CloudCheckr

# The Public Sector Guide to IaaS Success

## A Primer for Federal, State, and Local Agencies

# Contents


**Introduction** 3

**Benifits of the Cloud** 4

**Key Compliance Frameworks for Federal Agencies** 4

**How Cloud Providers Deliver Their Services** 6

Governmental Regions 7

IaaS Offerings 7

Management and Security 9

Service Comparison 10

**Cloud Best Practices** 11

**What Types of Workload Are Right for the Cloud?** 12

**Enlist the Help of a Cloud Management Platform** 13

# Introduction

More than half of all government data centers have closed in recent years. Why? High operating costs, budget constraints, and obsolescence of equipment are motivating many of these organizations to switch to cloud computing. Despite the modernization of the public sector, agencies still face challenges when it comes to data privacy in the cloud.

To meet stringent security and compliance requirements, governmental bodies and their subcontractors must store and process sensitive federal data separately from private sector workloads. Until recently, their choices for hosting workloads in the cloud had been limited.

To provide a clear path to IaaS success, leading public cloud providers such as Amazon Web Services (AWS) and Microsoft Azure set up isolated governmental regions to serve the specific needs of the public sector. Shortly thereafter, Amazon's GovCloud (US) and Microsoft Azure's US Government regions were certified to the highest level of FedRAMP compliance.

This has helped to accelerate cloud adoption in the federal space, with public authorities now moving to the cloud at a faster rate than private corporations.

But migrating to the cloud represents a seismic shift away from traditional IT practices. This not only requires a different approach to regulatory compliance but also operational management and application architecture.

In this paper, we tackle the essentials of the cloud from a public sector perspective. We take you through the key compliance frameworks that apply to governmental agencies, examine the types of IaaS offerings available and provide you with introductory guidance to cloud best practices.

But, first, let's start with the benefits the cloud can bring to the public sector.

# Benefits of the Cloud

The most widely acknowledged benefit of the cloud is reduced cost. With on-premise data centers, you need sufficient hardware capability to accommodate peaks in demand and future growth. So for much of the time, such as outside 9–5 hours, most of your capacity remains unutilized. By contrast, you can scale your cloud infrastructure up and down as required. With good cloud management, this can make it far more cost effective.

The cloud also offers a more agile approach to IT. Users can spin up resources in a matter of clicks, reducing delays in project development. By sharing infrastructure, authorities can also develop integrated IT systems, helping them to make operational efficiencies and better serve the public. And through access to big data technologies and DevOps tools, organizations can gain new insights and leverage automation to speed up application delivery lifecycles.

But, above all, the cloud offers a pay-as-you-go (PAYG) alternative to procuring IT infrastructure, with no upfront costs. This lends itself perfectly to the use it or lose it spending culture in the public sector—where, provided you maintain good visibility and control over your cloud consumption, you can align your monthly IT costs to your budget burndown rates.

# Key Compliance Frameworks for Federal Agencies

When you move to the cloud, you introduce a third party into the process of storing and managing your data. So you'll need to prove your cloud vendor also meets your compliance obligations in order to maintain your Authority to Operate (ATO) status. Dedicated cloud services, such as Amazon GovCloud (US) and Microsoft US Gov, meet the standards of security required to comply with many regulatory frameworks. These include:

**NIST 800-53:** A catalog of controls designed to protect the security and integrity of data on all federal information systems. It forms a critical component of compliance with the Federal Information Security Management Act (FISMA).

**FIPS:** FIPS 199 and FIPS 200 provide a framework for determining the baseline NIST 800-53 controls that are appropriate to the confidentiality, integrity and availability requirements of your organization. Different categories of controls apply depending on the security objectives of your organization—which, in turn, are determined by the level of potential impact in a breach scenario.

**FedRAMP:** A tailored set of legal requirements for storing and processing information on government systems in the cloud. FedRAMP is also based on NIST SP 800-53. However, it is adapted to address the unique security responsibilities that relate to the cloud. These are shared between the cloud provider and cloud user. So, to avoid unnecessary and cumbersome duplication of roles, FedRAMP provides two streamlined sets of controls—one for the cloud vendor and the other for the federal agency using its services.

