Cloud Computing Services Program Management Office
Federal Acquisition Service

General Services Administration

Best Business Practices

for

USG Cloud Adoption

September 2016

Table of Contents

Purpose

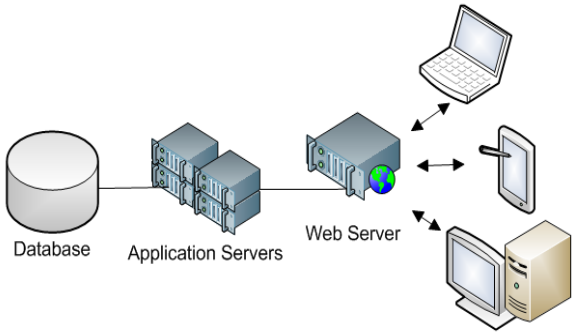
This guide provides an overview of business practices for federal agencies to consider when preparing for a migration to the Cloud. It provides Program Managers (PMs) with actionable guidance for the planning and solicitation of their products or services through a Systems Integrator (SI) into an environment hosted by a Cloud Service Provider (CSP). Being a PM is a privilege, and as such, you must constantly think about how each activity or event impacts your program baseline. Successfully accomplishing this requires the use of innovative strategies to meet changing budgetary realities while remaining responsive to the needs of your mission partners. To assist the PM in planning the transition earlier in the program lifecycle and to successfully execute transition to a CSP, this guide documents best practices and lessons learned along with suggested processes. Additionally, it is crucial to your program's success to collaboratively engage your stakeholders throughout the acquisition lifecycle to improve IT capability delivery and Mission Partner satisfaction. Considerations for planning a migration to the Cloud include:

- Knowing your current architecture and developing a technology program/project schedule.
- Developing a plan to migrate products and/or services to the cloud to include capacity management, performance metrics, and historical contractual costs.
- Service Level Agreements (SLA)

Background

System automation has remained at the core of the Federal Government Information Technology (IT) infrastructure for decades. From the Hollerith mechanical tabulator (1890 Census Bureau) to the Army's first programmable digital computer, the ENIAC, there has been a constant evolution to perform quickly and more efficiently with the use of computer technology.

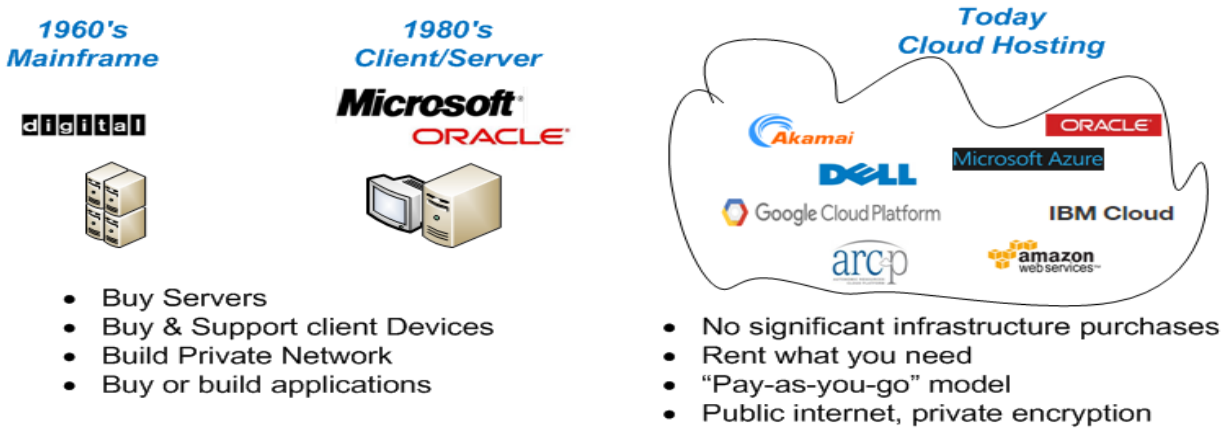
National Aeronautics and Space Administration (NASA) grasped the incredible power of IT in the 1960's with the space program and the advent of mainframe server farms and data centers. NASA even developed one of the first notebook style computers for the 1985 space shuttle mission. Data centers consisting of mainframe computers, later known as servers, were not only crucial in the Federal Government, but also corporate and educational environments.



The expansion of personal computing, data center management, and software applications led to the evolution of overly expensive infrastructure within the Federal Government during the 1990's.

Knowledge Management: In the early 2000's, VMware created virtualization of servers to reduce the infrastructure footprint. Through virtualization, agencies minimized the infrastructure from thousands of servers to approximately two hundred. The military services then initiated programs such as Knowledge Management (KM) to increase the sharing of knowledge, leveraging the internet, and provide near-ubiquitous access to information no matter where a person is geographically located in the world. KM was a successful evolution for the reduction of servers, loss of intellectual data as a result of personal computing, and overhead burden of the vastly dispersed data centers. Each service maintains its own version of KM (Air Force Knowledge Online, Army Knowledge Online, Joint Knowledge Online, etc.). The transition to KM within DoD was the initial attempt to deliver what we call "Cloud Computing" today, but it was not enough. Not only was the data center becoming overly expensive to manage, the threat of malware, or malicious coding, increased data center operational costs astronomically.

By 2010, the Office of Management and Budget (OMB) implemented the Data Center Consolidation Initiative to reduce costs, eliminate redundant applications, and optimize the vast amounts of data centers dispersed globally. In 2011, OMB initiated the "Cloud First Policy" to enable scalability and use only the resources that are required to compute data. Today, this evolutionary change in IT has changed the landscape in how we use IT resources and is the impetus for this guide.



Hosting Methods: Then and Now – Moving from Mainframe to Cloud Architecture

What Is This Cloud Computing Stuff?

Cloud computing, or the cloud, is the access of information through the internet from a third party provider. Users have been using this infrastructure model from a commercial perspective going back to the days of America Online (AOL). Today, the landscape is so diverse with CSPs such as Google, Microsoft, Amazon Web Services (AWS), Autonomic Resources, Oracle, VMware, and many others.

Essentially, cloud allows agencies to rent the computing resources it requires, rather than modify a "brick and mortar" establishment, build the infrastructure, employ IT personnel, and operate and maintain the data center. To further enhance the cloud basics, the National Institute of Standards and Technology (NIST), defines the essential characteristics of cloud computing in the below table:

Essential Characteristic	Description
On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically, without requiring human interaction with each service provider.

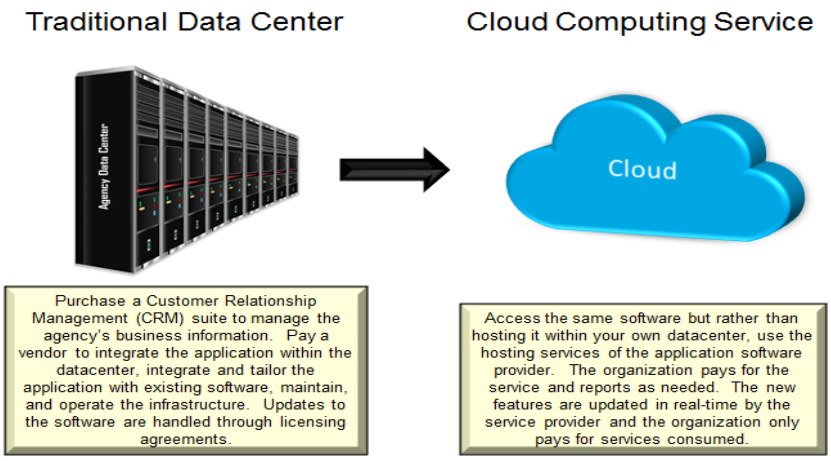
Essential Characteristic	Description
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

NIST Essential Characteristics of Cloud Computing

NIST's Essential Characteristics of Cloud Computing – is a link to NIST Special Publication 800-145 explaining the essential characteristics what IT services are considered cloud computing.

