Strategic Cloud (IaaS) Contracting Best Practices

GSA Office of Technology Policy and the FinOps Foundation
Cloud Acquisition Working Group

October 2023

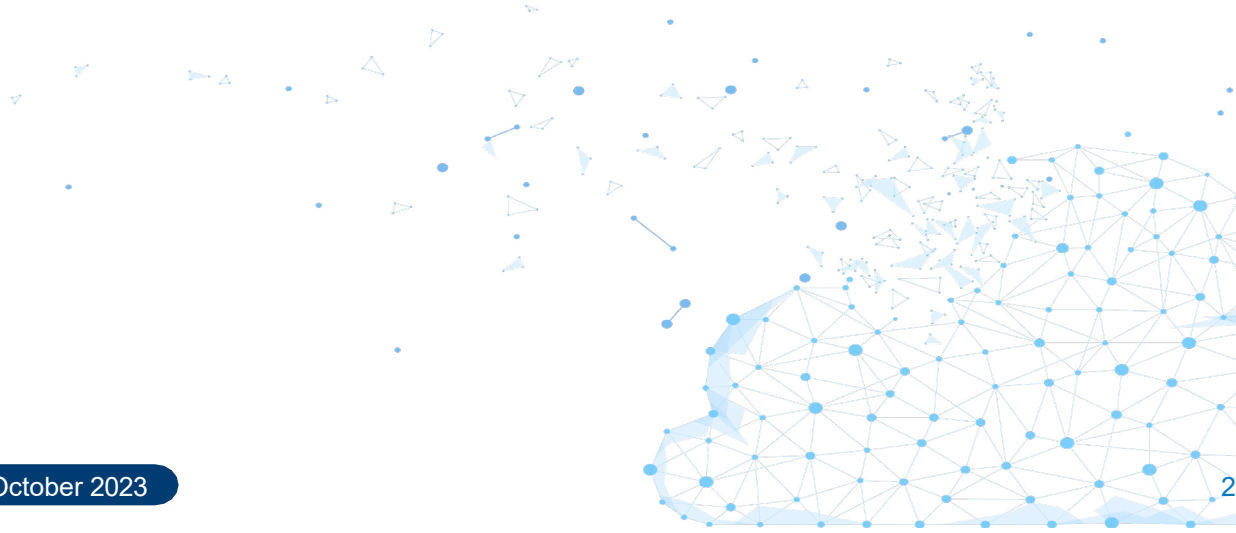


Table of Contents

Introduction

This document is sponsored by GSA Office of Technology Policy, GSA IT Vendor Management Office and the FinOps Foundation as a quick reference guide on cloud acquisition best practices. The scope of this document is limited to Infrastructure as a Service (IaaS) and the primary Cloud Service Providers (CSP) of IaaS services. This document's objective is to outline the most effective means to purchase cloud at the best possible price through MAS IT and SEWP schedules.

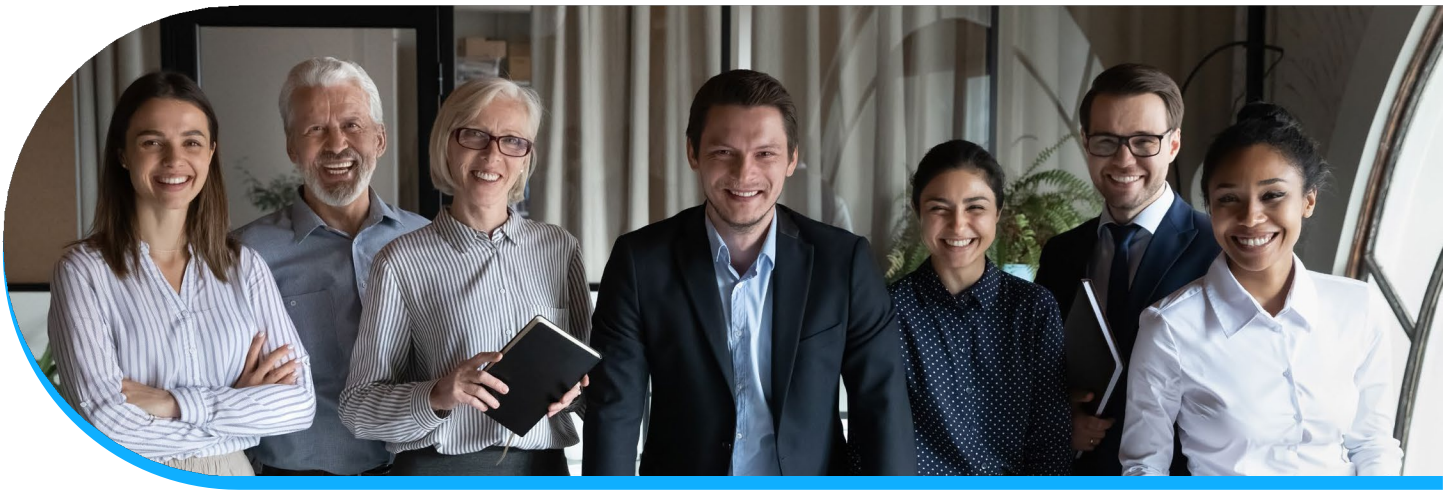
Cloud computing, particularly Infrastructure as a Service (IaaS), represents a transformative shift in compute and storage for information technology. Unlike traditional computing models that rely on local servers and infrastructure, IaaS enables organizations to access and manage computing resources over the internet, much like a utility service. In essence, it provides a virtualized environment where users can procure and scale computing resources dynamically, including virtual machines, storage, and networking, on a pay-as-you-go basis. IaaS eliminates the need for businesses to invest heavily in physical hardware and infrastructure, allowing them to leverage the computing power and storage capabilities of remote data centers. This not only fosters flexibility in adapting to varying workloads but also facilitates cost efficiency by shifting the burden of infrastructure maintenance and upgrades to the service provider. Ultimately, IaaS empowers agencies to focus more on their core operations, modernization, and innovation, unburdened by the complexities of managing and maintaining extensive on-premises hardware.

