Microsoft

Top 5 considerations for U.S. government cloud procurement

Table of contents

01 /

Introduction

This whitepaper covers top considerations for cloud procurement for U.S. Government organizations and their partners, with specific guidance on planning, governance, licensing, and eligibility for Azure Government. This guidance is intended for the early stages of your cloud journey, to help you think strategically about your organization's transition to the cloud and ensure you're aware of the resources available to help you optimize your investments and advance your mission.

For commercial entities that need to meet U.S. government compliance requirements, you may wish to skim to page 6 for more information on how Azure Government can help you meet regulatory commitments. You'll also want to be aware of the options for purchasing Azure Government starting on page 11, and how to check your eligibility for Azure Government on page 14.

02 /

Top 5 considerations for cloud procurement

Plan for outcomes that advance the mission

For many agencies, the procurement and budgeting process is aligned more to traditional hardware purchasing than the 'pay as you go' model of the cloud. To bring in the many benefits of the cloud, government CIOs will often partner with their business lead and procurement team to create a strategic plan based on outcomes. In this way, the organization can pre-allocate dollars for cloud services that enable these outcomes. This gives the IT organization the ability to move forward in an agile and cost-effective manner, gaining access to new cloud capabilities as they become available.

The Acquisition Professional's Cloud Adoption Survival Tips, Lessons Learned and Experience, or CASTLE Guide from the federal Cloud Center of Excellence outlines common challenges regarding procuring cloud within government and provides recommendations to solve these challenges:

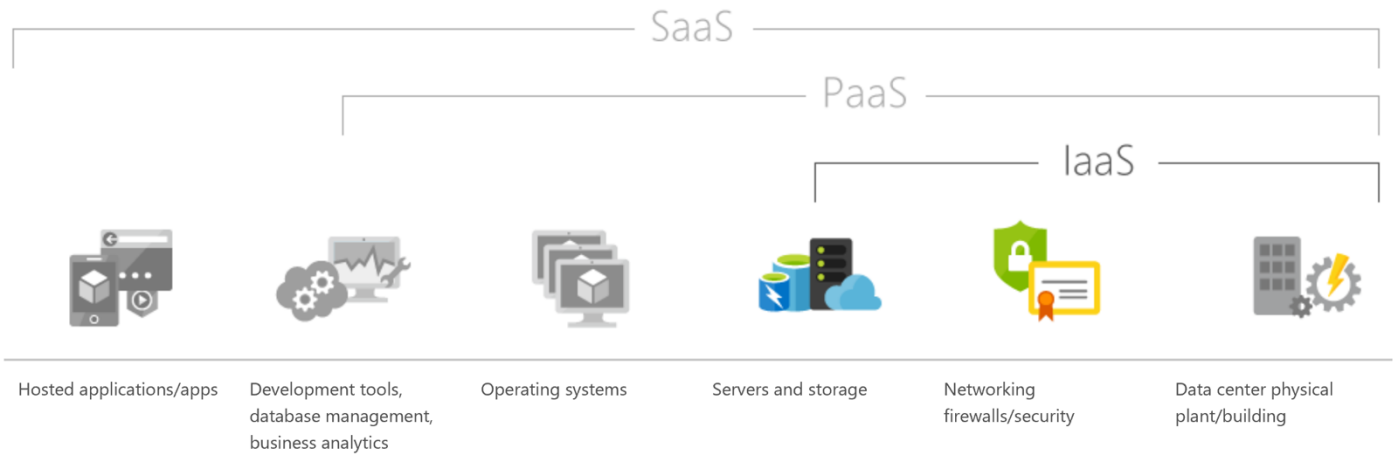
"Consumption-based payment is a fundamental component of cloud computing. . . The broad deployment of those services within the Federal Government puts pressure on Government systems that were not designed to accommodate the variable usage and quick-pay cycles that are the hallmark of the commercial cloud computing models. . .