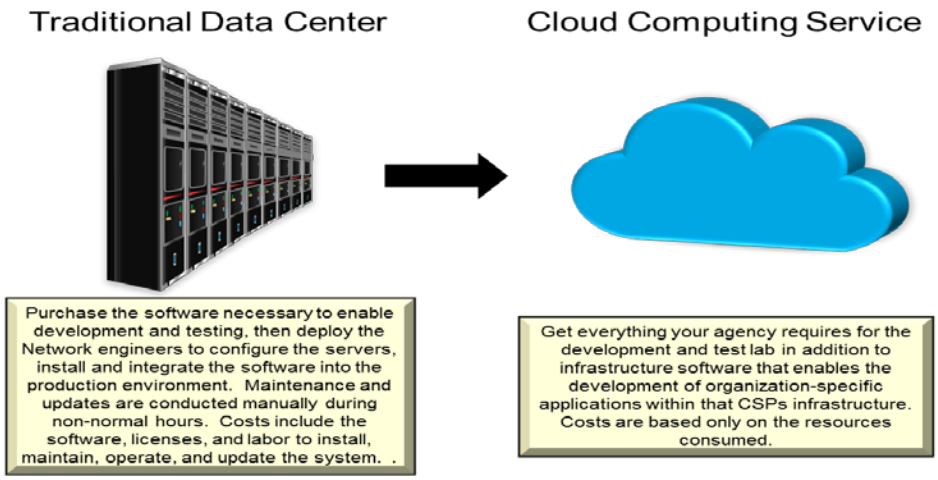
NIST further defined three (3) delivery models for Cloud Computing:

1. ***Software as a Service (SaaS).*** The capability is provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. With the possible exception of limited user-specific application configuration settings, the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities.



Software as a Service Delivery Model

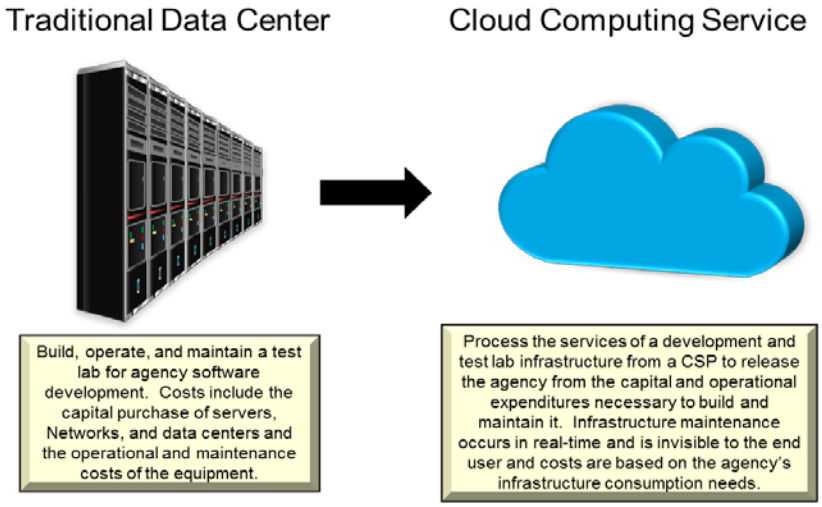
2. ***Platform as a Service (PaaS).*** The capability is provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.



Platform as a Service Delivery Model

3. ***Infrastructure as a Service (IaaS).*** The capability is provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the

underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).



Infrastructure as a Service Delivery Model

The following are the four (4) deployment models as defined by NIST:

Model	Cloud Infrastructure Is	Managed by	Location
Private cloud	Provisioned for exclusive use by a single organization comprising multiple consumers (for example, business units, etc.).	Owned, managed, and operated by the organization.	On or Off premises
Community cloud	Provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).	May be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination.	On or Off Premises
Public cloud	Provisioned for open use by the general public.	Owned, managed, and operated by a business, academic, or government organization, or a combined organization.	On the premises of the cloud provider.
Hybrid Cloud	Composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.	Each infrastructure may be owned, managed, and operated by one or more of the organizations involved.	On or Off Premises

NIST Cloud Deployment Models

Your Agency Is Directed To Move To The Cloud, Now What?

There are so many areas to consider when adopting cloud computing hosting. The challenge is to determine where to begin. It seems relatively simple to understand the service and deployment models, but the overall strategy is much more comprehensive. To address some of these concerns, this section provides recommendations that agencies can consider to facilitate a better decision-making process and determine their unique business case (depending on mission requirements) and maximize cloud hosting benefits.

The following are the suggested steps to take as part of moving to the cloud computing environment[1]:

1. Determine the reasons for migrating or placing systems in the cloud. These can be to:

    - Reduce infrastructure costs,
    - Improve security,
    - Meet CIO mandate, etc.

2. After one or many reasons have been identified and it is determined that it appears to be advantageous to migrate to the cloud, an evaluation needs to be conducted to include:

    - Cost benefit analysis,
    - Comparative performance analysis, and
    - Metrics established for expected performance advantages.

Contingency, technical and security analyses need to be completed to determine expectations and scenario planning once the applications or systems are hosted in the cloud.

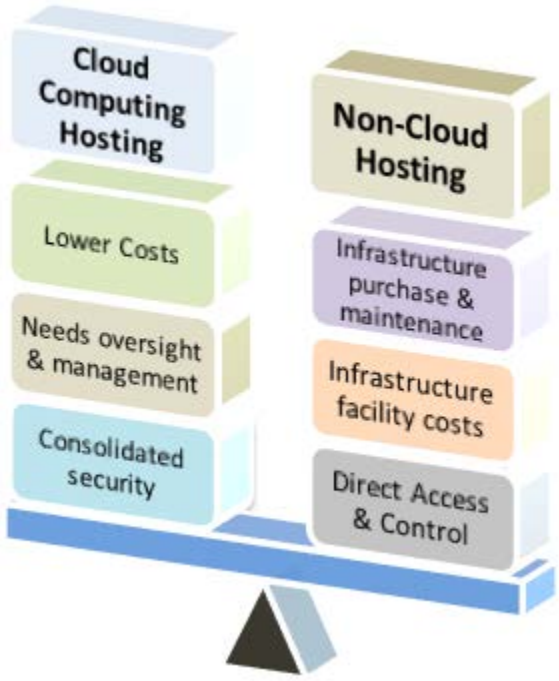
Depending upon your agency's prior experience, it may turn out to be that initial requirements gathering/planning, system customization, administration and migration services are needed in moving to the cloud. It is recommended to have this training also be provided to current federal System Administrators and IT professionals so that they can manage cloud hosting entirely on their own subsequently while working with the SI's/CSP's during the initial phase.

---

[1] Also see: US Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements to Further USG Agency Cloud Computing Adoption. The following web link may be used to view the roadmap: US Government Cloud Computing Technology Roadmap, Volume I