NOTE: This document outlines procurement of commercial cloud services and makes mention of cost reimbursable contract types which may be applicable to organizations not bound by the Federal Acquisition Regulation (FAR). Cost Reimbursable Contract Types are prohibited by the FAR as per FAR 16.301-3 Limitations Section (b) The use of cost-reimbursement contracts is prohibited for the acquisition of commercial products and commercial services (see parts 2 and 12)

Audience

This guide is specific to Infrastructure as a Service (IaaS) and is designed to support individuals with novice to intermediate knowledge of IaaS procurement in relation to Cloud Service Providers (CSPs).The guide is intended to increase awareness of nuances in infrastructure acquisition and to be a complement to other cloud acquisition resources (linked in the reference section), such as the Cloud (SIN) 518210C Ordering Guide which provides general information that we also reference within, however, this document goes into additional detail specific to IaaS. Contracting Officers, Contracting Officer Representatives, Program Managers and other acquisition professionals considering cloud computing services can benefit from
this guide.

This guidance is applicable to all Government actions regardless of the entity being required to follow the FAR or the type of acquisition action.



Acquisition Approach

Enterprise Contracting: Whenever possible contracting for IaaS cloud services should be done at the enterprise level, under the CIO, to maintain the most control and most consistent pricing across all constituent groups. It is important to note that the act of executing IaaS at the enterprise level on a contract does not necessarily provide the “best rates”. As a general practice to secure the “best rates”, IaaS purchases in bulk (ex. via a single task order, CLIN, etc.) offer the best possible rates because of the opportunity to discount at an aggregated volume. Therefore, even if contracting is not at the enterprise level it should pool resources as appropriate to achieve volume discounts.

As an example, the Department of Defense (DoD) has created the Joint Warfighting Cloud Capability (JWCC) contract. All current cloud capabilities will move to JWCC as their current contract period of performance expires and DoD organizations will use JWCC for any new cloud requirements going forward. Additional contracting options may include:

1. **Multiple and Single Award Indefinite Delivery/Indefinite Quantity Contracts (IDIQ) (FAR 16.504):** IDIQ contracts provide for an indefinite quantity, within the stated limits, of supplies or services during a fixed period. This type of contract is best used when the Government cannot determine, above a specified minimum, the precise quantity of supplies or services the Government will require during the contract period. The contract includes maximum and minimum quantities the Government may order. IDIQs allow for acquisition of broad-ranging cloud projects through single or multiple providers, under which the work is parceled out through separate task orders for different requirements within the

scope of the IDIQ and at different security levels authorized under the IDIQ award (i.e., Unclassified, Confidential, Secret, Top Secret) falling under the Federal Information Processing Standards (FIPS) 199 for categorization of federal information systems (e.g., Low, Moderate, High)) as particular agency needs are identified.

a. Cloud Considerations: IDIQs provide the framework for enterprise-wide solutions that support scalability and elasticity; multiple applications; high demand; and allow for varied consumption based on specific Government requirements.

b. Advantages: Firm-Fixed-Price (FFP) option for multiple award; simple to administer; streamlined ordering process for award of task/delivery orders; satisfies recurring requirements; reduces administrative efforts by eliminating repetitive, individual orders and payments. Multiple Award IDIQ continues to promote competition at the task/delivery order level to ensure a fair and reasonable price. Additionally, Multiple Award IDIQ contracts provide a framework that preserves competition for price, services, and features while ensuring the Government retains access to the new improvements and
most innovative technologies from multiple approved cloud providers already under contract. Acquisition teams, along with the Government Customer, will have the flexibility to compete and select the cloud architectures and solutions that best meet their specific requirements. Finally, a Multiple Award IDIQ helps mitigate the risk of “vendor lock”.

2. **Blanket Purchase Agreements (BPAs) (FAR 13.303 or 8.405-3 General Services Administration (GSA) Multiple Award Schedule (MAS)):** A BPA is a simplified method of filling anticipated repetitive needs for supplies or services. The Contracting Officer can establish a Division/Program specific BPA under FAR 13.303 or under the GSA MAS IAW FAR 8.405.3. BPAs are established when there is a wide variety of items in a broad class of supplies or services, but
the exact terms, quantities, and delivery requirements are not known in advance and may vary considerably. Once the exact requirements are known, the Contracting Officer then issues a request for quote resulting in the award of a binding Order. BPAs may be established as a sole source or as a multiple award for services of the same type to provide maximum practicable competition. The difference between “traditional” BPAs and BPAs established under the GSA MAS is that “traditional” BPAs are subject to the requirements of FAR Part 13. FAR Part 13 does not apply to GSA MAS BPAs. GSA manages several Governmentwide MAS BPAs that are consolidated to address specific needs identified across Government agencies.

   a. Cloud Considerations: The GSA MAS Information Technology Category (ITC), Special Item Number 518210C, Cloud Computing and Cloud-Related IT Professional Services, offers commercial cloud services (IaaS, SaaS and PaaS) and cloud IT professional services, which the Government[1] may use to establish a BPA.

   b. Advantages: BPAs provide convenience, efficiency, reduced costs, and a simplified ordering process. BPAs offer shortened acquisition lead times; satisfies recurring requirements; promotes competition at the Order level. Under GSA MAS BPAs, the BPAs inherit the GSA MAS and SIN level Terms and Conditions (T&C). The Government can incorporate any additional terms and conditions required in the awarded Order as long as they do not conflict with GSA’s MAS and SIN T&C.

Acquisition Requirements and Strategy

Cloud computing is an evolving paradigm and the offerings within today’s commercial Information Technology (IT) environment have far-reaching impacts for the Government and the Contractor. It’s crucial for Government acquisition and IT professionals to prepare an overarching cloud computing acquisition strategy that best suits the organization’s requirement and achieves its objectives.

