

The GSA logo consists of the letters "GSA" in white, sans-serif font, positioned inside a dark blue square. The background of the entire page is a photograph of a bright blue sky filled with numerous white, fluffy clouds. The sky is clear and vibrant, with the clouds scattered across the frame, creating a sense of depth and openness.

GSA

2017

HYBRID CLOUD ALMANAC

CLOUD COMPUTING SERVICES

U.S. General Services Administration

Table of Contents

2017 Forecast.....	2
2016 Hybrid Cloud Adoption Trends.....	4
2017 Industry Best Practices For Hybrid Cloud Implementation.....	5
How GSA Can Help You Acquire Hybrid Cloud.....	10
2017 Closing Remarks.....	16
Appendix 1: GSA Tools for Hybrid Cloud Solutions.....	18
Appendix 2: Cloud Reference Documents.....	19

2017 Forecast

In 2016, prominent cloud experts predicted the death of enterprise public cloud and the birth of agency shifts to “commodity” cloud providers. 2016 brought in enterprise workload management in both on-premises and in public cloud environments (what we now call hybrid clouds) as well as the difficulty of finding programmers who can develop and maintain applications in cloud environments. Meanwhile, the proliferation of DevOPS practices emerged to provide constant delivery and updating of applications in increasingly demanding markets. Some CSPs struggled with shifting from virtual machine hosting (which often requires the continuation of legacy processes) to using containers for increased efficiency and security.

Consequently, the outlook for hybrid cloud adoption in 2017 is very good. According to International Data Corporation (IDC), 80% of Enterprise IT organizations will commit to hybrid cloud architectures in 2017. Agencies have been realizing the benefits of cloud solutions, and have taken their IT to another level by adding the dynamic flexibility of hybrid. IDC projects the cloud market within the Federal sector will increase to \$9 billion by 2017. In a recent Gartner survey of Federal IT Managers, 75% indicated plans to implement a hybrid cloud solution by the end of 2017. Many factors contribute to the expected growth in Federal hybrid cloud adoption, and this section outlines the primary drivers.

Cloud is not a secret any longer: Agencies have been exploring cloud solutions since the emergence of the “Cloud First Policy”, a part of the Office of Management and Budget’s 25 Point Plan to Reform Federal IT. In the beginning, it was uncharted territory with many unknowns looming. As innovators forged ahead, a robust library of lessons learned have been developed. There is now a proven roadmap to cloud implementation, solid use cases, and answers to all previous concerns such as security.

Convergence of Digital Services: Many Federal agencies are beginning to embrace a customer first approach to developing new processes and technology, focusing instead on the experience not the solution. As the Digital Services Playbook gains traction, agencies will dive deeper into streamlining websites for ease of use, developing intuitive apps and portals, and making their data open. Hybrid cloud solutions such as public hosting, and large volume data repositories accent and support these sites.

Security is now a strength: A major objection to diving into the cloud for early adopters was security concerns. Federal agencies have an obligation to maintain transparency of data, access and security, not to mention sorting sensitive and non-classified data sets and making them work in unison. Recent studies have shown that private clouds hosted by larger cloud service providers are more secure than on-premise solutions. Agencies no longer have to stress about building security into their solution. FedRAMP certifications give a sense of assurance that a certified vendor is able to provide a compliant and secure hybrid environment. For those who still want to maintain control and ownership of sensitive data, hybrid technologies have allowed a seamless integration of services that include on-premises hosting of classified data, while maintaining a lower cost public cloud for public facing websites. Hybrid offers security and control, as well as cost effectiveness, resource pooling and flexibility.

Administration change- Agencies are always concerned with shrinking budgets, and election years make this even more of a concern. A new administration brings new goals, and attempts to curb government spending; the easiest method is to slash budgets. Agencies are still required to achieve their mission, but innovation is required to do so. Hybrid cloud allows an agency to keep capabilities, reduce IT bloat, and become more agile for future innovation.