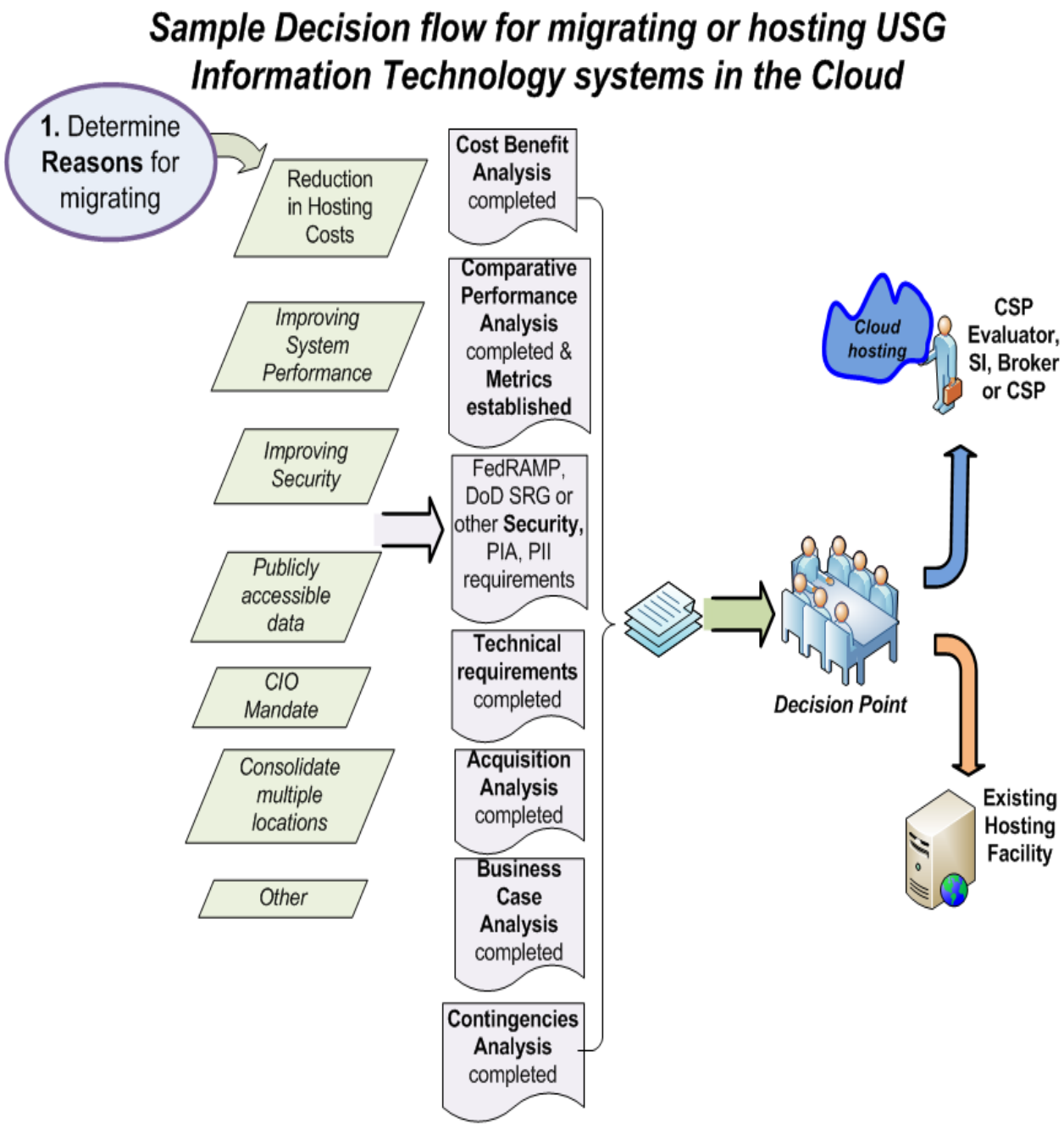
3. After collecting the above from step and any other rationale or information specific to the agency, a decision point has to be made by the appropriate Agency Executives with input from Subject Matter Experts.

4. A decision is then made to either move to the cloud (if it is more advantageous in terms of reduced costs, improved security and cloud hosting offers a better overall Return on Investment (ROI) than other hosting options, etc.). However, if the application/system is deemed to be managed in an environment other than cloud due to specific attributes, then it should remain hosted in its current environment, or other non-cloud options as needed.



Comparing all the options

It is important to thoroughly consider all pros and cons of each option before deciding to migrate to the cloud. The following is a sample decision flow process and includes potential areas to consider before moving to the cloud.



Sample Decision Flow Process.

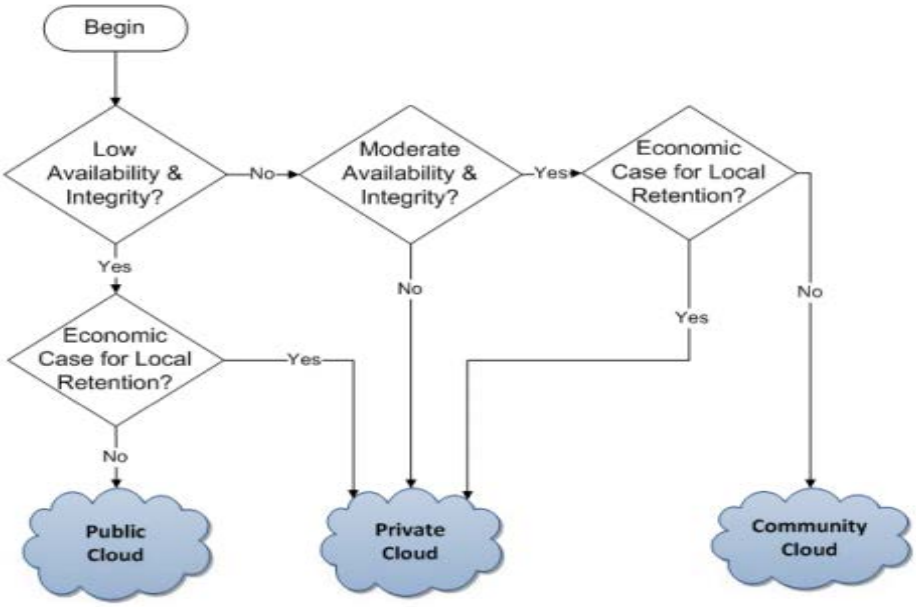
(See Appendix 1 for an explanation of the terms)

Technical / Business Requirements Considerations

1. If Migrating to the Cloud, What Cloud Hosting Deployment Model Can Meet My Agency's Needs?

If you consider your agency's operational needs, mission and the security requirements of the systems to be hosted, this will assist in selecting the cloud computing model that will make your agency's operations most efficient and cost effective. After a decision has been made to use cloud hosting, a key input to your decision should be to determine the overall approach to transform your datacenter and decide on a strategy for what services will be accessible in the cloud. The strategy should consider the deployment model types, the enterprise's relationship to the cloud, and the business case analysis.

The following image is an example of determining the security impact of systems and the cloud model to choose accordingly.



Cloud Model Selection Decision (*from the NOAA website: Cloud Transition Decision*)

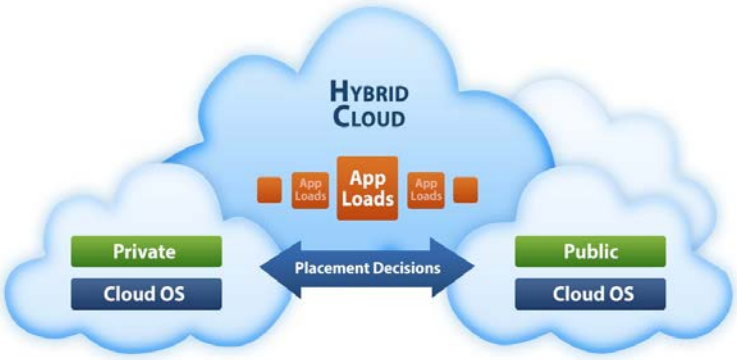
While not all inclusive, let's start with these scenarios:

Private Cloud – A private cloud may be hosted by any Federal agency such as the U.S. Patent and Trademark Office (USPTO), National Oceanic and Atmospheric Administration (NOAA), or

even the Defense Information Systems Agency (DISA). In private cloud models, the infrastructure is usually hosted inside the organization's firewall, but it can also be hosted off-premises by the CSP. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation. With the private cloud, computing power is spread across the enterprise. Departments can receive extra computing cycles when they need it. This scenario affords savings across the enterprise.

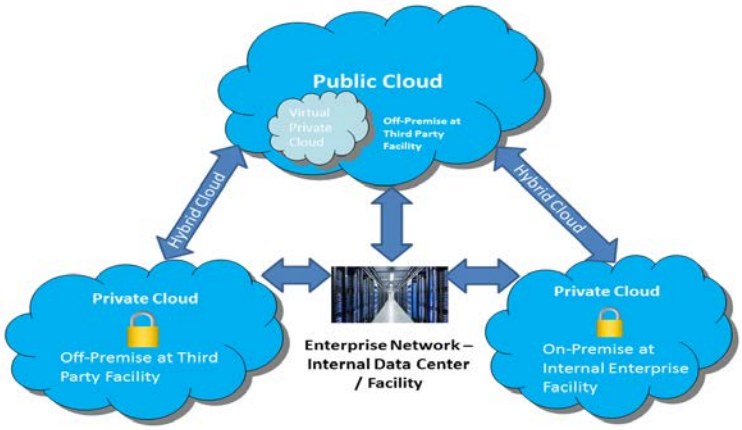
Public Cloud – A public cloud may be hosted by a commercial CSP. In a public cloud model, the infrastructure is usually hosted outside the agency's or organization's firewall. All applications and data of the organization are hosted by the CSP. This eliminates all burden of responsibility of the agency from maintaining and operating the infrastructure required to provide digital services to the citizen. Often, the CSP enables the customer organization to develop applications in its cloud infrastructure for use by its customer. The range of public cloud capabilities is expansive, but may not have the best ability to ensure the protection of sensitive agency data.