1 Eligibility determination

In shaping a future cloud computing procurement, the acquisition team should immediately conduct a detailed requirements review to assess:

1. Various work needed to migrate and integrate applications, services, and data[2].
2. Required storage, access, control, and retention of the applications and data.
3. Potential use of currently available cloud enterprise solutions or common applications and services, which may have already been invested and may have centrally funded some portions.
4. Required cyber security and security information impact levels[3];

A poorly understood and translated cloud requirement may invite a protest and claims from contractors due to ambiguity about the organization's actual needs. In concert with the above four (4) key assessment areas, the team should also begin to identify and document the skills required to effectively support migration, modernization, and refactoring initiatives, as they are key factors for success:

a. Inventory of the organization's "as is" IT architecture; acquisition teams should recognize that their applications may have linkages and data dependencies that have far wider impact than the application itself.

b. Rationalization of the existing inventory and applications to determine if refactoring and migrating to a new platform, retaining its legacy platform, or sun setting (retiring the application) is required.

c. Baseline for the requirement and strategy against the potential cloud solution models and desired outcomes/deliverables/objectives (including any multi-cloud elements such as CSP-to-CSP considerations).

d. Developing a forecast and budget that accounts for existing cloud growth, additional migrations to the cloud and any net new cloud native applications

e. How to procure the requirement, e.g., as a service.

f. Application Program Interface (API) and Non-API integration requirement, which may signal the need for development activities, additional work beyond the commercial offering, and /or multiple fund types for the procurement.

g. Potential cloud offerings to ensure conformance with the agency specific requirements, as well as other Federal requirements: e.g., Federal Risk and Authorization Management Program (FedRAMP) certifications, record retention rules, Continuity of Operations (COOP), and statutory obligations.

h. Applications and/or data migration is appropriately approved for migration to a commercial cloud environment.

i. Risks, in coordination with the Network Enterprise Center (NEC) management agency, concerning any expansion of the cloud-based solution, network traffic or having potentially more intricate features that may impact or cause disruption of the networks.

j. Potential terms and measurements required within the SLAs, which may include military unique requirements, protocols, and specifications, e.g., security, encryption, timing, outages, and integration.

k. Program plan with schedule to track the sun setting, migration, and deliverables (e.g., applications should have a documented lifecycle management plan).

l. Federal contract instrument that currently exists, which can potentially meet the requirements and strategy.

2 The application rationalization playbook provides additional guidance

3 FIPS 199 Standards for Security Categorization of Federal Information Systems

3.3. Commercial Acquisition Procedures: To the maximum extent practicable, the acquisition team should consider the use of commercial acquisition procedures provided in the FAR. In deriving the inherent full flexibility and evolving opportunities offered by CSPs, market research is critical to making an informed commercial determination on whether the cloud solution services are best acquired under FAR Part 12 to deliver the intended requirement and operational effects. In addition, the commercial determination must adequately describe how the use of FAR Part 12 procedures address the program and cost risks. The Contracting Officer is responsible for making a Commercial Item Determination (CID) in writing that an acquisition over $1 million meets the commercial item definition in FAR 2.101.

Different acquisition requirements may be based on the acquisition vehicle type. There may be others in addition to the reference of FAR 12, FAR 15 Contracting by Negotiation (e.g., Alliant) and for GSA MAS FAR 8.406-1 Order Placement.

Contract Structure

Cloud Service Providers (CSPs) provide mechanisms to relate accounts/subscriptions/tenancies to each other and align them hierarchically to how they will be consumed and funded. Agencies can take advantage of the CSP's optional account/sub account (i.e. management account/member account, account/subscription, etc.) structure to maximize buying power and discounts. This approach can reduce costs overall and yet preserve the autonomy of individual bureaus or agency components independently funding, operating, and managing their cloud instances.

Recommended Contract Types and Ordering Instruments: Federal Acquisition Regulation (FAR) Part 16 identifies multiple contract types available to the Government in formulating the acquisition strategy for a cloud computing implementation. Cloud computing requires a formal instrument, such as contract or Other Transaction Authority (OTA) (where applicable) type, service agreements, and approaches that promote the essential elements of cloud: flexibility, metering and measuring performance, paying for what is used, and responsiveness. There is no straightforward answer on what contract type to use; the Contracting Officer, in coordination with the Program Manager and Mission Partner, should apply innovative thought, along with their planning and risk considerations in determining the contract type.

However, if an existing acquisition vehicle is being used (e.g., GWAC, MAS) those acquisition vehicles have defined allowable contract types under the acquisition vehicle so not all contract types are available under all acquisition vehicle (GSA MAS Fixed Price, Labor Hour, T&M, Hybrid). Additionally, allowable contract types are fixed priced, requirement contracts, and labor hour. Risks may include unforeseen increase or decrease in users, over or under payment for services, downtime (unplanned outages), security and privacy, limited control and flexibility, and unknown third-party agreements.

The below sections describe contract types with cloud considerations and potential advantages associated with each option.

1. **Firm Fixed Price (FFP):** A FFP contract provides a price that is not subject to any adjustment based on the Contractor's cost in performing the contract. This contract type places maximum risk and full responsibility for all costs and resulting profits or loss on the Contractor. It provides maximum incentive for the Contractor to control costs and perform effectively and imposes a minimum administrative burden upon the contracting parties. The contract price is the price proposed, with no incentives or fees added. Cost responsibility is placed wholly on the Contractor. FFP is the preferred type when cost risk is minimal or can be predicted with an acceptable degree of certainty. In contrast, FFP contract may not be the best contract type for refactoring or migration work based on the potential uncertainty and risk associated with the work.

    a. **Cloud Considerations:** FFP may be appropriate for the IaaS cloud computing models when there is no labor required and may provide an ability to aggregate cloud spend to negotiate larger volume discounts. When labor is required, the Contracting Officer may use a Labor Hour Contract / CLIN for better flexibility. Additionally, based on the evolving cloud environment, Contracting Officers should consider whether the FFP type will allow the Government the best flexibility and use of the cloud's characteristics, such as improvements on infrastructure, rapid elasticity, measured service, and on-demand self-service.