To solve the funding challenge, the Guide recommends a set of actions to mitigate these disadvantages. Most importantly, it recommends the use of Time and Materials (T&M) type contracts for cloud computing contracts, and a clarification of T&M contracting within the Federal Acquisition Regulations (FAR). Specific approaches, pros and cons, and additional details are located in the Guide chapter 'Paying for Cloud.'"[1]

[1]https://fcw.com/~/media/GIG/FCWNow/Documents/2017/CASTLE%20Guide%20v11.0%2020170830.pdf

With this guidance in mind, agencies can build a strategic plan for purchasing cloud capabilities to modernize legacy infrastructure, increase agility, and advance the mission of the organization.

Understand the shared responsibility model



As your agency's plans for cloud services take shape, you'll want to be aware of the shared responsibilities between your agency and your cloud computing service provider. These shared responsibilities depend on the type of service you're considering, whether it's Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service.

IaaS is an instant computing infrastructure, provisioned and managed over the Internet. IaaS helps you avoid the expense and complexity of buying and managing your own physical servers and other datacenter infrastructure. The cloud computing service provider manages the underlying infrastructure, while you purchase, install, configure, and manage your own software—operating systems, middleware, and applications.

Platform as a service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. Like IaaS, PaaS includes infrastructure—servers, storage, and networking—but also middleware, development tools, business intelligence (BI) services, database management systems, and more. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating. You manage the applications and services you develop, and the cloud service provider typically manages everything else.

SaaS provides a complete software solution that you purchase on a pay-as-you-go basis from a cloud service provider. Common examples are email, calendaring, and office tools (such as Microsoft

Office 365). The underlying infrastructure, middleware, app software, and app data are located in the service provider's data center. The service provider manages the hardware and software, and with the appropriate service agreement, will ensure the availability and the security of the app and your data as well.

In addition to the type of platform you choose and the implications of that choice in terms of shared responsibility, you'll want to ensure that all stakeholders are aligned on shared responsibilities for access control and defining who is permitted to work on your Azure Government account. You can use the access control features within Azure Government to help you manage permissions at a granular level.

Learn more about shared responsibilities here, and learn more about how to secure your operations through the lifecycle of your cloud-based services here.

Simplify governance of your IT resources

In planning a cloud initiative, you'll need to consider governance of your cloud resources from an organizational perspective, a subscription perspective, and a technical perspective. From each of these viewpoints, you'll want to understand the array of governance controls implemented within Microsoft Azure Government to help you achieve an elevated level of governance of your IT resources.

From an organizational perspective, you'll want to focus on implementation of policies, processes, and procedures to meet agency priorities and ensure the right level of security and continuous compliance with appropriate organization standards.

As mentioned above, this organizational governance includes (but is not limited to) managing your shared responsibilities and choosing who you permit to have access to your agency's account.

From a subscription perspective, you'll want to ensure you have the right internal cloud governance solutions in place. For example, Enterprise Agreement customers can use the Enterprise Portal for internal cloud governance (read more about Enterprise Agreements in the section: 'Options for purchasing Azure Government'). In addition, you can select from several Azure solutions and other software offerings to help you optimize cloud resources, manage departmental budgets, and allocate costs.

Azure Advisor is a free offering that helps you to follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry to recommend solutions

that can help you improve the cost effectiveness, performance, and high availability of your Azure resources. You may also be interested in Azure Partner Marketplace solutions for cloud management, which can help you govern usage across your organization.

From a technical perspective, you'll want to review the Azure Government Documentation and some of the articles focused on the security-related capabilities available in and surrounding the Azure platform, including:

- Isolation in Azure: This article outlines how Microsoft Azure provides isolation against both malicious and non-malicious users and serves as a guide for architecting cloud solutions by offering various isolation choices to architects.
- Performance monitoring and alerting: This article provides a summary of the range of tools for monitoring Azure applications and services.
- Azure Government Monitoring + Management: This article outlines the monitoring and management services variations and considerations for Azure Government.

Utilize existing compliance standards and regulatory commitments

To help your organization meet ever-evolving requirements, Azure Government includes the most comprehensive set of compliance offerings of any cloud service provider, including FedRAMP, the Department of Defense (DOD) Security Requirements Guide (SRG), US Criminal Justice Information Services Security Policy (CJIS), and International Traffic in Arms Regulations (ITAR). You can find the certifications and attestations for the Microsoft cloud at the Microsoft Trust Center.