Hybrid Cloud – Multiple clouds work together, coordinated by a cloud broker that federates data, applications, user identity, security, and other details. A hybrid cloud can be delivered by a federated cloud provider and has the capability to combine its own resources with those of other providers. The provider of the hybrid cloud must manage the cloud resources based on consumer requirements.



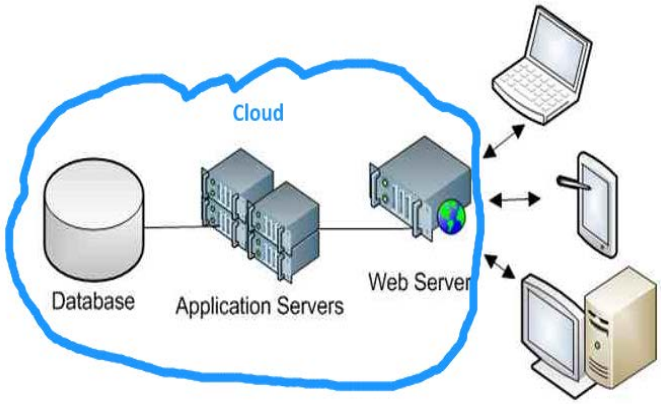
Hybrid Cloud

Enterprise to Cloud to Enterprise – This refers to cloud applications running in the public cloud and interoperating with mission partners applications. In this scenario, identity, an open client, federated identity, location awareness, metering and monitoring, management and governance, security, organizational Terms and Conditions (T&C), Application Program Interface (API) for storage and middleware, SLA, and life cycle management are considerations for this particular environment.



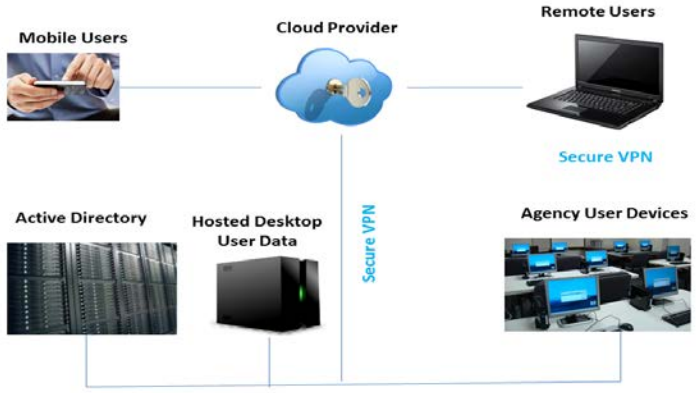
Enterprise to Cloud to Enterprise

End User to Cloud – This includes applications running in the cloud such as Salesforce, Microsoft Office 365, or Google applications. In this scenario, the end user is accessing data or applications in the cloud. Common applications of this type include email hosting, social networking and etc. The user doesn't want to keep up with anything more than a password since the data is stored in the cloud.



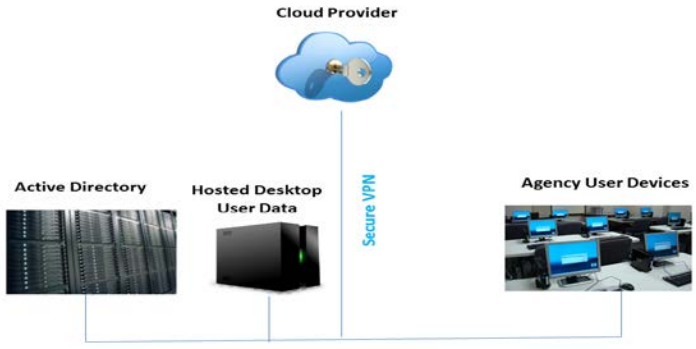
End User to Cloud

Enterprise to Cloud to End User – Applications running in the public cloud and accessed by employees and customers. When the end user interacts with the enterprise, the enterprise accesses the cloud to retrieve data, and sends the results to the end user.



Enterprise to Cloud to End User

Enterprise to Cloud – Cloud Applications integrated with internal IT capabilities. This might be a common use case during the early stages of an agency migrating to the cloud. This affords the enterprise to have the most control of its resources. Some uses are the storage for backups or archived data, using virtual machines to bring processors online to handle peak loads, or using applications in the cloud for certain enterprise functions (i.e. Customer Relationship Management (CRM) software).



Enterprise to Cloud

2. Develop the Business Case Analysis

Business Case Analysis - This Business Case Analysis (BCA) includes an objectively documented analysis, comparison of alternatives and recommendation to address the critical mission need(s), requirement(s), gap(s), or problem(s). It is submitted to the decision authority name for review, feedback, and final decision.

Perform a Business Case Analysis (BCA) on cloud enabling technologies. A business case is a documented argument intended to convince a decision maker to approve some kind of action. The strength of the business case is every bit as important as the value inherent in the project. A business case document should follow a fairly standard format that is relevant to any type of project. There are particular considerations for different types of business cases.

The DOD IT Business Case Analysis template is as an example BCA template to consider.

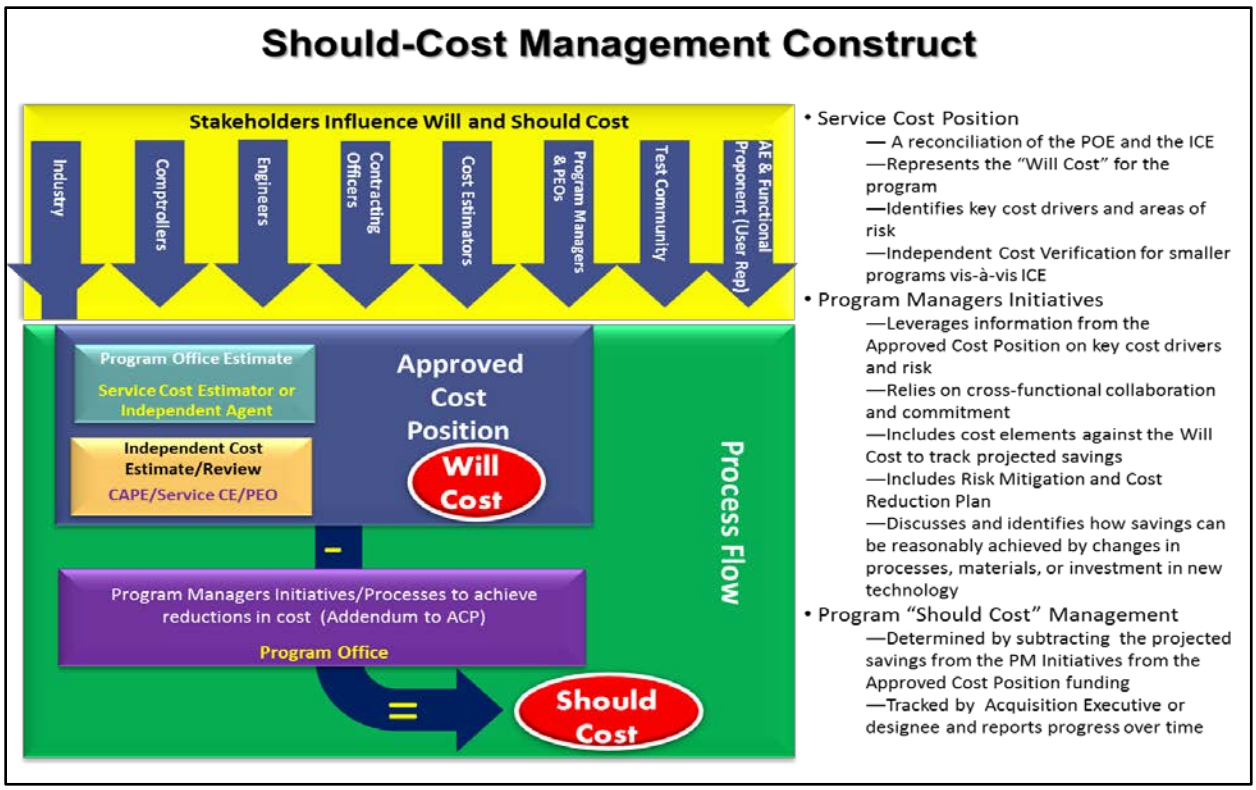
As a basic outline, the following are some recommended considerations for a business case.