    Firm Fixed Unit Price: The Contracting Officer can also consider use of a Firm Fixed Unit Price contract, as an alternative. This approach fixes the unit price for a catalog of services, however, allows the Government to modify the volume of the work and only pay for actual utilization. This contract type would allow for better implementation of the cloud characteristics (utility based, self-service). However, in this methodology some burden rests on the Government as it is imperative that the Government closely monitor usage of the cloud infrastructure to ensure the ceiling is effectively managed.

    b. **Advantages:** Easy to administer; forces CSP to control costs; prevents cost overruns by the CSP; potential better discounts with larger purchases; CSP assumes all the risk

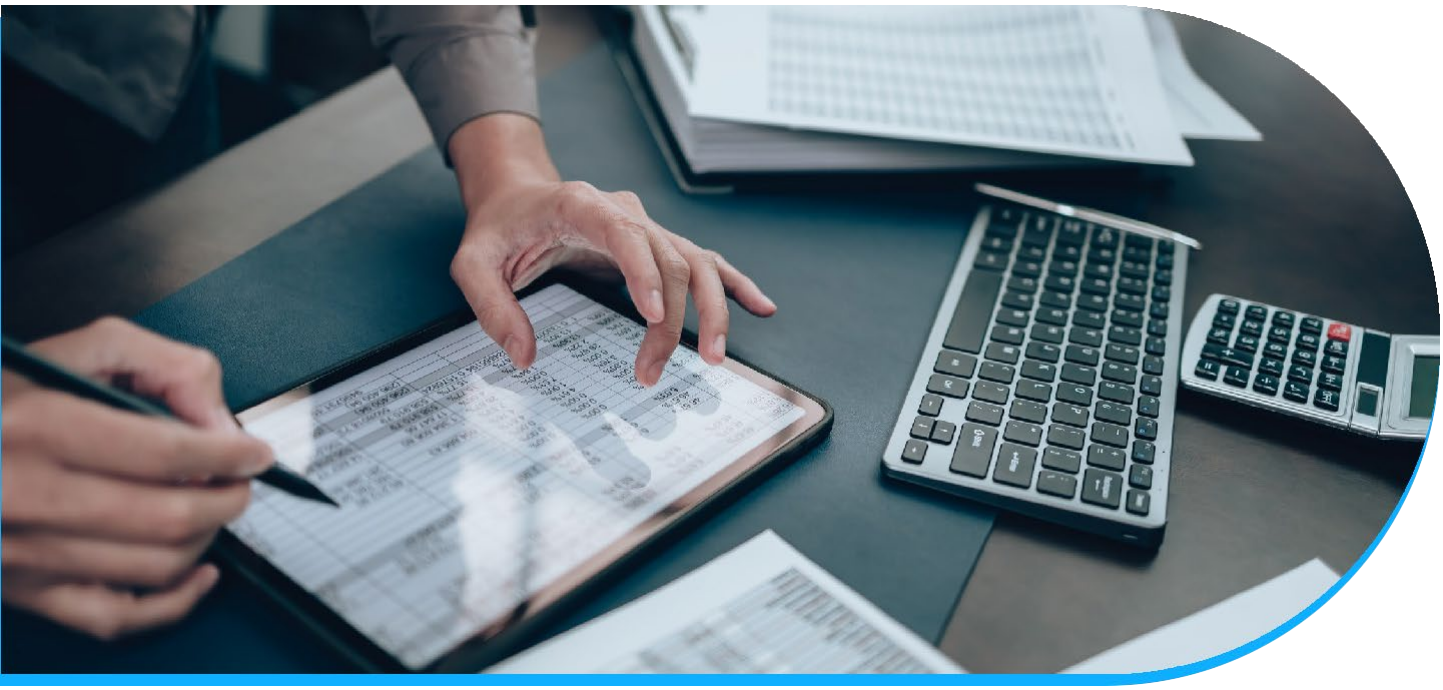
2. **Fixed Price Contract with Prospective Price Redetermination:** This type is best used in acquisitions of quantity production or services in which it is possible to negotiate a fair and reasonable firm fixed price for an initial period, but not for subsequent periods of contract performance. A fixed-price contract with prospective price redetermination provides for a firm-fixed price for an initial period of contract deliveries or performance and prospective redetermination, at a stated time or times during performance of the price for subsequent periods of performance. This type of contract is helpful when the Government and the Contractor can agree on an arrangement in the short term, but there are concerns about the arrangement in the long term. The initial period should be the longest period for which it is possible to negotiate a fair and reasonable firm fixed price. The Contracting Officer should include in the contract the stated times during contract performance when the price for the next period will be determined. Redetermination periods should be at least 12 months long.

    a. Cloud Considerations: Fixed price with prospective price redetermination is suitable for any cloud solution model because of the ability to control the Contractor's price during the contract's life. Depending on the pricing model used, cloud computing prices such as usage, time, or content can fluctuate, and allowing for interval price redetermination can be a cost savings over the long-term.

    b. **Advantages:** Ability to negotiate a fair and reasonable FFP for the initial contract period (i.e., 12 months/base year) and then subsequent redetermination periods. Establishes price redetermination periods to negotiate a fair and reasonable FFP price; forces the CSP to control costs and prevents cost overruns by the CSP.

c. **Disadvantages:** The contract type shall not be used unless negotiations have established that the conditions for use of a firm-fixed-price contract are not present (see 16.202-2); and a fixed-price incentive contract would not be more appropriate. Additionally, the prospective pricing periods must be made to conform with the operation of the contractor's accounting system; and there is reasonable assurance that price redetermination actions will take place promptly at the specified times.

Pricing Model



Negotiated Discounts

One large agency has been able to achieve significant negotiated up-front discounts from each vendor's published price. Some agencies have reported discounts from 15% to 38% depending on provider. All contracts should contain an upfront negotiated discount off list price. In most cases any additional discounts associated with Reserved Instances or Savings Plans add to this baseline discount.