FedRAMP High
The Office of Management and Budget now requires all executive federal agencies to use FedRAMP to validate the security of cloud services. Azure Government has been issued a P-ATO at the High Impact Level, the highest bar for FedRAMP accreditation. Learn more about FedRAMP and the Microsoft Cloud in the FedRAMP compliance backgrounder.

US Department of Defense (DoD) Provisional Authorization
The DoD Cloud Computing Security Requirements Guide (SRG), developed by the Defense Information Systems Agency (DISA), a combat support agency of the DoD, defines the baseline security requirements for cloud service providers that host DoD information, systems, and applications. Azure Government has achieved a Provisional Authorization for both Information Impact Level 4 and Level 5.

Learn more in the DISA backgrounder, and learn how to accelerate your own compliance with DISA standards using our security control implementations.

US Criminal Justice Information Services Security Policy (CJIS)
The Criminal Justice Information Services (CJIS) Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI)—for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the CJIS Security Policy. Learn more about how Microsoft works with states to meet CJIS Information Agreements.

International Traffic in Arms Regulations (ITAR)
While there is no compliance certification for the ITAR, Microsoft operates and has designed in-scope services to be capable of supporting a customer's ITAR obligations and compliance program. Microsoft Azure Government provides commitments for customers with data subject to the ITAR through additional contractual terms regarding the location of stored data, as well as limitations on the ability to access such data to US persons. Microsoft provides these assurances for the infrastructure and operational components of these government cloud services, but customers are ultimately responsible for the protection and architecture of their applications within their environments. Learn how to accelerate your ITAR deployment in the ITAR Deployment Overview for Azure Government

Consider your options for technical support

Government customers and their partners often have specialized support requirements, and there are several options available:

Cloud Solution Provider (CSP) Support
Many government customers who are already working with Cloud Solution Providers (CSPs) choose this avenue for ongoing technical support (Read more on CSPs in the section 'Options for purchasing Azure Government'). CSPs can offer you customized support options depending on your needs, from initial planning and architectural guidance, to implementation and managed service offerings, to technical support and governance. Reach out to your CSP to discuss your support needs and ensure this is considered as part of your strategic plan.

Microsoft Enterprise Services
You may also be interested in the support solutions from Microsoft Enterprise Services. Microsoft Enterprise Services' digital advisors, engineers, consultants, and support professionals help you implement and adopt Microsoft products, services, software, and devices to solve, envision,

and understand new possibilities for your business. Contact your Microsoft Enterprise Services Account Representative for details about Support Solutions.

Additional Planning Resources:

Microsoft FastTrack for Azure
FastTrack for Azure helps you build solutions quickly and confidently with direct assistance from Azure engineers who work hand-in-hand with partners. During a typical FastTrack engagement, we help you define the business vision to plan and develop Azure solutions successfully, assess your architectural needs, and provide guidance, design principles, tools, and resources to help you build, deploy, and manage your Azure solutions. We'll also check in periodically to ensure deployment is on track and help remove blockers, match you with skilled partners for deployment services, on request. This a separate program with distinct eligibility requirements from Azure Government, including an active paid Azure subscription and a project estimated to consume a minimum of $5000/month of Azure services. Read the eligibility requirements for FastTrack for Azure to assess whether this is a fit for your organization.

Azure Security & Compliance Blueprints
These publicly available framework documents provide security and compliance solutions and support, tailored to the needs of customers in a variety of industries, to accelerate cloud adoption and utilization for customers with regulated or restricted data. For example, these guides are designed to help cloud solution architects and security personnel understand how Azure Government services and features can be deployed to implement a subset of customer-responsibility FedRAMP and DoD security controls.

03 /

Options for purchasing Azure Government

Azure Government is available to US federal, state, local, or tribal government entities and their solution providers. To determine if your entity is eligible, consult the requirements below or apply for an Azure Government 90-day trial.

Azure Government may be available to purchase as a pay-as-you-go (PAYG) online subscription, through an Azure Government Cloud Solution Provider (CSP), or as an Enterprise Agreement, depending on the size and needs of your organization.