1. Executive Summary – Decision makers often read and analyze the Executive Summary first, making it a critical part of the overall product support strategy documentation. It is more beneficial if the Executive Summary is written last even though it is usually the first section read. The Executive Summary must be concise. It must identify the problem statement in question, and highlight key elements of the recommendation. It should summarize mission and business impacts, risk and sensitivity analyses results, as well as briefly address other important sections as required to help the reader quickly understand the BCA's product support strategy recommendation. Items within the recommendation section should minimally include:
    a. Key assumptions that produced the recommendation
    b. Brief description of the alternatives if the primary solution is not holistically feasible.
    c. Description of the approach to solving the solution
    d. Summary of objective criteria and conclusions
    e. Description of the implementation plan at a level of detail necessary to support the recommendation

2. Introduction of Overview - This section provides guidance on developing the problem statement and provides background information. The introduction lays out much of the background and reasoning for conducting the BCA and helps to define the issue being addressed and supported by the analysis. Ensure the requirements of the overview have traceability to address high level requirement(s), to include: strategic alignment, mission needs, mandates, functional needs, Data Impact Level Assessment per DoD Risk

Management Framework, and DoD Cloud Security Model and Mission Impact Assessment.

3. Assumptions, constraints, and evaluation methodologies - This section describes assumptions and constraints (financial and non-financial) critical to the business case analysis. The Assumptions and methodology are two items to be explored early in the BCA process.
    a. An assumption is an informed position about what is believed to be true for a situation in which explicit factual knowledge is unobtainable.
    b. Constraints are factors that limit the analysis, possible solutions and/or expected outcomes.
    c. Costing Consumption and Constraints describes the Life Cycle Cost Elements (LCCE) for your agency's potential cloud enabling technology.
        i. From a contracting perspective, this section is covered under the Federal Acquisition Regulation (FAR) 15.4 (Contract Pricing).
        ii. This section must describe an Independent Government Cost Estimate (IGCE) with key costing assumptions and constraints critical to the BCA and include all applicable fiscal years within the life cycle for each Alternative.
        iii. The preferred method is Will-Cost and Should-Cost Management illustrated in the below image. It is based on realistic technical and schedule baselines. This method assumes success-oriented outcomes from implementation of efficiencies, lessons learned, and best practices.
        iv. It is designed to drive efficiencies into programs and incorporates the results of contract direct and indirect cost reviews.



Will-Cost / Should-Cost Management

d. Agencies should develop, describe, and choose a list of alternatives. Brainstorming and drafting alternatives must be conducted early in the process. For more formal programs in DoD, this information can be found in the Initial Capabilities Document (ICD) or the Capabilities Development Document (CDD). For non-DoD agencies, this information may be located in the Federal IT dashboard under the IT portfolio summary dashboard associated with your agency. Once this information is gathered, there should be a comparison of alternatives. When adequate data is sufficient to make a life cycle product support strategy decision, regulations stress the importance of making the best possible use of the enterprise and industry resources at the system, subsystem, and component levels while maximizing the use of outcome based product support strategies.

e. Finally, agencies should state the final conclusion and recommendation on which strategy to choose and why that strategy should be chosen. Provide the rationale, justification, and supporting information for each recommendation. Other pertinent information to include is a roadmap and implementation plan that includes time for validation and approval of Product Support BCA, documenting or archiving the Product Support BCA, determining gaps, and documenting other lessons learned.

4. Determine a baseline for the applications under consideration for migrating to the cloud. The baseline consists of application profiling and a cost baseline.
   a. Application Profiling – Network engineers must collect a sample of real usage data. It is important to understand total number of connected users and profile this activity for information such as requests, transaction rates, and request latencies. All performance requirements shall specify measurement points (i.e., where measurement will be taken). Historical data profile is important to capture the variances in daily, weekly, and annual usage. Performance measures include metrics such as the average availability, connectivity, up-time and down-time of a system, as well as expressions such as error rates or sample rates among other underlying or abstract metrics that comprise the metric being observed. Anything constant in the expression, such as an interval time like the number of days in a week or the length of time of the sampling rate is a parameter which should always be identified.

      ➢ The sampling rate should be defined in accordance with the business case and SLAs set forth by the program requirements. A sampling rate could be event driven, schedule driven, or based on some statistical distribution. Systems/services are sampled on a continual basis for reporting to management, even if "continual" is sampling every few minutes such as for a low usage system. Reporting may use moving averages and peaks in the last specified time period (e.g. 48 hours) as deemed useful to the program and supported community. Use of GMT for time reference is strongly preferred for common usage in the operations community.

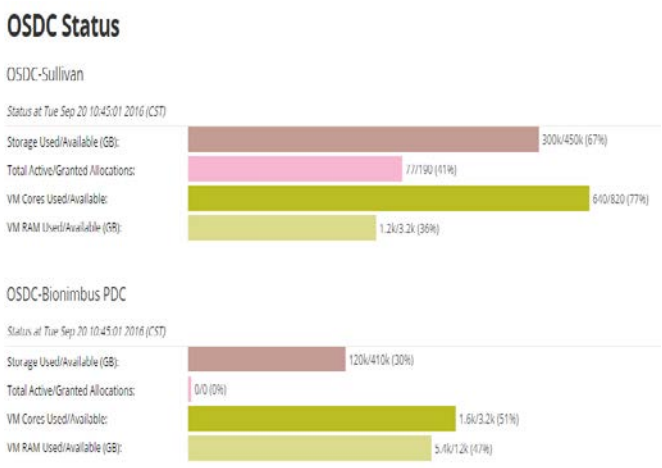
      ➢ All performance requirements shall specify a threshold representing minimal acceptable performance and an objective representing the best desired performance.[2]

      ➢ All performance requirements shall be measured and collected to support verification of the requirement.

   Other usage data, but not all inclusive, that affords how the agency articulates their application needs to the SI in determining how to size the application in the cloud are:

[2] In a commercial context, SLAs often point out "exclusions" or factors that the CSP cannot be held accountable for that would cause an unacceptable performance. It is important to note what these exclusions are during any negotiations with a CSP.

- ➢ System / Service Response Time - Response time measures are related to capacity measures, in that the system is expected to respond within a specified response time, if it is not overloaded.
- ➢ Task Completion Time - Task completion time is the time for a function to be performed; it does not include a response to a requestor.