There are also tiered discounts available from most CSPs that can range from 5% to 15% based on annual consumption. Tiered Discounts should be explicitly called out and defined at the order level … tiers should be defined either on monetary levels or specific usage levels (e.g., 100 GB). They should also define exactly what account holders and what services count toward the tier calculation. Do not leave it open to the interpretation of the vendor. It is also recommended that discounts and tiers be broken out by major categories (e.g., compute, storage, transport) to ensure the agency gets the best discount across the offerings. Discounting practices vary significantly between cloud service providers. AWS often offers detailed discounting options by individual service, while Azure is less inclined to offer such detailed discounts.

For example, a vendor might be able to offer a 20% discount on storage services but only a 5% discount on compute services. Without the flexibility to apply discounts at this detailed level, you might end up with an overall discount constrained by the lowest available discount (e.g., 5%). Therefore, agencies should have a clear understanding of their cost drivers and prioritize negotiating discounts in those key areas to maximize their savings. If you use more high-performance compute vs storage and egress, you want to focus on your compute costs over storage and transport costs.

Cost and Price Considerations: The term "costs" is used interchangeably throughout this Section to mean the total cost and total price of a cloud solution with the understanding that in FAR based acquisitions, there are different cost and price analysis techniques.

- As referenced above, at this point the cost and pricing are established as part of the environment and the Government has already negotiated the cost and pricing structure based on collective buying power.
- There is the potential for major cost savings benefits to commercial cloud computing. However, there is also the risk of overlooking potential hidden costs, which may be obscured in the solution providers' pricing structure, if the Request for Proposal (RFP) or Request for Quote (RFQ) is not properly structured, and the proposals are not thoroughly evaluated. First, commercial cloud computing allows the organizations to pool resources and pay only for the computing capability that they use. As mentioned, the Government and the CSP should monitor, control, and report in a transparent manner, all resource usage. Second, the costs of implementing a cloud computing environment includes more than just servers and storage. CSP may charge additional costs for ancillary requirements such as IP addresses, domain strength, data transfers into and out of and between the servers, security, management, patching, and back-up. Many organizations may not be aware of certain egress fees. These can include costs associated with data transfers between regions, between availability zones (AZs), and between virtual machines over the internet. CSPs charge fees for data transferred to the cloud and associated labor costs with synchronizing the Government's data to be transferred from the legacy system to the future cloud model. The acquisition team will also want to consider the potential need for Government employees to continue using legacy applications and data while the future cloud solution model is being stood-up. This latency will have budget implications as the organization continues to fund existing operations, while simultaneously funding CSP contracting activities until switching to the new cloud environment.
- The cloud computing industry is a competitive market with CSPs offering many common services using similar, as well as different package and pricing methods; thus, the opportunity for competition and competitive pricing exists at all levels. The CSP's utilize various formulas to calculate their prices. When determining price, the Contracting Officer must be cognizant of how the CSP designs the package and formulates the proposed price of the cloud solution models. The CSP tends to focus on what the CSP can provide the Government, rather than what the Government requires. Unless the Contracting Officer requires the CSP to propose the same pricing method, the CSP pricing models are in favor of the CSP and possibly provide additional cost and capability not required by the Government. It is also important to understand that certain requirements are better suited to one CSP over another. For example, it is unlikely that any organization would use AWS for a Microsoft Active Directory service.
    - **Equitable Cost Comparisons:** The goal is to perform a "like-to-like" analysis of the CSPs' proposed prices/costs. If not, the Contracting Officer will struggle in determining what cost elements the CSP used to formulate the proposed price. This can be a very tedious and time-consuming task especially if Offeror's fail to propose a price for each element. Use of a standard cost/price template is the optimal approach. CSPs competing for the same business need to propose costs using the same method. Costs should be provided as unit costs per service or utilize a Universal Product Code UPC. It is important to avoid bundled or 'lot' pricing. The use of a standard cost/price template, which references the required elements from the solicitation or RFP, where the CSP annotates their proposed price/cost (direct and indirect) data may help ease the Contracting Officer's burden in performing cost and price analysis. The CSPs have multiple price/cost elements to include but are not limited

to hardware, usage rates, data management, professional services (labor), technical support, and maintenance. The CSP elements may be calculated by volume and or on an hourly, daily, monthly, or yearly basis.

*Note: *Any expected quality above the normal commercial offering may influence price; higher quality and performance demand levels tend to increase price. The Government must identify the quality required and its description and measurement within the SLA. SLAs are important instruments to hold the CSP accountable and can incentivize performance when properly structured, as well as protect the Government when the CSP quality levels decrease.*

- **Lowest Price Technically Acceptable (LPTA):** CSPs have pricing structures for calculating the price for the cloud solutions. LPTA is not likely at the CSP level due to technical capabilities specific to particular applications. This is a big part of the reason most agencies will support a multi-cloud environment. However, as with any acquisition, the goal is to obtain the maximum benefit (i.e., high quality) for the best price and if competition is amongst re-sellers of that solution the government is likely to achieve the best price.

- **Cloud Cost Calculators:** Cloud service providers (CSPs) offer cost calculators designed to estimate the expenses associated with an organization's current infrastructure. However, it is important to note that these calculators provide only a very rough approximation of costs. They typically do not account for factors such as Enterprise Discount Programs (EDPs) or other specialized discounting options, such as commitment-based discounts, including Savings Plans (SPs), Reserved Instances (RIs), or Spot Instances. As a result, the actual costs may differ significantly from the estimates provided. The more accurately an organization inventories and documents its current infrastructure and understands its future requirements, the more accurately the CSP calculators will estimate the cost for the cloud solution(s). The calculators generate cost based on the level of detail provided, such as hardware specifications (i.e., memory, storage type and size), applications, number of users, access speed to data, types of professional services. In addition, the calculators consider other variables or ancillary requirements as identified above. A generated report can itemize the cost elements and estimate the cost both monthly and annually.

The calculators can be used, in combination and without preference, early in the acquisition process to assist in the development of an Independent Government Cost Estimate (IGCE) and are available regardless of a CSP being selected. Acquisition teams may find the following CSP calculators useful[4]:

- Amazon Web Services (AWS) Total Cost of Ownership (TCO) Calculator and more in-depth monthly cost calculator
- Google's Cloud Platform Pricing Calculator
- Microsoft Azure's Pricing Calculator
- Oracle's Cost estimator
- Rackspace's Calculator
- IBM Bluemix's Calculator
- Others

4 There may be many other calculators available, and the ones mentioned do not constitute a government endorsement of any type.

