White Paper: **February 2023**

The State of U.S. Public Sector Cloud Management

Table of contents

Executive summary

Over the past several years, new trends have arisen in the public sector, including modernizing legacy systems, improving cybersecurity, and central IT assuming the role of a cloud service broker. The most significant trend, however, has been the acceleration of cloud adoption.

Faced with U.S. federal initiatives, laws for securing sensitive information, and restrictive budgets, government agencies are under immense pressure to adopt the cloud. Government agencies transitioning from a traditional IT services model to a cloud model face new obstacles as they develop a cloud strategy. Effective cloud management does not begin or end with the development of a cloud strategy, however; public sector organizations—whether they are federal, state or local—need to execute on that strategy and maintain alignment with the mission. This will require collaboration and alignment between central IT and the various business units.

This white paper addresses the evolution of public sector cloud adoption, key compliance considerations when evaluating cloud service providers, and best practices for managing cloud infrastructure.

U.S. federal initiatives drive public sector cloud adoption

Throughout the past decade, public sector cloud adoption has been increasing as a result of U.S. federal initiatives, such as the Federal Data Center Consolidation Initiative (FDCCI) of 2010 and the Cloud First Policy of 2011. The purpose of the FDCCI was to reduce the real estate footprint and costs associated with maintaining government data centers.[1] The Cloud First Policy was created shortly after with the intent of requiring government agencies to evaluate cloud computing options.[2]

The Cloud First Policy later became incorporated into the Federal Information Technology Acquisition Reform Act (FITARA) in 2014, which required agencies to inventory their data centers and set goals for consolidation. In 2016, the Data Center Optimization Initiative (DCOI) superseded the FDCCI and further enforced consolidation efforts.[3] Included within the DCOI are standards for server utilization and automated monitoring, energy metering, power usage effectiveness, facility utilization, and virtualization.[4] While these initiatives are mandates for federal agencies, many state and local governments have followed suit. These initiatives have driven public sector organizations to realize the value and benefits of cloud computing, such as greater agility and scalability, and opportunities for cost optimization and improved security.

[1] Data Center Knowledge. "NASA Light Years Ahead on Data Center Consolidation." Karen Riccio. March 31, 2017.

[2] U.S. Department of the Interior. "Cloud Smart Strategy."

[3] Executive Office of the President Office of Management and Budget. "Data Center Optimization Initiative."

[4] Executive Office of the President Office of Management and Budget. "Data Center Statistics."

Key compliance considerations for the cloud

Federal regulations have been established to standardize government cloud use and safeguard sensitive information. A broad set of compliance and regulatory controls have been put in place for protecting criminal justice information, Controlled Unclassified Information, and individually identifiable health information, as well as for providing accessibility. A few of the most notable regulations include the Federal Risk and Authorization Management Program (FedRAMP), Criminal Justice Information Services (CJIS), the Defense Federal Acquisition Regulation Supplement (DFARS) and the National Institute of Standards and Technology (NIST) publication 800-171, the Health Insurance Portability and Accountability Act (HIPAA), and Section 508. Security and accessibility concerns must be satisfied by government agencies, as well as the cloud service providers that they leverage.

FedRAMP

FedRAMP provides an approach for how federal agencies can meet the security validation standards required for adopting cloud services. To demonstrate compliance, cloud service providers (CSPs) must earn a Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB); receive an ATO from a federal agency; or work independently to develop a CSP Supplied Package that meets program requirements. Following compliance, CSPs are granted FedRAMP authorizations based on low, medium or high impact levels, which reflects the impact that the loss of confidentiality, integrity or availability could have on an organization.[5] FedRAMP is only required for a subset of federal agencies. Although other agencies may choose vendors based on whether or not they are FedRAMP compliant, they will find that it can significantly limit their vendor options.

CJIS

CJIS is a division of the Federal Bureau of Investigation (FBI), which provides access to criminal justice information to government agencies and law enforcement. Thirteen policy areas have been compiled to establish the CJIS Security Policy. Cloud service providers must evaluate their services to determine if they meet the relevant requirements and controls for transmitting, storing and processing criminal justice information.[6] All federal agencies, state and local governments, and cloud service providers that process criminal justice information must sign the CJIS Security Addendum.

DFARS and NIST 800-171

DFARS and NIST 800-171 mandate cloud service providers to provide evidence as to how they protect Controlled Unclassified Information from the Department of Defense (DOD). DFARS and NIST 800-171 define safeguards for cyber incident reporting obligations.[7,8]

[5] Microsoft. “Federal Risk and Authorization Management Program (FedRAMP).”

[6] Federal Bureau of Investigation. “CJIS Security Policy Resource Center.”

[7] Microsoft. “Defense Federal Acquisition Regulation Supplement (DFARS).”

[8] Microsoft. “NIST SP 800-171.”

HIPAA

HIPAA is a U.S. law that was established to safeguard individually identifiable health information. Covered entities and business associates, such as cloud service providers, are required to meet the standards for privacy, security, enforcement and breach notifications included within the law.[9]

Section 508

Section 508 is an amendment to the Rehabilitation Act established by the U.S. Congress. The law requires federal governments to make their electronic and information technology accessible to people with disabilities. Section 508 specifically focuses on eliminating barriers in IT.[10] A Voluntary Product Accessibility Template (VPAT) is available for businesses and vendors to disclose how well their product or service conforms to Section 508 standards.