- ➢ System / Service Capacity - Planning factors such as "8,000 concurrent active users in tele-conference meetings can be supported on each conference server, plus 10% of a web server, 10% of a load balancer, and maybe with one terabyte of assigned SAN storage" to support the functions within the SLAs specified
- ➢ Storage data input/output per second (IOPS) – How efficiently data is transported between storage nodes.
- ➢ System / Service Availability - A system or service is considered available if it can perform all of its functions while meeting other performance requirements; otherwise, it is considered unavailable.
- ➢ Service Desk Metrics - While the typical focus will be incident management, document appropriate metrics for event management, access management and request fulfillment
- ➢ Network Data Variables - Dropped connections, connections per second, and throughput

Upon final migration, the agency can use these metrics to evaluate if the level of service is improved upon migrating to the cloud.

b. Cost baseline – After the agency has identified potential applications that may be migrated to the cloud, a thorough cost analysis should be conducted. Some areas of consideration are:

   i. License Management – It is critical to understand the application licensing and the impacts on third party software dependencies.

ii. Application Re-design – Agencies may wish to consider if the applications require re-design when migrated to the cloud. Many organizations integrate applications over years and are integrally coupled with other applications. De-coupling an application may require a re-design before migrating to the cloud.

iii. IT Service Management (ITSM) - ITSM is often not thoroughly defined and documented in many organizations. Migrating applications will incur a detailed capture of policies, processes, and supporting procedures that are performed by an organization.

iv. Application Deployment – It is recommended that agencies ensure the costs for engineering, design, and testing in the cloud environment are incorporated into their requirements for the SI.

v. Developing Cloud Skills – An agency's pertinent personnel may require additional skills training to support cloud migration. Incorporate this training into your planning and whether it can best be given over the web (recorded sessions) or in-person.

vi. Cloud Service Costs – The CSP on-going fees are incorporated into your cost baseline. With the historical application profiling, the agency can estimate the CSP costs, but also incorporate additional fees to handle peak load periods.

5. Concept of Operations - Producing a Concept of the Operations (CONOPS) is critical and requires going through a decision making process on the types of applications to migrate to the cloud, conducting application profiling, a cost analysis, and developing a business case. A CONOPS is an outline of the agency's roadmap to migrate to the cloud. The CONOPS facilitates the alignment of the IT architecture and services it will provide with the governance system. It provides insight into the interior / exterior boundaries, information flow, system characteristics, configuration management, system security architecture, life cycle costs, etc. A link to a CONOPS template is in the References section.

3. Cost Baseline Evaluation

Since one of the main areas for consideration is a cost comparison, the following image lists an example evaluation of costs in a cloud and existing environment. The cost baseline can also be used in the Cost Benefit Analysis.

	Area	*Estimated Annual Cost Percentage*	*My Current Costs*	*My Current Percentages*	*My estimated Cloud Hosting Costs*	*Difference from Current hosting environment to Cloud (Includes one-time migration costs)*
1	**Consulting Services**	**85%**	**$2,057,000**	**64%**	**$2,090,000**	($33,000)
	Application Development	30%	$1,000,000	31%	$1,000,000	
	Project management	10%	$250,000	8%	$250,000	
	Security Certification & Accreditation (includes FedRAMP, Privacy Impact Assessment, Personally Identifiable Information Assessment and related costs)	5%	$100,000	3%	$100,000	
	Application maintenance	30%	$500,000	d	$500,000	
	Systems administration	10%	$200,000	6%	$75,000	
	Cloud environment management				$50,000	
	Migration (one-time)*				$35,000	
	Customization (one-time)*				$75,000	
	Travel		$7,000		$5,000	
	Miscellaneous					
2	**Hosting Environment**	**15%**	**$1,150,000**	**36%**	**$235,000**	$915,000
	Infrastructure	10%	$1,000,000	31%		
	Software Licenses	2%	$100,000	3%		
	Software Patches	1%	$25,000	1%		
	System or Software Upgrades	2%	$25,000	1%		
	Network or Infrastructure customization (one-time)*				$35,000	
	Miscellaneous					
	Total	***100%***	***$3,207,000***	***100%***	***$2,325,000***	***$882,000***

* One-time Migration costs in moving to the cloud hosting environment

Cost Baseline Example

4. Changing Cloud Service Providers

This is a scenario when a Federal agency using a CSP decides to switch to another CSP or work with additional CSP's. This scenario can apply to any of the service models (IaaS, PaaS, and SaaS). The key to this scenario is open standards for applications. To ensure success, vendors should have an open client, location awareness, security, SLAs, a common file format for virtual machines, and common Application Program Interfaces (API).

Changing Cloud Service Providers

While this section is not totally comprehensive in all the details that an agency requires to develop a cloud migration strategy, it provides a framework for understanding the detailed thought processes that should occur in roadmap strategy development. Early, flexible planning will reap huge rewards during the migration if conducted properly.

How Do I Procure Services For The Cloud?

Now that a detailed analysis of the agency's cloud computing requirements has been approved, the next step is to begin the procurement process. In this section, we're going to discuss the contract strategy, method of payment, and review practices to consolidate the information into a performance based acquisition. Your department may still have a number of concerns at this point. The agency may be apprehensive about an enterprise-wide approach or even the ability to migrate vast number of systems. It may also consider having a direct contract with the CSP or through a systems integrator, depending upon its needs. The best approach is to leverage the

modular contracting approach and start small with a single application (within one region) as a pilot. Your department may face a learning curve while attempting to leverage cloud computing services. So, start small, conduct After Action Reports (AAR) after each migration, and use the lessons learned to improve the next migration.

1. **Modular Contracting.** The primary challenge for the acquisition professional is to shorten the procurement lead time as much as practicable so that successive, single-award contracts can be added to continue a pilot and maximize the benefit of the modular approach. Modular contracting (FAR 39) deconstructs complex problems into manageable chunks of work compared to the traditional approaches that try to define every requirement and outcome up front. Successful application of modular IT development and contracting also requires a commitment to taking advantage of Integrated Product Teams (IPT), and understanding what structures, strengths, and benefits they provide. Benefits of modular contracting are:

Benefits of Modular Contracting

2. **Contract Types**. While the method of procurement is a concern for your agency, there are Pros and Cons to each contract strategy.

    a. Strategic and Shared Services. Government Wide Acquisition Contracts (GWACs) are useful ways to buy commodity IT services, single applications, as well as supporting data consolidation efforts.

b. IDIQ-type vehicles. These vehicles have been very successful with enterprise solutions. IDIQ contract vehicles have a broader scope of work which makes them well-suited to support programs with a high and varied demand for cloud-enabled IT services and are effective for modular contracting approaches.

c. Requirements-type vehicles. Requirements contracts are addressed in Federal Acquisition Regulation (FAR 16.503). These contracts are simpler to administer at the ordering level because they are single award and rely on firm fixed priced units. Simplicity may support a better control of the consumption habits of the customer, but the scope may also be narrow.

d. Standalone – contracts. Stand-alone contracts are ideal to support modular contracting (FAR 39.103). They can be used for systems integration, acquisition strategy support, or engineering advisory services. While modular contracting requires additional administration because of the successive contracts, this administrative workload should be considered by the agency for more compartmentalized efforts.

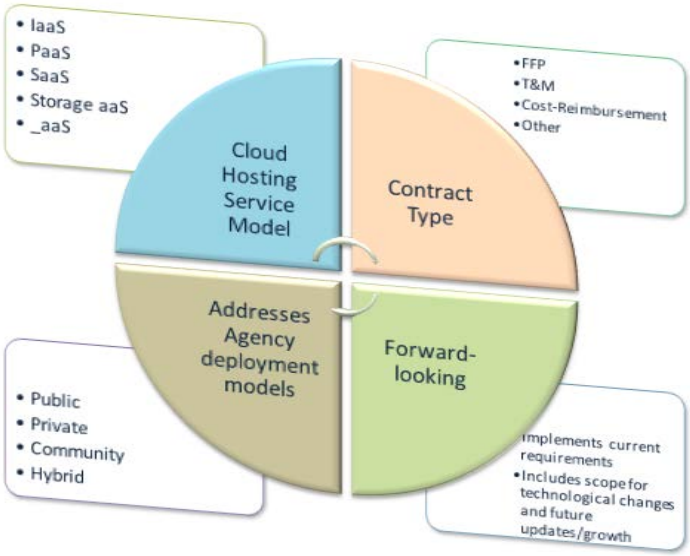
e. Cloud brokerage. An evolving strategy for cloud enabling IT services is a cloud broker. This methodology is ideal for allowing a single vendor to manage the effort to connect the Government agency with the CSP. While the evolving strategy supports reduced priced reductions, the trade-off is that the agency has less visibility into the procurement process.