Pricing Structures

CSPs offer multiple pricing structures with the goal of maximizing profit; however, due to the competitive cloud market, Contracting Officers should benefit from competition and negotiation of the variety of offerings. The goal of the Government is to receive a fair and reasonable price with a high quality of supplies and services. There is a wide range of pricing available and below are three (3) examples of the most widely used:

1. **Pay-Per-Use:** In this price structure, the Government would pay for what is used. The price can be based upon the time or quantity of a specific service. For example, storage may have various cost components to consider depending on the requirement; 1) storage pricing per GB; 2) request and data retrieving pricing; 3) data transfer and transfer acceleration pricing; and 4) data management features. There is a price associated with each of the components. As the amount of storage and/or number of users increase, the Contracting Officer should structure the contract for price to decrease incrementally. This option is a good candidate to combine with Teir / Volume pricing mentioned above.

2. **Consumption Usage-Based:** Using this price structure, the Government would receive a discount based on the volume of usage. For example, a "Sustained-Use-Discount" pricing built on the usage level offers multiple discounts depending on the requirement; however, the higher the usage during the month, the cheaper the unit price. The discounts are applied on incremental use after reaching certain usage thresholds which means the Government would pay for only the number of minutes that is used in that instance.

3. **Volume-Based:** Using this price structure, the Government would pay a price for user access within a range. Once the established range is achieved, access will then come at a lower price. For example, a volume-based price for company X, who is a third-party reseller of a CSP may offer multiple categories. i.e.: 1) standard; 2) premium; and 3) bring your own license volume-based pricing. Pricing is based on performance and expanded capacity for a wider range of users and applications.

Consolidated Billing Availability and Future Multi-cloud Standardization

In an organization, the management account is responsible for paying all member accounts' charges. An administrator of a management account with the appropriate permissions can view aggregated usage costs across all managed accounts. Consolidated billing combines the usage across all accounts in the organization to share the volume pricing discounts, RI discounts, and Savings Plans. Access to consolidated billing can generally be found in the CSP Billing and Cost Management console.

Commitment Based Discounts

A key to achieving better pricing is to provide CSPs with commitments for future use. From the cloud vendor's perspective, commitments allow them to better understand and plan the demand for their services. From a government perspective, the award of a Task Order is awarding a long-term commitment to the awardee if the base and options are executed. If the Task Order as a Total Period of Performance of 5 years, the Task Order pricing should by default align with pricing for 5-year RI. If the contractor continues to perform well it is highly probably the government will continue to execute the Task Order option periods.

In the commercial sector, RIs are used to tie the user to the CSP for a period of time … Vendor Lock-In … the Government in the issuance of a Task Order has basically locked the government into that vendor for the duration of the Task order therefore pricing should be commensurate with RI instance pricing of the same time period.

Reservations or Reserved Instances (RIs) and Savings Plans are the two most common types of commitments and apply to infrastructure and not licensing. Pricing models are similar between RIs and Savings Plans in allowing monthly, partial upfront or all upfront billing (Cloud computing services must be paid for in arrears in accordance with 31 U.S.C. 3324) arrangements. Savings Plans and RIs are available for 1- or 3-year commitments and billed per hour of consumption.

The key difference between RIs and Savings Plans are as follows:

RIs are purchased for a specific region and instance type, however there is some flexibility around the instance family. In some cases, an exchange marketplace is available to facilitate transitioning between instances. However, it's important to note AWS limitations regarding the resale of EC2 Reserved Instances (RIs) on this marketplace. Additionally, it's helpful to specify what constitutes "good" commitment-based coverage, typically ranging from 85% to 95%.

Savings Plans have greater flexibility where the only required information is choosing the scope, plan amount and the term. There is no need to choose a region or instance type. The Savings Plan will apply to the maximum discounted compute resource and will automatically adjust the savings to the applicable running resources. Be certain that any savings plan commitment is below the forecasted spend. An 80% watermark is a generally accepted practice to account for fluctuation in demand and prevent the commitment from exceeding the actual usage.

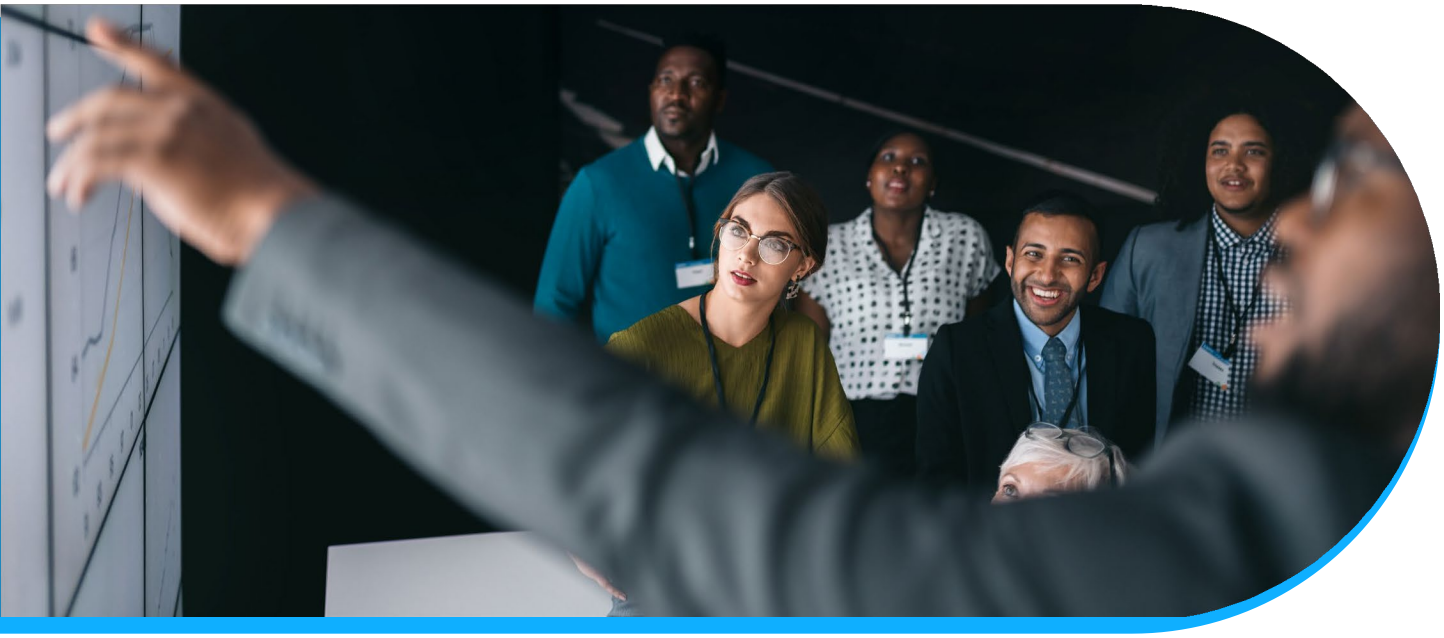
Currently, the Government is limited in its ability to make multi-year commitments, which have the best pricing. Example situations which have enabled the government to make these commitments and receive pricing associated with long-term commitments are from the Cloud SIN ordering guide which states:

- If using the Multi-Year Contracting special contracting method under FAR 17.1 an Ordering Activity could potentially award a 5-year Period of Performance (PoP) in accordance with the requirements set forth at FAR 17.1. A 3-year reservation could be executed anytime in the 1st and 2nd year, but once the contract was 2 years and 1 day into the PoP the Ordering Activity would not be able to execute a 3-year reservation since the reservation period would extend beyond the end of the PoP. Please note that Contracting Officers will need to work with the finance organization, OCAO, and legal counsel before using Multi-Year Contracting and reservations greater than one year.

Multi-year money

Multi-Year has been used for a three-year commitment but does require legal review in the contracting process. Typically, an organization can secure a 20% discount on top of other discounts. If this refers to an Enterprise Discount Program (EDP), it's worth noting that this level of discount is on the higher end of cloud spending and is not commonly observed in general cases.

Requirements



Performance and Availability

Defining and enforcing a Service Level Agreement (SLA) is paramount when implementing cloud computing. A cloud SLA is an agreement between a CSP and the Government that ensures a minimum level of service is maintained. It guarantees levels of reliability, availability, and responsiveness to systems, application owners, and data while also specifying who will govern when there is a service interruption and changes to services.

SLAs are extremely important to a government customer as the migration to cloud computing becomes more prevalent. A cloud SLA ensures the CSP adheres to defined enterprise-level requirements and provides the government customer with a clearly defined set of deliverables. The Contracting Officer should validate the SLAs are structured using robust terms, enforced through meaningful penalties, and monitored through effective reporting.

1. The SLA complements the awarded contract with the CSP and further sets expectations for the contractor relationship. The Contracting Officer, working in conjunction with the Subject Matter Experts (SMEs), must negotiate the SLAs to meet the Government's needs prior to contract award or signing the SLAs. The SLA and contract must be written to protect the Government's cloud computing investment and the SLA should be incorporated into the awarded contract at the time of award. It is important to note that there may be a cost to the government for an overly strict SLA and that the SLA should be tailored as a 'Minimum Viable SLA' for the services being provided.

    a. Contracting Officers should negotiate a measurable system and service-level availability targets based on the business criticality of the application and/or data required. The more mission-critical the application or data, the higher the acquisition team should set the service-level availability targets. An SLA will commonly use technical definitions that quantify the level of service. The awarded contract, with the incorporated SLA, must articulate precise quantifiable levels of service and service availability, as well as the recourse if the CSP fails to deliver the service as described. This allows the quality to be measured, reported, benchmarked and, when stipulated by the contract and/or agreement, rewarded or penalized accordingly.

    b. An SLA assessment is required for every new cloud computing requirement. The SLA is a living agreement, and as services change, the SLA must be reassessed. The SLA must be specific and measurable with a predefined schedule to review and modify as services change.

2. The following are additional considerations when creating the SLA with the CSP:

    a. Specify roles and responsibilities of all stakeholders with respect to the SLA, and, at a minimum, include the Government Customer (e.g., agency/program, etc.) and the CSP. These definitions would include, for example, the persons responsible for oversight of the contract, audit, performance management, maintenance, and security.

    b. Specify key measurable terms, such as the activation dates, service availability, down time, and maintenance time. Other examples include:

        i. Level of service (e.g., service availability—duration the service is to be available to the agency).

        ii. Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users).

        iii. Response time (e.g., how quickly cloud service provider systems process a transaction entered by the Government Customer, response time for responding to service outages).

        iv. Specify how and when the Government Customer will access its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA.

        v. Specify how the CSP shall return or transition Government Customer data, as directed by the Government, as the CSP's contract is modified, completed, or terminated.

c. Specify data requirements to ensure accessibility and protection of Government Customer data and its reuse, specific to:

   i. Location of the data (e.g., consistent with local legislation)

   ii. Access to the data (e.g., data retrievable from provider in readable format)

   iii. Portability of the data (e.g., ability to move data to a different provider)

d. Request and review the CSP's documented disaster recovery plan and continuity of operations plan to assess the compliance to the Government Customers requirement. The plan should address how and when the CSP is to report such failures and outages. In addition, it should state how the CSP will remediate such situations and mitigate the risks of such problems from recurring. Upon agreement, the plan should be incorporated into the contract.

e. Identify any pertinent exceptions the CSP claims do not apply to the measurements (e.g., down periods due to scheduled maintenance or updates may not apply when calculating system availability). Some CSPs exclude downtime related to third-party failures when calculating uptime. Additionally, CSPs may exclude "internet congestion and slowdown." As a result, access to the systems may be available, but no access to applications or data. Contracting Officers should document and understand the potential impact these exceptions may have on the "actual" performance and fine tune the SLA accordingly.