Streamlined Procurement- Cloud is not well suited for the federal procurement practices employed by the federal government. It must be treated as a utility, procured similarly to an electricity bill. Customers don't have to forecast how much electricity they use for the next month or more, instead they use the service, and pay for what they have consumed. Cloud usage is difficult to project, especially early on in an agency's cloud experience. Coupled with the difficulties in projecting use, the market is flooded with CSPs offering endless assortments of solutions which often result in less than optimal procurement of the best solution at the best price. The General Services Administration (GSA) is on the cutting edge of cloud technology and is working to streamline the procurement of cloud solutions through pre-competed contracts, scope reviews and other activities, which will further streamline the process. Agencies do not have to go at it alone, there are experts with resources that will help ensure their cloud migration is a success.

Phased Approach- Agencies are able to leverage existing capabilities, focusing instead on workflows that will make the most business sense. Some systems were recently implemented, and have a steep price tag. Justifying eliminating these systems a few years after they were launched makes no sense. Instead, an agency can begin updating solutions as needed, while maintaining orchestration of existing technologies and continuation of services.

The conditions for a huge year in hybrid cloud adoption are present for 2017. The experts and practitioners agree that cloud is the solution for years of neglected and antiquated IT systems, and hybrid cloud is the path forward.

2016 Hybrid Cloud Adoption Trends

In 2016, Federal Agencies were adopting cloud as much as budgets and available technical expertise allowed to continue towards achieving objectives outlined in the “Cloud First” policy. In particular, agencies are finding the hybrid cloud deployment model to be highly advantageous by allowing some IT resources to be supported in the public cloud while storing sensitive information in on-premise or consolidated legacy architectures.

Based on a survey of 1,060 IT enterprise technical professionals, hybrid cloud proliferation is growing as cloud users and cloud providers are maturing. Lack of resources and expertise has surpassed the challenge of ensuring sufficient security. 82% of enterprises held firm on hybrid cloud strategy between 2015 and 2016. Hybrid cloud adoption has increased by 13% year to year while overall cloud adoption has increased 2%. Cloud users are leveraging 6 clouds on average, with 17% of enterprises now having over 1,000 virtual machines in public clouds, up from 13%. Private cloud use has increased by 22% among enterprises. Additionally, enterprise business units have shown an increased acknowledgement of central IT setting policies by 13% since last year. 38% of respondents now have established approval policies for cloud over 2015’s 30%, signifying the growing role of cloud governance. Cost challenges continue to increase as optimization efforts lag. Few companies are taking action to minimize cloud costs by shutting down unused workloads or selecting lower-cost clouds. Overall cloud computing growth this year has led to an increased proliferation of a multi-cloud type environments, including hybrid.

The flexibility offered by hybrid cloud is responsible for the growing numbers stated above. Agencies no longer have to ‘discard’ IT investments in order to move to the cloud. Hybrid allows agencies to phase in an updated IT solution over the course of time. Many IT leaders view hybrid as a safer alternative to moving everything to the cloud at once. Hybrid allows lessons learned to be discovered that are agency specific, and factors in that not all systems are suited for the cloud. It allows for the integration of security of on-premises infrastructure with the availability and cost savings of public, in a blended and well-orchestrated solution.

Adopting hybrid cloud or multi-cloud configurations effectively involves using best practices observed both in industry and government. Each agency should consider many variables, as their mission and resources differ from those they may pull lessons learned from. In any event, the following section details best practices that should be considered when implementing a hybrid cloud.

2017 Industry Best Practices For Hybrid Cloud Implementation

Create a Roadmap for Hybrid Cloud Adoption

In any migration to cloud computing, planning cannot be overdone or under-emphasized. Agencies need to look at the short and long term costs of migrating, and realize they are going to be saving money in network administration, security patching, and infrastructure modification costs to meet usage demand. To calm agency concerns about data loss and security during a migration, some system integrators will replicate the legacy applications and systems in a DEV environment so stakeholders can compare the efficiency of the cloud against the legacy solution. However, agencies need to have a clear list of milestones to complete this transition. Current best practices call for prioritizing the order of application and data migration from easy to difficult in order to most expeditiously meet Federal OMB “Cloud First” policy mandate, as well as the [Data Center Optimization Initiative](#) effective as of August 1, 2016.