**NIST SP 800-171:** A series of requirements and guidelines outlining the responsibilities of organizations, which store or process controlled unclassified Department of Defense (DoD) data, when acquiring commercial cloud services. It is a prerequisite for compliance with the DFARS clause of the Federal Acquisition Regulation (FAR), which came into force on 31 December 2017.

# How Cloud Providers Deliver Their Services

Each of the leading global cloud vendors operates a network of data centers, which are grouped together into geographic regions based in different physical locations across the world. Each region is an independent service, with different pricing, product availability and local compliance offerings.

In the case of AWS, each region is made up of several discrete Availability Zones, typically two or three, which allow solutions architects to build low-latency fault-tolerant applications within the same region. By contrast, Azure uses a system of availability sets at virtual machine level to provide for redundancy and availability.

In a 2019 interview with theCUBE, AWS Worldwide Public Sector Vice President Teresa Carlson emphasized that agencies like the Federal Bureau of Investigation require high availability and redundancy in order to identify critical events and improve crisis response times.

**The FBI [is] a perfect example of us helping them move faster to do their mission. Time to catch the bad guys. Time to share that data with other groups so they could quickly disseminate and get to the heart of the matter."**

**Teresa Carlson**

*Vice President of the Worldwide Public Sector at AWS*

## Governmental Regions

To meet the strict compliance requirements of the public sector, cloud vendors provide their governmental services in distinct isolated regions. These are only available to governmental bodies at federal, state and local level, as well as authorized contractors, and are managed exclusively by vetted US citizens.

AWS currently operates one standard US governmental region, consisting of two Availability Zones. Microsoft offers four standard governmental regions, although the availability of its services varies considerably between them.

However, Amazon's range of governmental services also includes Commercial Cloud Services (C2S) —a sequestered cloud region, built specifically for the CIA to support classified data.

Microsoft offers two of its own highly specialist government regions, US DoD East and US DoD Central , which are designed to meet the security requirements of the US Department of Defense (DoD) under the DoD Cloud Computing Security Requirements Guide (SRG). Both clouds are designated exclusively for US DoD customers.

## IaaS Offerings

Although each public cloud provider has its own unique set of features, selling points and service concepts, they all follow a common approach to infrastructure delivery.

The main categories of IaaS offering they each provide are as follows:

**VIRTUAL MACHINES (VMS)**

Cloud vendor offerings include a range of different machine types and sizes designed for different use cases. Some are general-purpose instances that provide a balanced mix of CPU and memory. Some offer additional CPU for compute-intensive workloads, while others come with low-cost directly attached storage for management and analysis of large amounts of data.

Most instance types offer a choice of operating systems and licensing options. What's more, you can launch VMs from your own preconfigured machine images—or

from one of the many prebaked templates available on your chosen cloud provider's marketplace of approved third-party solutions. Many of these are in the form of a full-stack application environment that's ready for immediate deployment.

You can scale your cloud infrastructure in two different ways—either vertically, by changing the size of your VMs, or horizontally, where you increase or decrease the number of servers in a distributed cluster of VMs.

Ideally, you should base the design of your cloud applications on a distributed architecture of smaller, loosely coupled components. This will allow you to take full advantage of horizontal scaling, which facilitates fine-grained control and more efficient use of your application resources.

And, finally, some cloud providers also provide discounted alternatives to On-Demand pricing. Both AWS and Azure offer Reserved Instances and AWS also offers Savings Plans which offer significant potential savings in exchange for an hourly spend commitment for one or three years.

**Beware:** Make sure you first check the availability of any machine type you decide to use, as cloud providers rarely support all their products and features in governmental regions.

**STORAGE**

**Ephemeral block storage:** Low-latency temporary storage disks, available to certain instance families in AWS and all instances in Azure, which are physically attached to your VM. They are generally employed as short-term storage for uses such as swap files and one-off batch jobs.