Contract Type	Used for	Pros	Cons
Strategic & Shared Services	Commodity IT Services, Single Applications, Consolidation Initiative.	Scale, scope, and service.	Less control over metrics, Service Level Agreements, and Terms & Conditions.
IDIQ	Enterprise Solution, Multiple applications, High demand / varied consumption.	Simple to administer better visibility into consumption habits.	Management of task and delivery order in a multi-vendor environment.
Requirements	Commodity IT Services, Closed Systems, Storage and Data Processing.	Reduced resource costs, priced competition, selection.	Greater potential for lock-in, but narrower in scope.

Contract Type	Used for	Pros	Cons
Stand-alone contracts	Single Applications, Cloud Support Services, Systems Integration.	Reduced resource costs, price competition, selection.	Less procurement control and visibility, variation in "Brokerage" Definition.

Advantages and Disadvantages of Contract Types

3. **Contract Funding**. There are three (3) primary categories: firm fixed price, cost plus, and time and materials (labor hour) contract types. While cloud computing offers "pay-as-you-go", which is similar to mobile phone plans, the Financial Management Regulation (FMR) and Federal Acquisition Regulation (FAR) limit the ability to pay for cloud consumption above a predefined limit. As a workaround, a seasoned acquisition professional can leverage FAR subpart 16.2. FAR subpart 16.2 provides an explanation of fixed-price types of contracts. Fixed price contracts provide for a firm price or, in appropriate cases, an adjustable price. Fixed-price contracts that provide for an adjustable price may include a ceiling price, a target price (including target cost), or both.



Sample Cloud Computing Contract Capabilities and Benefits

a. Firm Fixed Price (FFP) with Economic Price Adjustment – FAR 16.203 provides an option, stating that a fixed-price contract with economic price adjustment can be used when the contracting officer determines that it is necessary. It may be necessary either to protect parties involved against significant fluctuations in labor or material costs, or to provide for contract price adjustment in the event of

changes in the contractor's established prices. The following are considerations for FFP with economic price adjustment (EPA):

i. Adjustments based on established prices. These price adjustments are based on increases or decreases from an agreed-upon level in published or otherwise established prices of specific items or the contract end items.

ii. Adjustments based on actual costs of labor or material. These price adjustments are based on increases or decreases in specified costs of labor or material that the contractor actually experiences during contract performance.

iii. Adjustments based on cost indexes of labor or material. These price adjustments are based on increases or decreases in labor or material cost standards or indexes that are specifically identified in the contract.

b. Additional Considerations for Firm Fixed Price with Economic Adjustment. As an acquisition professional, if a decision to use firm fixed price with economic adjustment is made, the following are some considerations:

i. Determine the economic triggers that may activate the cost adjustment.

ii. Maintain a contractual description of the cost and labor and materials and the rationale of how fluctuations affected each.

iii. Provide a schedule to review the cost adjustment and validate with your agency's consumption remains within objective and targets metrics.

Type	Description	Use	Conditions on Use
Firm Fixed Price Contracts	Contractor agrees to provide supplies or services to the procuring activity for a specified price.	When acquiring commercial items or other supplies and services when there are reasonably definite specifications, and fair and reasonable prices can be established at the outset.	N/A
Fixed Price with economic price adjustments	Contractor agrees to provide supplies or services to the procuring activity for a specified price that could be adjusted if certain conditions change during period of performance.	Used when stability of market prices or labor conditions during an extended period of contract period is uncertain, and contingencies that would be otherwise be included in the contract price can be identified and separately addressed in the contract.	Contract officer must determine that a price adjustment clause is necessary to protect the contractor and government against significant fluctuations in costs, or to provide for price adjustment in the event of changes in the contractor's established prices.
Fixed price contract with prospective price redetermination	Contractor receives a FFP for a specified initial period of performance, with the price for later periods revised in an equitable manner based on variables.	Used to acquire quantity production or services when it is possible to negotiate a fair and reasonable FFP for the initial period, but not for later ones agreed upon by both parties.	Negotiations have established that conditions for use of FFP contract are not present, and a fixed price incentive contract is not more appropriate; the contractor's accounting system is adequate for redetermination; pricing periods can be made to conform to accounting system; and there is reasonable assurance redetermination will take place as scheduled.
Firm fixed price, level of effort term contracts	Contractor receives a fixed amount for providing a certain level of effort over a certain period of time on work that can be state only in general terms.	Investigation or study in a research and development area whose anticipated value is generally less than $150,000; usually yields a report describing the R&D results.	Work required cannot be otherwise be clearly defined; required level of effort is identified and agreed upon in advance; and there is reasonable assurance that the intended result cannot be achieved by less effort.

Types of Fixed-Price contracts

4. **Performance Based Acquisition (PBA)** – Performance Work Statements (PWS) and Statements of Objectives (SOO) are all methods of defining work the Government desires to be accomplished. Typically, the Program Management Office (PMO) or the Contract Officer Representative (COR) is responsible for developing PBA documents in concert with a team of acquisition professionals. While most agencies have guides or formats for these documents, this best business practices document intends to provide considerations for the PBA documents produced.

    a. PWS – Performance based acquisition is defined in FAR part 2.101. FAR part 2.101 provides explanations of many acquisition terms including the PWS. FAR 2.101 requires structuring the aspects of the agency's acquisition around the purpose of the work performed, ensuring the requirements are clear and specific. It also mandates that objective terms with measurable outcomes be provided.

    b. SOO – A SOO is a Government-prepared document incorporated into the solicitation that states the overall performance objectives. It is used in solicitations when the Government intends to provide the maximum flexibility to each offeror to propose an innovative approach. That portion of a contract establishes a broad description of the government's required performance objectives. For example, Commercial Cloud Computing Resources needed to support the federal governments DoD level 2 systems in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) and applicable DoD cloud computing security requirements.

Estimating the Pay-As-You-Go pricing

For IaaS, PaaS, SaaS or any _aaS cloud computing option, once the previously mentioned gathered metrics have been determined for your agency, ideally as a part of a pilot. These metrics can contain: system's security requirements, system / service capacity & availability, network data variables, on-premise / off-premise needs, within the CONUS (Continental United States), etc. Instead of specifying the amount of resources needed and constantly going through the acquisition changes as new technical upgrades or requirements come up, it is suggested to then include "what needs to be done" in the PWS using performance based objectives.

It is then recommended for the Request for Quote (RFQ) to have the CSP or SI recommend what is needed (in terms of resources) to meet the systems requirements.

And an evaluation based on these results can then be used to obligate funding with the caveat that the SI or CSP inform the agency when a specific threshold is reached, For example, When funding is 90% depleted, notifications will be sent by the CSP or SI to the federal PM, etc.

And, in case of any unused funding at the end of the Fiscal Year (FY), it can be either de-obligated or rolled over (depending upon the acquisition authority granted to your agency) to the next FY.

A similar approach can be helpful for planning needed cloud computing administration or migration consulting support.

My Application has been migrated to the Cloud, Now What?

Assuming that the necessary actions have been taken beforehand, and the cloud migration plan has been executed, continual management of cloud hosting and related activities is an ongoing effort. Some of these tasks include:

- Regularly scheduled contingency testing depending upon application criticality. Does the CSP automatically shift the system with no loss of data or impact to users to a secondary location in case of primary location failure?

Cloud Computing: Constant Management

- Is security monitoring conducted regularly with summary reports or logs provided to the government?

- Are the applications meeting SLA requirements for performance, auditing, etc.?

- Are the costs including the latest decreases in infrastructure hosting? Are services costs being gradually reduced? Also, set-aside costs for planned future technology upgrades, license management, etc. should be considered.

- Is the overall move to the cloud environment reflecting what was expected? Are advantages being realized during the analysis phase (prior to moving to cloud)? If not, why not? What can be done to realize those benefits?

- Ongoing coordination with Service Integrator and/or CSP to achieve needed results.

- Training provided for new technologies for the government cloud hosting management workforce, etc. This can also allow experienced system administrators and other Federal IT professionals to change their roles from maintaining data center infrastructure to managing cloud infrastructure instead.

- Understand how new technology releases may impact the cloud environment and incorporate new advances, as needed.