It is first important to understand the types of cloud deployment models available and how they differ from each other. The below table explains some key differences.²

²

Model	Cloud Infrastructure Set-up	Managed by	Location
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units)	Owned, managed, and operated by the organization	On or Off-premises
Community cloud	The cloud infrastructure is 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)	It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them	On or Off-Premises
Public cloud	The cloud infrastructure is provisioned for open use by the general public	Owned, managed, and operated by a Cloud Service Provider.	On the premises of the cloud provider.
Hybrid cloud	The cloud infrastructure is a 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		

In a 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.

Considerations For Implementation

1. Integration- Integration is critical in a successful hybrid implementation. Hybrid aggregates capabilities and solutions from cloud service providers, and those hosted on-site in order to leverage the best available combination. Service Oriented Architecture (SOA) Representational State Transfer (REST), Application Programming Interfaces (APIs), and cloud management and orchestration frameworks have opened up new options for integrating cloud services.
2. Composition- The appeal of hybrid cloud solutions is that it allows for an agency to attain desired business outcomes through combining services and capabilities in a way that promotes agility, is budget friendly, and secure. The hybrid model allows flexibility in terms of the length of use of each solution. Some applications may be required for only a short period of time, while others are used for years.
3. Organizational Impact- Take into consideration that hybrid cloud solutions are not traditional IT projects and their impact can be felt throughout an organization. Successful agencies have implemented coaching programs to help facilitate the change in technology and processes for their many diverse stakeholders.

2016 industry trends supported the practice of conducting an initial assessment of the current architecture and forming solid requirements. The requirements gathering process is not strictly specific to cloud - most of the points here might apply to any systems migration, even if the migration target is on-premise hosted. Industry leaders advise agencies to first identify services and/or applications to be migrated to a cloud host. The following steps should be taken:

- Conduct a thorough inventory of all current IT assets:
 - IT Infrastructure; server farms, etc., and their details -
 - Servers (including VMs) and their OS plus any middleware components
 - Facilities where infrastructure is housed.
 - Data connections for each infrastructure grouping and their capacity.
 - List each application's interfaces and all dependent systems.
 - Include existing systems that lie outside of IT control.
 - Applications, including:
 - Names of stakeholders for each application, including owners, systems administrators and end users.
 - Applications that can be migrated to a public vs. community vs. private cloud.
 - Current physical location of host and bandwidth availability.
 - Software licensing model (e.g., seats, servers, clients) for all applications, including cost and length of term OS, Storage, processing, database, libraries requirements.
 - Any configuration management programs and/or policies in place.
 - Network bandwidth requirements for each application, including connection type (e.g., VPN).
 - FISMA / FIPS PUB 199 impact level and security needs for each application.
 - Access controls and dependencies (e.g., MS AD, Method of Authentication and SSO).

- Consider number of staff and skill set needed to maintain the application (admins, programmers).
- The points of integration between the application and other systems.
- Email services, such as SMTP servers for receiving outbound emails generated by the application
- Identify network and systems monitoring tools used by your agency's Network Operations Center.
- Identify messaging queues such as an Enterprise Service Bus (ESBs) or other middleware.
- What other applications depend on data furnished by the application being migrated?
- IT Governance:
 - Consider how current on-premises compute resources are provisioned and allocated across the departments.
 - Identify who shall be delegated to review, approve, and execute the provisioning of cloud services.
 - Determine cloud services reporting requirements. How shall chargebacks to sub-departments for consumed cloud services be handled? This step must not be neglected. Lack of governance of cloud services will result in a hard to manage sprawl of cloud services and runaway expenses.
 - Include a requirement for a cloud center of excellence, to promote and govern use of cloud best practices and develop a core cloud services competency.

Once requirements have been identified, the next step is to consider the following cloud services which will help you identify the type of cloud service provider (CSP) needed.