Volumes only persist as long as your VM is running and whenever you reboot your machine. However, you can build in persistence by replicating data across more than one cloud region or group of data centers. This allows you to exploit the storage method's fast read and write performance in a wider range of use cases.

**Persistent block storage:** Durable network-attached disks designed for direct use with VMs. Persistent disks tend to offer more functionality than ephemeral storage. For example, cloud vendors usually provide native facilities to take snapshot backups of your persistent volumes. You can stop and restart VMs without loss of your data.

And you can also attach more than one persistent volume to a VM at any time.

On the other hand, however, an individual volume cannot be used by more than one VM at the same time.

Persistent block storage is suited to a wide range of use cases, including system boot volumes, relational databases, NoSQL frameworks and general enterprise applications.

**Object storage:** Standalone storage designed for unstructured data, such as static website content, digital media, log files and backups. Data is accessible via API from anywhere over the Internet.

By contrast with its block-level counterparts, where capacity is either provisioned in advance or governed by associated VM, you only pay for the storage you actually use. Object storage usually comes in a range of different SLAs and pricing—the choice of which will depend largely on how frequently you access your data.

**Archive and backup:** A low-cost option for unstructured data that's rarely accessed or requires long-term storage to meet compliance. Cloud vendors usually support a number of service tiers for different frequency of access and availability expectations. Tiers offering lower storage costs come at the expense of higher retrieval charges.

**DATABASE**

Leading cloud vendors also provide fully managed alternatives to standard VMs for hosting and managing your databases. Database-as-a-Service (DBaaS) offerings significantly reduce the management overhead involved in setting up and maintaining your databases, automatically taking care of time-consuming operational tasks such as hardware provisioning, patching and backups.

Solutions are available for all three main database models—relational databases,

NoSQL databases and data warehouses. They come with varying levels of scaling functionality and SQL query support.

## Management and Security

Another important aspect to public cloud services is the range of tools for managing security, compliance and the day-to-day running of your infrastructure. These

typically cover identity management, resource and event monitoring, alerts and automated actions , and best practice recommendations.

Each cloud vendor also supports an ecosystem of third-party cloud management software services. Most of the solutions offer extended functionality, such as high-level enterprise features and cross-platform capabilities, which complement a cloud provider's own proprietary tools.

## Service Comparison

The following table shows the key services available to AWS and Microsoft Azure governmental customers, categorized by equivalent or nearest equivalent offerings.

| | Amazon Web Services | Microsoft Azure |
|---|---|---|
| **Compute and Networking** | | |
| VMs | EC2 instances | Virtual Machines |
| VM auto scaling | Auto Scaling | Virtual Machine Scale Sets (VMSS) |
| Serverless | Lmabda | Functions* |
| Dedicated network connection to on-premise environment | Direct Connect | ExpressRoute |
| Load balancing | Elastic Load Balancing (ELB) | Load Balancer |
| Virtual provate network | Virtual Private Cloud (VPC) | Virtual Network |
| **Storage** | | |
| Block-level (directly attached volumes) | Instance store | Temporary disk |
| Block-level (persistent volumes) | EBS | Page blobs |
| Object storage | S3 | Block blobs |
| Archive and backup | Glacier | Azure Storage-Standard Cool |
| **Database** | | |
| Relational | RDS | SQL Database |
| N0SQL | Dynamo DB | DocumentDB and Table Storage |
| Data warehouse | Redshift | SQL Data Warehouse |
| **Management and Security** | | |
| Best practice recommendations | Trusted Advisor | Azure Advisor |
| Resource monitoring | CloudWatch (utilization)<br>CloudTrail (API calls) | Azure Monitor |

| | | |
|---|---|---|
| Authentication and authorization | Identity and Access Management (IAM)<br>Multi-Factor Authentication (MFA) | Azure Active Directory<br>Multi-Factor Authentication (MFA) |
| **Key Compliance Standards** | | |
| | FedRAMP<br>NIST 800-171<br>HIPAA<br>FIPS 140-2<br>ITAR<br>PCI DSS Level ! | FedRAMP<br>NIST 800-171<br>HIPAA<br>FIPS 140-2<br>ITAR<br>PCI DSS Level ! |
| *Not currently available in Microsoft Azure US Gov. | | |

Once you've drawn up a shortlist of providers that meet your compliance requirements, you'll then need to decide which governmental cloud best suits your organization's IT needs.