3. Specify metrics the CSP must achieve to meet the Government Customer's security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency's data). Specify the security performance requirements the CSP is to meet. This would include describing security performance metrics for protecting data, such as data reliability, data preservation, and data privacy. Clearly define the CSP and Government Customers access rights, as well as their respective responsibilities for securing the data, applications, and processes to comply with federal requirements.

a. Describe what would constitute a breach of security and how and when the CSP is required to notify the Government when the requirements are not being met. Specify performance requirements and attributes defining how and when the CSP is to notify the Government when security requirements are not met (e.g., data breach occurrence). Ultimately, the government must document the severity of security breaches and the CSP's remediation to ensure there is no recurrence.

b. Explicitly for DOD organizations, the Defense Information Systems Agency (DISA) Provisional Authorization (PA) for cloud services is the additional security validation for IaaS PaaS and SaaS services that have a Federal Risk and Authorization Management Program (FEDRAMP) approval, but the DoD wants to authorize them for use at Impact Level 4 and higher. DOD uses impact levels, which are based on the type of data to be processed, to assess a provider's offering. These impact levels range from level 2, publicly releasable and non-mission critical unclassified information, to levels 4-6 which address controlled unclassified information and other information categories that require higher levels of protection. If the cloud service provider is able to demonstrate compliance with the FedRAMP moderate controls, that vendor is provided a DOD PA at impact level 2 for their cloud service offering. Subsequently obtaining a DOD cloud provisional authorization at impact level 4 requires meeting about 10 percent more controls than the 325 FedRAMP controls.

4. Specify a range of enforceable consequences, such as penalties, for non-compliance with SLA performance measures. Identify how the Government will impose and exercise enforcement mechanisms. Penalties and remedies are a must to enforce compliance with contract terms when situations arise. Further, implementing meaningful penalties clearly incentivizes Contractors to maintain a high level of performance.

    a. Define consideration for the Government if the CSP fails to meet the terms and conditions of the SLA. A CSP can offer a tiered service credit plan that provides the Government credits based on the discrepancy between SLA specifications and the actual service levels delivered. Service credits should be at least proportional to the decline in the level of performance and act as an incentive for the Contractor to improve quality and availability of the services. The CSP may offer credits up to 100% of the monthly fees; however, the availability may have to fall to a very low level, such as a drop of 50% availability for a particular month, before reaching the CSP's established standard offering. Simply, service credits differ between CSPs with some Contractors providing no credits, while others may provide 100% of the monthly subscription fees paid if the system uptime falls to 95%. Finally, the tiered service credit plan for non-performance should be defined in the awarded contract.

5. The SLA should specify any routine reporting and meetings, such as a biannual meeting with both the Government Customer and CSP to review results of system testing, incidence of service outages, mitigation actions, SLA compliances, and actions taken by the Contractor to improve the services. Further, the Contracting Officer should specify in the contract and/or SLA the requirement for the service management reporting, such as:

    a. How the CSP monitors performance and reports results to the Government.

    b. When and how the Government is to confirm performance of the CSP.

    c. How the CSP identifies problems and resolution expectations to include dispute mediation processes (e.g., escalation process, consequences).

    d. When and how the CSP informs the Government on changes – updates or new services (Change Management process).

It is important to note that the SLAs provided by the CSPs are constantly changing/updating as new cloud services or offerings are made available, additional CSP "nodes" are brought online, and technology continues to evolve.

Resellers - Value Added Resellers (VARs)

It's important to understand other factors that also influence price/cost to better measure the overall value and quality of the CSPs' offerings. In the recent past CSPs were reluctant to deal with the government directly, but that has changed and most CSPs will now contract directly with the government. Organizations may negotiate pricing with the CSP even though the purchase of cloud is through a reseller. Small and socio-economic businesses often operate as various types of resellers in this market. So, where appropriate, resellers should be evaluated to contribute to agency small business goals. Resellers can offer services in addition to being a broker for the CSP. It is essential to evaluate the reseller to understand the value they provide to the contract and the agency. They operate on margin from the CSP pricing and fall in one of three general categories.

1. Reseller
    a. An organization that acts as a broker between the CSP and the agency and assumes very little risk.
2. Value Added Reseller
    a. An organization that acts as a broker between the CSP and the agency but also provides cloud management services and is willing to take on risk by providing 3 year or 5-year discount pricing knowing that the government can cancel or lose funding in any given fiscal period.
3. Systems Integrator
    a. An organization that mainly provides configuration, management and development services who bundles cloud costs with those services.

When working through a reseller of any type it is imperative that the government entity owns all accounts, subscriptions, subaccounts, etc and not the reseller. The government should also have access to all monthly billing data from the source provider and not rely on generic reporting from the reseller.

Authorized Resellers

The FedRamp marketplace is a searchable and sortable database of Cloud Service Offerings (CSOs) that have achieved a FedRAMP designation, a list of federal agencies using FedRAMP Authorized CSOs, and resellers.

Appendix

Forecasting

The scope of the contract must align with the actual consumption of cloud services so that the government doesn't commit to more than it can consume. This means that there must be an understanding of forecasting the increase or decrease of existing cloud resources in addition to any net new systems, services or applications that are being migrated or spun up in the cloud. These Government systems and applications may include large enterprise resource planning (ERPs) systems, and/or smaller legacy applications. As mentioned previously, the Government must identify the need for configuration, management, and integration with the CSP's platform. The acquisition team needs to work with the application and engineering teams to forecast and rationalize the necessary resources for the upcoming contract period.

References

Below lists and links to other related resources that may also be beneficial for IaaS procurement.

- GSA's Cloud Information Center
- GSA's IT Software Cloud Computing & Services Ordering Guide
- ITC's Best Business Practices for USG Cloud Adoption
- GSA's White Paper: Best Practices for Effective Cloud Computing Services Procurement within Federal Government
- GSA CoE's Cloud Adoption Playbook