Conclusion

The challenges that agencies face while planning for cloud computing adoption need to be addressed as part of a comprehensive process that begins with analyzing the benefits of moving to cloud hosting and then taking the required ensuing steps. The provisioning of cloud computing services is a cultural as well as organizational change. However, performance based acquisition and modular contracting are perfect methodologies to bridging the cultural change. With performance based contracting, the agency can focus more on the performance characteristics of the application, the SLA, and the desired outcome of the user experience. The agency will rely heavily on metrics and have a better grasp on the expectations of the SI and CSP. However, in order to prepare for cloud adoption, it is critical that agencies understand the performance characteristics of the current architecture and take steps towards the “desired-state”.

When addressed properly in the business case and CONOPS, the potential SI and CSP can develop a solution that minimizes risk to the Federal Government, reduces cost, and creates an effective user experience. In modular contracting, the need for a system is attained through successive acquisitions of interoperable increments. Each increment complies with common or commercially accepted standards applicable to information technology so that the increments are compatible with other elements of information technology comprising the overall system.

Continual management of cloud hosting (SI’s, CSP’s and other mission stakeholders) and ensuring that the migration realizes the expected benefits within the planned timeframe are important and ongoing objectives to realize the maximum benefits for your agency.

Appendix 1: Terms used in the Sample Decision Flow Process

Cost Benefit Analysis - A Cost Benefit Analysis (CBA) document lists and compares the costs of the current hosting environment and costs of having the Information Technology (IT) system in the cloud. The CBA includes costs related to:

- Migration Costs (includes any applicable service costs),
- Services (Systems Administration, Maintenance, etc.)
- Network Capacity or Bandwidth,
- System modification (if needed),
- Security impact, Vulnerability Scanning and related costs.

Comparative Performance Analysis - Compares the performance of a traditional hosting environment (non-cloud) and a cloud hosting environment by setting (and periodically checking) specific metrics such as:

- Application response time,
- Load Balancing (time taken for auto-switching to an alternate site),
- System Availability time (Percentage uptime: e.g., 99.9%,),
- Data Transmission speed,
- Disaster Recovery response time,
- Number of concurrent users, etc.

Technical Requirements - In case of an existing application or system, agencies should determine the cloud hosting system requirements compatibility with the application. For example:

1) Does the application require modification or customization so that its existing functionality is intact before moving to the cloud?

2) Which deployment model should I choose and why?

3) Does the cloud environment support and improve the application's current hosting? Consider:

    - Current performance response time,

- Number of concurrent users/maximum expected users,
- Network capacity requirements,
- Interconnections with (or dependencies to) other applications/systems,
- Data Retrieval/Transfer from the cloud environment,
- Load balancing/failover functionality,
- Disaster Recovery process,
- Data Archiving process,
- FOIA process,
- Physical location of applications, systems, data center, etc.

For a new application, in addition to pertinent factors listed above, the following determination needs to be made:

1) Does the cloud environment include an application/system consisting of data which is non-classified or classified security categorization and what are the impacts related to:

    - Data access & authentication,
    - Trusted Internet Connections (TIC), IPv6 and other related compliance,
    - Data cleansing,
    - CSP's FedRAMP status,
    - Infrastructure hosting in CONUS or other locations,
    - Security Privileges & Accessibility (CONUS location, shared or dedicated application access rights, etc.) for System Administrators, Users accessing the systems, etc.

2) Is the cloud environment subject to a FOIA?

Business or Acquisition Strategy

1) As part of an initial project, agencies can benefit from conducting a pilot to determine estimated cloud costs. For example: Use a subset (approximately 5%) of locations or users that are a close representation of the whole, to conduct a pilot. The purpose of the pilot is to determine the following:

    - Anticipated costs,
    - Capacity/resource usage,
    - Services needed to support the cloud,
    - Acquisition contract type needed,

- Technical requirements evaluation (see the ***technical requirements*** section listed previously), etc.

2) Agencies can also benefit from using lessons learned during the pilot to conduct a bigger subset (increase to 25%) of the whole and determine the results, apply lessons learned from the previous pilot.

3) Agencies may then wish to apply the lessons learned from the previous iterations to fully define the acquisition contract and technical/service requirements to the rest of the locations/users. They may also consider any travel costs as part of the implementation if the application/system is in multiple locations.

4) It is also recommended to have discussions with other Federal agencies with existing cloud hosting to get any recommendations or best practices that can be implemented. And, in case of the criticality of data/systems being shared with other nations outside the U.S., develop SLAs and share best practices with them. As an example, the Australian Government Cloud Computing Policy is based on NIST's cloud computing definition. This web site hyperlink: Australian Government Cloud Computing Policy leads to their cloud computing policy.

5) As part of the acquisition strategy, develop Service Level Agreement's (SLAs) with metrics (see sections on ***Comparative Performance Analysis*** and ***Technical requirements***), and regularly review the metrics to ensure the CSP is complying. In case of serious concerns or repetitive issues with the CSP not complying with the SLA or worse issues (such as Service Integrator going out of business, etc.), plan for migration of data/system to a different CSP or contract. This migration plan to another CSP (and any related steps) needs to be a part of the initial business and acquisition strategy.

Contingency Analysis

1) Agencies should develop risk and mitigation plans for business, technical, security & acquisition related areas. Regularly evaluate and test any areas, as needed.

2) It is recommended that agencies have an exit plan defined before-hand. Instead of being locked down with one CSP, agencies should develop a strategy early in the planning phase on what needs to occur (both from the government-side and the vendors area) in

case of transitioning to a different CSP. This should also be spelled out in the SLA and other acquisition documents and discussed/established with the SI/CSP, as needed. Also, determine data, application ownership rights, etc. as part of the exit plan.

3) Agencies may wish to develop Standard Operating Procedures (SOPs) and define them to include the following:

   - Roles of the CSP, Federal government and any other interdependent Subject Matter Experts,
   - Continuous monitoring related to Security & Vulnerability analysis,
   - Actions to conduct (and responsible Point-Of-Contact (PoC)) during a security incident,
   - Regularly test the SOP's and update with current PoC information details as needed.

So, as a precursor, an agency can no longer use the traditional mindset for a data center solution, but must consider the desired outcomes. Some desired outcomes are responsiveness to the end-user, storage availability, on-demand services, and cost savings in relation to total cost of ownership.

References

1. Army Cloud Computing (2016). Retrieved on September 8, 2016 from http://ciog6.army.mil/Portals/1/Army_Cloud_Computing_Strategy%20Final_v1_0.pdf
2. Best Practices Guide for DoD Cloud Mission Owners (2016). Retrieved on September 8, 2016 from http://iasecontent.disa.mil/stigs/pdf/unclass-best_practices_guide_for_dod_cloud_mission_owners_FINAL.pdf
3. Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative Report (2014). Retrieved on September 8, 2016 from https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report(1)(1).pdf
4. Creating Effective Cloud Computing Contracts for the Federal Government (2012). Retrieved on September 8 2016 from https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf
5. Data Center Optimization Initiative (DCOI) (2016). Retrieved on September 8, 2016 from https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_19_1.pdf
6. Department of Defense Cloud Computing Security Requirements Guide (2016). Retrieved on September 8, 2016 from http://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf

7. Department of Defense Concepts of Operations Template for Project Name (2015). Retrieved on September 8, 2016 from https://acc.dau.mil/adl/en-US/511208/file/64104/SWTM024.DOC
8. Department of Defense IT Business Case Analysis (2010). Retrieved on September 8, 2016 from http://dodcio.defense.gov/Portals/0/Documents/DOD%20IT%20Business%20Case%20Analysis.pdf
9. Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap (2011). Retrieved on September 8, 2016 from http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf
10. DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process (2014). Retrieved on September 8, 2016 from http://www.dodig.mil/pubs/documents/DODIG-2015-045.pdf
11. DoD Needs an Effective Process to Identify Cloud Computing Service Contracts (2015). Retrieved on September 8, 2016 from http://www.dodig.mil/pubs/documents/DODIG-2016-038.pdf