This will involve a far deeper comparison beyond simply the cost of their respective services. In particular, you'll need to consider how a cloud vendor can address the individual IT challenges your organization faces.

AWS has historically been an obvious choice for governmental cloud, as it boasts the broadest range of products and features. Microsoft, on the other hand, offers particularly strong hybrid capabilities. Your choice may also come down to your preferred approach to service delivery. For example, AWS is geared more towards self-service, whereas Microsoft is more oriented towards its network of sales representatives.

# Cloud Best Practices

The cloud promises great potential for both efficiencies and innovation in public sector IT. However, it's important to understand the implications of moving to a dynamic PAYG environment.

It's incredibly easy to spin up new instances in the cloud. But it's just as easy to lose track of unused and underutilized resources. And, without good cloud governance,

your infrastructure can easily become vulnerable to attack and costs can quickly spiral out of control.

As a result, cloud best practices largely revolve around security and cost management, where your key objectives will be to:

- Maintain full visibility over your entire cloud inventory
- Tag resources so you know exactly who is responsible or accountable for each of the services you're running at any given time
- Ensure all workload environments are safe and meet regulatory compliance requirements
- Optimize resource utilization to ensure a healthy balance between cost and application performance
- Understand how much each of your resources costs
- Allocate monthly cloud charges to the correct internal accounts

What's more, your application architecture should be fault tolerant, secure and make the most efficient use of your cloud resources. And finally, in line with standard governmental practice, you should maintain consistent monthly cloud costs so you neither overspend nor underspend your IT budget.

# What Types of Workload Are Right for the Cloud?

When you start your cloud journey, you should first focus on workloads that are either straightforward to migrate or call for dynamic infrastructure that can scale with demand. Typically these will be:

- New projects or existing applications that are due for redevelopment
- Standalone applications that run in isolation
- Workloads already running in virtualized operating environments
- Large one-off batch jobs, such as year-end financial reports
- Applications that experience strong fluctuations in demand

On the other side of the coin, you should beware of the risks of migrating applications that are heavily integrated with other systems. In addition to the high level of complexity, the extra communication layer can increase application latency and rack up unnecessarily high data transfer costs.

Amazon's public sector customers can learn more about AWS GovCloud and the latest cloud technology developments at the company's Public Sector Summit for government, education and nonprofits, held annually in Washington, D.C.

# Enlist the Help of a Cloud Management Platform

A move to the cloud is a complex undertaking that requires thorough research, careful planning and a range of new skills and expertise. But help is at hand in the form of each vendor's ecosystem of managed service providers and third-party cloud solutions.

You can find specialist migration support and guidance. You can find tools that help you overcome the complexity of managing a dynamic cloud environment, allowing you to take control of your cloud costs and providing important security safeguards.

But, above all, they can help you fulfil your ultimate mission of innovation, agility and cooperation, which are key to your organization's IaaS success and a better service to the US public.

When choosing a Cloud Management Platform (CMP), consider the security standards of that solution itself. If you are in the public sector, including Federal, State, and Local government agencies, you can ease your procurement processes by selecting a pre-approved solution. CloudCheckr Federal is the only CMP that has met the FedRAMP Ready standard. Agencies can start fast, without a long approval process, and rely on a highly available and secure solution to manage their cloud.

CloudCheckr

## About CloudCheckr

We deliver total visibility—from public cloud to hybrid workloads—making the most complex cloud infrastructures easy to manage. CloudCheckr customers deploy our SaaS-based platform to secure, manage, and govern the most sensitive environments in the world, from government agencies to large enterprise and Managed Service Providers. Our industry-leading solutions include Cost Management, FinanceManager, Cloud Security, Total Compliance, Inventory & Utilization, and Cloud Automation.