- Virtual Machines – Operating system, number of CPUs, quantity of RAM per virtual machine -
 - OS requirements:
 - Storage Type and Amount - GB/TB per VM. GB/TB total, drive type (e.g., solid state), IOPs requirements (higher for some databases, lower for more static)
 - Does the CSP support its current on premises OS version?
 - Can the application be modified to run on the CSP supported OS's?
- Bandwidth:
 - Include segments from agency to host and from host to public users.
 - Network topology can potentially be much more flexible in the cloud and CSPs often have varying rates for bandwidth charges depending on source and destination.
- Cloud deployment models offered by cloud service providers (CSPs):
 - Private Cloud - the most secure but most expensive
 - Public Cloud - the least expensive but possibly less secure[1]
 - Community Cloud - a little more expensive and a bit more secure
 - Hybrid Cloud - a mixture of less secure cloud infrastructure combined with much more secure on premises infrastructure
- Hybrid system example: A website that distributes information to the public is based on data residing in an on-premise ERP system. The ERP system is too costly and too risky to migrate currently. The related and dependent systems are to be migrated in phases to mitigate risk of disrupting the ERP, thus a hybrid solution is pursued.
- Cloud service models offered by CSPs:

- IaaS - Infrastructure as a Service
 - PaaS - Platform as a Service
 - SaaS - Software as a Service
- Load balancing - As demand changes, servers can be added to or subtracted from the resource pool and traffic routed accordingly.
- Availability of a system or component expressed as 98%, 99%, etc. in a given year.
- Backup – A data copy that is sent to on off-site data storage service (could be another cloud services vendor.)
- Vendor Operation and Maintenance – Vendor to provide patching of operating system and/or other components plus change management processes.
- Once services are identified, consider how these cloud services will integrate with existing in house infrastructure and established in house staffing and operational processes.
 - For example, consider whether a CSP has the capability to leverage existing MS AD group policies and extend and integrate them into the new cloud infrastructure.
 - Identify current agency mission application workflow changes that may become necessary due to migration to cloud services.
- Identify current roles and responsibilities. Then identify roles and responsibilities changes necessary to incorporate cloud services.
- Identify new change management process that will include the cloud service provider (CSP). For instance, consider the CSP give before applying OS patches to the cloud host of a mission critical application.
 - Does the CSP offer these managed services (e.g. patching) or will a systems integrator (or your agency IT staff) provide them on top of the native CSP services?
- Assess existing staffing resources, redeploy staff or hire new staff. Consider how much cloud architecture experience an administrator of a cloud hosted database should have.
- Application support impacts -
 - Review system/application support documentation for changes needed by cloud hosting.
- Legal Impacts:
 - Transactional data subject to FOIA
 - Data subject to eDiscovery or legal holds
 - Federal Records Act compliance
- Security:
 - FISMA compliance
 - ATO generation and signoff
 - FedRAMP
 - Agencies are now mandated by OMB to utilize CSPs with a FedRAMP authorization, and some may now require CSPs with FedRAMP High Baseline for classified data hosting.
 - A FedRAMP authorization held by a CSP may be leveraged by agencies when crafting their own ATOs.
- Application design considerations:
 - Will applications in the cloud be optimized for the cloud, or will apps be migrated using a “lift and shift” approach?
 - It may be easier to just re-host applications to the cloud with no optimization, but those applications may not perform as well as newly built, cloud native applications that are cloud optimized. For example, some custom-built

applications may currently serve their purpose adequately. Even though they are architected for legacy on premise data centers, starting a fresh round of systems analysis, functional requirements gathering, and subsequent development to rebuild these applications may make little business sense.

- What is the life expectancy of the application?
- Would the application benefit from a migration to the cloud?
- How much elasticity is there to manage varying workloads such as seasonal demand peaks?

Execute the Migration

- Migration:
 - Unit testing in the cloud hosting environment.
 - Leverage cloud benefits for ease of environment deployment to configure separate instances for Sandbox, Development, QA/UAT, and Production (or however configured and named) environments.
 - Practice and write your deployment playbook based on the Sandbox configuration and refine as you repeat it through each environment.
 - Engage super users first and then end-users in user acceptance testing.
 - Consider load testing where applicable prior to production launch – these kinds of surprises are not welcome.
- Testing:
 - Dependent systems are operating.
 - Legacy dependent systems are no longer operating.
 - Acceptance testing and signoff by all stakeholders.
- Repurpose or decommission legacy on premises software and their support contracts.
- Repurpose or disposal of on premises servers, networking switches and routers, equipment racks.
- Decommission legacy facility physical plant, e.g., backup generators, UPS, cooling, fire suppression, data circuits, and service contracts.
- Termination of real estate leases

