times" model to ensure FISMA compliance of cloud systems used by the government. Even if FedRAMP does not apply to a customer's particular public agency, the program publicly provides extensive security program details including guidelines, security controls, and security related standard contract clauses.

Key cloud security considerations that must be addressed include data residency and data ownership. Statutes and/or policies can specify and control where government or agency or

[8] http://www.dhs.gov/fisma
[9] http://www.fedramp.gov/

even specific program data can be stored. The automation built into cloud computing can easily result in data redundancy: data being copied to multiple data centers spanning multiple legal jurisdictions in order to ensure it is protected against loss. Similarly, procurement documents must address data ownership by specifying that all government data entered in the system remains the property of the government. This can often also be extended to include related CSP system log and audit file data related to the government accounts.

When consuming cloud services it is important for Federal agencies to understand what types of data they will be placing in the cloud to ensure the procurement documents include all appropriate security requirements. One example is Personally Identifiable Information (PII) which requires specific additional security controls.

The data types in the system combined with agency policies can also affect the available deployment models. Generally, however, in the absence of specific policy the deployment model need not be specified in the procurement since the goal is to meet and ensure security compliance with appropriate FISMA and FedRAMP policy and controls.

Service Level Agreements

Service Level Agreements (SLAs) are agreements under the umbrella of the overall cloud computing contract between a CSP and the organization for which services are provided. SLAs define acceptable service levels to be provided by the CSP to its customers in measurable terms. The definition, measurement and enforcement of the performance parameters specified in SLAs varies widely among CSPs. Federal agencies should ensure that CSP performance is clearly specified in all SLAs and that all such agreements are fully incorporated, either by full text or by reference, into the CSP contract.

One important element to understand in cloud computing SLA definitions is that a CSP's performance for its service as delivered may not directly correspond to the cloud outcome sought. An example of this would be Infrastructure as a Service [IaaS] hosting availability for virtual machines versus availability of your agency application as whole system. The CSP's virtual machine service may support a particular uptime percentage while the application hosted on those virtual machines can be different based on internal design and architecture.

This is another example of the transition to increasing levels of managed services. Metrics applicable to managed services that can be used as SLA's include service level objectives (SLOs) such as the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These often apply to application and service hosting scenarios. In relation to SLAs, understanding and defining of the following is recommended:

- Terms of conditions

- Measures – including definitions for any measurements and related calculations
- Enforcement mechanisms

Often for a CSP's standard offerings there will be little to no leverage for an organization to negotiate changes to CSP's standard SLA terms except for on the largest of contracts. However, as requirements move towards managed service offerings and are fulfilled by system integrators, these elements can be specified and negotiated with the impacts upon cost to deliver increasingly customized requirements. Care should be applied to understanding the cost benefit trade-offs in contracting approaches to ensure public sector organization goals are achieved at reasonable cost.

Termination and Moving to a New Vendor

Another important consideration for cloud procurement is planning from the very beginning for how the contract will terminate and services will be moved to another vendor. This may involve detailed determinations regarding, among other considerations: cessation of service, extraction of data, format(s) for the extracted data, sending the data to a new provider, and restarting key services on the new provider's platform. Building termination and migration requirements in advance will ensure that you are adequately prepared to transition the contract and associated services if/when necessary.

4. Establish Governance Processes

Successful program governance is a result of iteration with periodic performance reviews to assess and implement incremental corrections to governance processes. In cases where existing governance structures are not yet in place, process development need not be perfect from the outset but must be repeated and exercised to ensure the opportunity to refine the process exists.

To fully realize the economic benefits of cloud services, customers can expect costs to vary over time since they only pay for cloud IT services actually consumed and needed. This sometimes presents unique challenges for public entities based on established budgeting processes. Financial monitoring of these variable costs will need to be planned. Similarly, the performance and SLOs identified in the requirements will need to be collected and reviewed. The high level processes to implement monitoring of artifacts should be planned and established prior to implementation to ensure smooth operations and avoid unnecessary surprises.

5. Complete Acquisition Lifecycle

Once the program has established the scope, requirements, and as appropriate selected the contract vehicle, the program will develop the full solicitation. Contract templates can be very useful in these cases to ensure alignment to specific requirements of the contract vehicle and

provide additional guidance. Various existing GSA contract vehicles including Alliant[10], the EaaS BPA[11] and other agency vehicles publicly provide solicitation templates through their websites.

The evaluation criteria for vendor proposals also need to be established and considered during solicitation development. When possible, utilizing contracting vehicles that have pre-vetted requirements identified, such as NIST cloud computing characteristics, will remove or ease the need for teams to evaluate the vendor proposals for those features. This may simplify and shorten the overall acquisition process.

Another element of solicitation development with particular cloud impact is the identification, inclusion, and integration of all relevant terms and conditions. These can originate from statutory sources, the contract vehicles or authorities to be employed, and agency specific regulations, and should be considered in the context of the commercial standard terms that vendors typically provide. Usually, vendors that regularly do business with government entities have adopted appropriate and specific government terms for their public sector contracts, but in the cloud computing space the rush for innovation often brings vendors to the market that are unfamiliar with government contracting practices.

Once the program receives the responses, it will need to evaluate each vendor's technical response against the technical evaluation criteria previously developed. This source selection process needs to rate each proposal fairly to determine the best proposal submission. Once the evaluation and scoring is complete, the award is made and officially announced.

As outlined in this paper, cloud services can introduce new challenges to IT procurements. As with any project, a combination of key issue awareness, advance preparation, and collaboration with appropriate stakeholders will provide a path to cloud success.

Additional Resources

- Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service
- The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative
- Innovative Contracting Case Studies

Contact Information

To learn more, please visit the GSA Cloud Computing Services Program Management Office at www.gsa.gov/cloud or email CloudPMO@gsa.gov.

[10] http://www.gsa.gov/alliant
[11] http://www.gsa.gov/eaas

For more great resources like this, visit the Acquisition Gateway via the following link: http://go.usa.gov/x3YYP. http://go.usa.gov/x3YYP