Many large organizations have multiple cloud licenses with multiple providers, and you may choose multiple options to optimize price, flexibility, and service availability. Below are some of the factors to consider when making your decision:

Pay-As-You-Go subscriptions

With a Pay-As-You-Go subscription, you pay only for what you use with no minimums, scaling up or down on the fly. Pay with a credit card with easy monthly billing or invoicing and cancel anytime. To get started, request a trial. When you're ready, you can add a credit card to your account.

Customers choosing a Pay-As-You-Go subscription for Azure Government gain the benefits of immediate and direct billing with no monetary commitment. Pay-As-You-Go subscriptions receive the same service level agreement (SLA) as other license types, but do not include the benefits of the Azure Enterprise Portal or the value-added services that partners can provide. You can set up multiple billing containers/separate accounts to help your agency manage spend across cost centers.

Purchasing through a Cloud Solution Provider (CSP)

With a Cloud Solution Provider (CSP), you benefit from a partner who can build custom solutions on Azure Government and provide a single bill for both your Azure Government usage and any additional value-added services. The CSP program is a great fit for the US public sector where partners already build, deploy, and manage solutions on behalf of federal, state, local, and tribal entities. You can find a current list of Azure Government CSPs here.

Customers choosing to purchase Azure Government through a CSP gain the added value of a service provider who understands government requirements and can help you plan, build, deploy, and manage solutions. CSPs can help you navigate the purchasing process and may provide flexibility on billing that better aligns to your reporting needs. If you are already working with a CSP, this channel may minimize the need for a net new procurement process. In addition, many of the CSPs in the list above offer customized support options for government customers.

You can find a list of currently available services currently available through the CSP program here.

If any of the following requirements apply to your organization or if you have additional questions, please contact us to discuss your needs at Azure Government CSP:

- If you are subject to regulatory requirements such as ITAR, CJIS, DFARS, or IRS 1075
- If you are currently an Enterprise Agreement customer interested in moving to CSP
- If you are interested in purchasing Microsoft Cloud products other than Azure

If you are a partner interested in becoming a CSP, please start here.

Acquiring an Enterprise Agreement

With an Enterprise Agreement for Azure Government, you gain several licensing benefits, including: the broadest set of services, support for multitenant solutions, and access to the Azure Enterprise Portal. The Enterprise Portal is a great resource for customers managing multiple accounts or subscriptions. These licensing benefits differ from what is available through a Cloud Solution Provider (CSP). Enterprise Agreements are also a good choice for customers with specific business requirements for this type of license.

If you have an existing Enterprise Agreement and want to add an Azure Government subscription, you simply need to execute a Microsoft Cloud for Government enrollment to your existing agreement. Contact your Microsoft representative to learn more.

If you are interested in purchasing Azure Government through a new Enterprise Agreement, contact an Azure Government Licensing Solution Provider (LSP). Licensing Solution Providers can help you acquire your license. LSPs do not generally provide the same in-depth ongoing support as a CSP.

04 /

Check your eligibility for Azure Government

Azure Government is available exclusively to three distinct types of customers:

- A US government entity in its governmental capacity, such as a federal agency, state/local entity, regional or interstate government entity, or federally funded Research and Development Center (FFRDC).
- A partner using Azure Government to provide a solution that provides services or solutions to US government customers through direct or indirect contracts or serves US government customers through GSA or other contract vehicles.
- A commercial entity with data subject to government regulations. Accepted government data types include: International Traffic in Arms (ITAR), Controlled Unclassified Information (CUI), Department of Defense (DoD) Unclassified Controlled Nuclear Information (UCNI), Department of Energy (DoE) UCNI, Criminal Justice Information (CJI), Department of Defense Impact Level Data, and other types of data that require Azure Government

Proof of membership in one of the groups listed above will be required for access to Azure Government. An international commercial entity with data regulated by the US government may qualify, though the entity may be required to purchase the service through their US subsidiary. To determine if your organization is eligible, you may apply for an Azure Government 90-day trial.

Next steps

As you develop your cloud strategy, we're here to help. Please contact us with any questions.

You can also get started today by requesting a free trial, learn more about Azure Government, and subscribe to the Azure Government blog.

Contact your designated Microsoft account representative or partner to help you get started, or visit the Microsoft Azure website

https://azure.microsoft.com