How GSA Can Help You Acquire Hybrid Cloud

GSA provides government agencies several options for acquiring IT and cloud services. Prior to contacting GSA, an agency should begin exploring as many of the unknowns as possible, narrowing down a desired outcome for the project. Your agency may be apprehensive about an enterprise wide approach or even the ability to migrate a huge amount of services. The best method is to leverage a modular contracting approach and start small with a single application as a pilot. Your organization may have a learning curve to leverage cloud computing services. So start small, conduct After Action Reports (AAR) following each migration, and use the lessons learned to improve the next migration. The compiled lessons learned will be invaluable to future success within your agency.

GSA Federal Acquisition Service (FAS) Cloud Computing Services (CCS) Program Management Office (PMO) recommends agencies take the following steps in their hybrid cloud acquisition approach:

1. Assess IT Requirements and Goals

2. Complete Market Research and Determine Scope for Migration

3. Define Technical Requirements, Security Requirements, SLAs, Transition Process to New Vendor

4. Establish Governance Process: Establish and conduct periodic performance reviews, plan, monitor, and control costs based on usage.

5. Complete Acquisition Life Cycle: Develop contract solicitation, evaluate vendor proposals, identify terms and conditions, evaluate vendor technical response against technical evaluation criteria, complete source selection process (rate vendors), award contract.

GSA FAS CCS PMO can help your organization with the best IT acquisition practices either through the GSA Alliant, IT Schedule 70's Cloud SIN, or other contract vehicles. The CCS PMO can help evaluate your agency's need and direct you to the appropriate Federal contracting office.

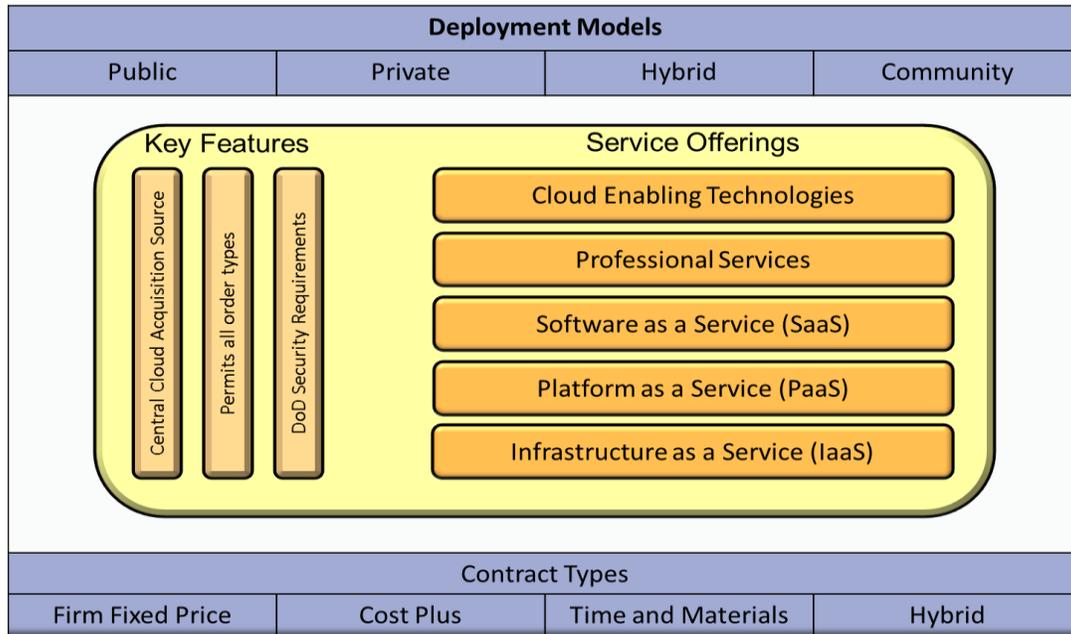


Fig 17. GSA Contract Vehicle Types Available for all Civilian and DoD Federal Agencies

GSA acknowledges the primary challenge for the acquisition professional is to shorten the procurement lead time as much as practical. Shortening the lead time enables maximized benefit of the modular approach through successive single-award contracts needed to continue pilots. Modular contracting (FAR 39) deconstructs complex problems into manageable portions of work compared to the traditional approaches that define every requirement and outcome up front. Successful application of modular IT development and contracting also requires a commitment to take advantage of Integrated Product Teams (IPT), and understanding what structures, strengths, and, processes are currently in place to enable IT acquisition within your organization.

Benefits of modular contracting are:



Figure 18. Benefits of Modular Contracting

Below are some fundamental acquisition concepts to take into account:

Envision	Evaluate	Outline	Design
<ul style="list-style-type: none"> • Determine business values and goals • Determine a cloud direction • Define scope 	<ul style="list-style-type: none"> • Conduct GAP analysis • Prioritize workloads 	<ul style="list-style-type: none"> • Cloud delivery strategy • Architectural parameters 	<ul style="list-style-type: none"> • Business case • Governance and organizational impact • Cloud design • Management framework
Initial roadmap-----> Current state----->Portfolio planning----->Transition plan			

And begin by asking yourself these two questions:

- 1. Is hybrid cloud the right model?**
- 2. What will make us successful at implementing a hybrid cloud architecture?**

Once these questions are answered for your agency, you can then proceed with determining whether a hybrid cloud provides enough business value by determining:

1. What are the gaps in capabilities between legacy and cloud systems?
2. How can I close my gaps?
3. Which workflows can move to the public and private clouds, respectfully?
4. Which workflows cannot move to the public and private clouds, respectfully?
5. How will the workflows perform in each cloud composing your hybrid infrastructure?

Next review contract Types. While the method of procurement is a concern for your organization there are Pros and Cons to each contract strategy.

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.

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.

Requirements-type vehicles. Requirements contracts are addressed in 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.

Standalone – contracts. Stand-alone contracts are ideal to support modular contracting (FAR 39.103) and 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 organization.

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 Cloud Service Provider (CSP). While the evolving strategy supports reduced priced reductions, the trade-off is the agency has less visibility into the procurement process.

Used for		Pros	Cons
Strategic and Shared Services	<ul style="list-style-type: none"> Commodity IT Services Single Applications Consolidation Initiative 	Reduced procurement time and potential for reduced savings (If fully leveraged)	Less control over metrics, Service Level Agreements, and Terms and Conditions
IDIQ	<ul style="list-style-type: none"> Enterprise Solution Multiple applications High demand / varied consumption 	Scale, scope, and service	Management of task and delivery order in a multi-vendor environment
Requirements	<ul style="list-style-type: none"> Commodity IT Services Closed Systems Storage and Data Processing 	Simple to administer better visibility into consumption habits	Greater potential for lock-in, but narrower in scope
Stand-alone contracts	<ul style="list-style-type: none"> Single Applications Cloud Support Services Systems Integration 	Reduced resource costs, priced competition, selection	Less procurement control and visibility, variation in "Brokerage" Definition
Cloud Brokers	<ul style="list-style-type: none"> Commodity services Single applications Storage and network 	Reduced resource costs, price competition, selection	Less procurement control and visibility, variation in "brokerage definition"

Figure 19. Advantages and Disadvantages of Contract Types

In addition, how your contract's funding is structured should also be considered. There are three (3) primary categories: firm fixed price, cost plus, and time and materials (labor hour). While cloud computing offers "pay as you go" contract structures which are 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. However, agencies may consider leveraging [FAR subpart 16.2](#), fixed-price types of contracts. Fixed price contracts provide for a firm price, or in appropriate cases, an adjustable price. Fixed-price contracts providing for an adjustable price may include a ceiling price, a target price (including target cost), or both. Below is a more detailed overview of different pricing structures:

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 either to protect the contractor and the Government 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. 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 organization’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	Used when stability of market prices or labor conditions during an extended period of contract period is	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

	could be adjusted if certain conditions change during period of performance	uncertain, and contingencies that would be otherwise be included in the contract price can be identified and separately addressed in the contract	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 RandD 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

Fig 20. (Types of Fixed-Price contracts)

Agencies may also want to leverage a Performance Based Acquisition (PBA) approach. Performance Work Statements (PWS) and Statements of Objectives (SOO) are two methods of defining work the Government desires to be accomplished. Under a PWS, performance based acquisition as defined in [FAR part 2.101](#) refers to structuring the aspects of the organization's acquisition around the purpose of the work performed, ensuring the requirements are clear, specific, and objective terms with measurable outcomes are provided. Using the SOO method, a Government-prepared document incorporated into the solicitation states the overall performance objectives and allows vendors to propose solutions to meet those objectives with the most flexibility to receive the most innovative offers. That portion of a contract establishes a broad description of the government's required performance objectives. Typically, the Program Management Office (PMO) or the Contract Officer Representative (COR) is responsible for developing the PBA documents in concert with a team of acquisition professionals.

2017 Closing Remarks

Although 2016 saw an uptick in hybrid adoption, and it appears agencies are beginning to realize the benefits of implementing cloud solutions, 2017 will still have challenges. The provisioning of cloud computing services is a cultural and organizational change. However, performance based acquisition and modular contracting are perfect for bridging the cultural gap. With performance based contracting, the agency can be more focused on the performance characteristics of the application, the service level agreement, and the desired outcome of the user experience. The organization will rely heavily on metrics and have a better grasp on the expectations of the system integrator and CSP. However, in order to prepare for hybrid cloud adoption, it is critical that agencies know the performance characteristics of their current architecture, and which applications and data belong in respectively different clouds based on security requirements. When addressed properly in the business case and CONOPS, the candidate SI and CSP can develop a solution that minimizes risk to the Federal Government, reduces cost, and creates an efficient, effective user experience. In modular contracting, the need for a system is satisfied in 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 system. Agencies may then continue increasing their procurements of cloud services both on-premise and within public clouds. All progress up until this point has clearly defined the character of cloud computing in the Federal Government. As the character continues to develop, the story will likely advance into application focused delivery and production in both on and off-premises environments.

References

1. GSA White Paper - Best Practices for Effective Cloud Computing Services - Procurement within the Federal Government - *Basic Steps for Public Sector Organizations*
<https://cmls.gsa.gov/servlet/servlet.FileDownload?retURL=%2Fapex%2FCMLSPubCategory%3FsearchKey%3DCA-0022134%26source%3D5-16-00339andfile=00Pt0000001RFhIEAG>
2. GSA Cloud Computing Services PMO Best Business Practices for Cloud Adoption
https://docs.google.com/document/d/1MNWTpXZp85_3tB0oUfUBvjBaHuFxmMdtK9zHA2LagFKM/edit
3. IDC FutureScape: Worldwide Cloud 2016 Predictions — Mastering the Raw Material of Digital Transformation <https://www.idc.com/getdoc.jsp?containerId=259840>
4. GSA White Paper - Cloud Computing IaaS Migration Roadmap for Agencies
https://docs.google.com/document/d/1sXBA_YmbpKr5kf6p0DLVtjw1Zt8XPhYsilEsFfIXmvg/edit
5. Eleven Critical Cloud Predictions to Take into 2016 <https://www.oracle.com/cloud/cloud-predictions.html>
6. The National Law Review - CIO's Five Cloud Computing Predictions for 2016
<http://www.natlawreview.com/article/cio-s-five-cloud-computing-predictions-2016>
7. 5 Cloud Computing Predictions for 2016 <http://www.cio.com/article/3024329/cloud-computing/5-cloud-computing-predictions-for-2016.html?page=2>
8. Cloud Computing Trends 2016 State of the Cloud Survey Results
<http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey>
9. 5 IT Industry Predictions for 2016 From Forrester and IDC
<http://www.cio.com/article/3006976/it-industry/5-it-industry-predictions-for-2016-from-forrester-and-idc.html>

Appendix 1: GSA Tools for Hybrid Cloud Solutions

[GSA Cloud Special Item Number \(SIN\) Project](#) - shows all vendors who meet the NIST definition of cloud service provider.

[GSA IT Schedule 70](#) - Schedule 70 is an indefinite delivery/indefinite quantity (IDIQ) multiple award schedule, providing direct access to IT products, services and solutions from more than 5,000 certified industry partners.

[GSA Alliant GWAC](#) - Alliant, GSA's premier enterprise GWAC, provides flexible access to customized IT solutions from a large, diverse pool of industry partners. Alliant allows for long-term planning of large-scale program requirements.

Appendix 2: Cloud Reference Documents

Document Name	Description
NIST Definition of Cloud Computing	Defines cloud computing and describes the five essential characteristics of cloud computing.
NIST Cloud Computing Standards Roadmap	Includes the reference architecture and discusses standards for government wide adoption as well as use cases and standards gaps.
NIST Cloud Computing Reference Architecture	Presents the NIST Cloud Computing Reference Architecture (RA) and Taxonomy (Tax) that will accurately communicate the components and offerings of cloud computing.
NIST Cloud Computing Related Documents	Listing of all other cloud related documents.
GSA Hybrid IT Strategy	Discusses agency hybrid cloud adoption use cases, benefits, and risks. Provides recommendations for building a hybrid cloud.
GSA Cloud Governance Considerations White Paper	Describes cloud computing governance framework considerations for federal agencies.
GSA Draft: Guide to Cloud Computing Adoption and Migration	Prototype paper on cloud computing adoption. In draft.
GSA Cloud Computing Best Practices	Federal Agency's Best Practices Document for Cloud Computing Procurement.
GSA Hybrid Cloud Implementation Checklist	A basic implementation checklist to increase the chance of success with federal hybrid migrations.
Gartner Article: The Final Case for Moving to the Cloud	Confusion around financial impacts is slowing down the adoption of cloud by organizations. While using cloud can increase operating expenditure costs, CIOs should consider other financial factors before making a decision about whether or not to adopt cloud. Developing business cases.
Gartner Article: Solution Path for Evolving From Server Virtualization to Private Cloud.	Evolving existing virtualized infrastructure to an automated and service- oriented private cloud delivers many benefits. This Solution Path outlines the organization and technical requirements as well as practical steps necessary to architect and build a private cloud solution.
Gartner Article: How to Optimize Your Network for Hybrid Cloud	The data center is not the center of the world anymore. Before the era of hybrid cloud computing, enterprises optimized their WAN for data center connectivity. This document guides cloud architects on optimizing WANs for IaaS and SaaS connectivity and evaluates emerging technologies such as SD-WAN.
Gartner Article: Hosted Private Clouds; The Guide to Building It Yourself	A private cloud is expensive and complex to build. Enterprise architects can solve these issues by utilizing a hosted or outsourced private cloud offering. This document analyzes the strengths and weaknesses of hosted or outsourced approaches and the major types of offerings available.
Gartner Article: Cost Optimization in the Age of	Many organizations are already behind the curve in terms of funding digital business. An economic slowdown further

Digital Business	threatens organization's' ability to make these investments. CIOs should be proactive about IT and business cost optimization to fund digital business.
Gartner Article: A Three Part Approach to Jumpstart Your Cloud Strategy	Best practices to guide cloud adoption.
OMB Memo for Heads of Executive Departments and Agencies, Subject: Data Center Optimization Initiative (DCOI), August 1, 2016	Memo calling for transition to the cloud to optimize data centers and to report on progress.
OMB 25 Point Plan to Reform Federal IT	Describes mandated shift to “cloud first” policy.
Federal Cloud Computing Strategy	Discusses how the government will implement the “cloud first” policy.
Federal Information Technology Shared Services Strategy	Underscores the need for cloud-based shared services.
The Digital Government Strategy	Mandated by President Obama in 2012, this strategy provided a 12 month roadmap for Federal Agencies to ensure their services are accessible to citizens through any platform or device.
The Common Approach to Federated Enterprise Architecture	Promotes increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies. This includes principles for using EA to help agencies eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among government, industry, and citizens.