Cloud service providers are taking action

As a result of these key compliance mandates, cloud service providers have created government cloud regions, specifically for handling sensitive information and regulated workloads. Regulatory compliance should no longer be a barrier to migrating to the public cloud.

Table 1: Cloud service provider regulatory compliance

	Amazon Web Services[11]	Microsoft Azure[12]	Google Cloud[13]
FedRAMP	High	High	Moderate and High (P-ATO)
CJIS	•	•	•
DFARS and NIST 800-171	•	•	•
HIPAA	•	•	•
Section 508	VPAT	VPAT	VPAT

[9] U.S. Department of Health and Human Services. "HIPAA for Professionals."

[10] Amazon Web Services. "VPAT/Section 508."

[11] Amazon Web Services. "AWS Compliance Programs."

[12] Microsoft. "Federal Risk and Authorization Management Program (FedRAMP)."

[13] Google Cloud. "Compliance resource center."

Cloud management best practices

Without visibility into their cloud environment, government agencies may struggle with decentralized management and unexpected cost increases. As they transform their business, central IT leaders will realize that legacy IT service management tools are not suitable for managing cloud applications and infrastructure. They need a solution that will streamline management, define governance policies, and help deliver on service levels. A cloud management platform can help central IT leaders track mission projects, ensure effective use of IT funds, and improve operational efficiency.

The following are six best practices for cloud management.

Migrate to the cloud

For government agencies just beginning their cloud journey, migration is a key component of their overall cloud strategy. There is tremendous pressure to accomplish a great deal with tight budgets and strict regulatory requirements. The first question to ask is which applications and workloads should be migrated to the cloud, taking into account whether they are critical in terms of operating costs or important for aligning to the agency's overall mission. Applications or workloads that do not fall into the aforementioned categories should be classified as a lower priority for migration.

Additionally, government agencies need to be aware of the resource impact of the applications as some applications may be more labor-intensive than others. They will need to decide if it would be more efficient for employees to run them on legacy systems, or perhaps cloud services could simplify management and help employees reclaim time.

Migrating to the cloud is a high-involvement process, and deciding which workloads to migrate is just the beginning. Government agencies will have to carefully and thoroughly evaluate different cloud providers, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, on their services offered and cost-effectiveness. They will also have to choose a migration approach. There are several options for migration, including lift and shift, partial refactor, full refactor, and incorporating software as a service or platform as a service.

Some cloud management platforms are able to help government agencies move faster in their migration process. For example, the Migration Assessment of VMware Tanzu CloudHealth® analyzes your physical and virtual servers, and generates migration recommendations based on your existing configuration or utilization for the cloud of your choice. Organizations can evaluate the cost of migrating to the cloud with a side-by-side comparison of on-premises costs compared against cloud configuration costs, and leverage recommendations based on asset types, region, reservations and projected costs—all of which can help ease the burden of migration planning.

Establish a cloud center of excellence

The emergence of an internal governing team, commonly referred to as the cloud center of excellence (CCoE), is becoming critical as government agencies transition from a traditional IT services model to a cloud model. Many organizations find that one of the most significant challenges is getting their staff and processes to adapt to a digital-first world. To overcome this, members of the CCoE are seen as advisors who provide best practices, architectural standards, and guidance to agencies across three areas of excellence: cloud financial management, cloud operations, and cloud security and compliance.

The CCoE is typically composed of stakeholders for each area of excellence, various business leaders, and an executive sponsor. Overseeing the cloud transformation and ensuring the cloud strategy is aligned with the agency's mission are the core points of focus for the CCoE.

Common responsibilities for the CCoE include:

- Creating a cohesive cloud strategy
- Determining and analyzing key metrics to report on cloud success
- Defining and enforcing policies and governance
- Continuously optimizing the organization's cloud infrastructure as it scales

The primary reason for having a CCoE is to prevent business units (also referred to as bureaus or departments) from making cloud-based decisions independently of one another. Due to the wide variety of cloud computing options, a successful transformation requires strong collaboration across the key stakeholders. Without a CCoE and a coordinated strategy in place, each business unit could deploy resources from different cloud providers, using inconsistent tagging practices, and make measuring success across the agency more complex. A cloud management platform, such as Tanzu CloudHealth, can act as the hub of the CCoE. Tanzu CloudHealth helps organizations progress through four phases of cloud management maturity: visibility, optimization, governance and automation, and business integration.

Align business context to data

As government agencies increasingly consume cloud resources to modernize operations and deliver improved services to constituents, they need to maintain control over their cloud spend. A preliminary component to this budget adherence is ensuring visibility into cloud data. An initial but crucial task in the cloud is to develop a consistent tagging strategy to better identify and allocate spend and usage. Taking this a step further, many cloud management platforms have the ability to further group resources in a way that's meaningful to the organization, such as building dynamic business groups by environment, department, owner or the like. In Tanzu CloudHealth, these are known as Perspectives.

With assets properly tagged and viewable, the CCoE can then drive accountability across the organization and can show each group exactly how much they're spending and what they're spending it on. This will help the CCoE, and specifically the finance leader, establish an accurate budget. That way, when the next mandate to cut costs comes through, the team can make educated decisions on where to make adjustments.

Additionally, the CCoE can use this granular visibility to ensure that everyone is working from the same data set, identify misconfigured and noncompliant assets, establish showback and/or chargeback, and determine key performance indicators (KPIs) and metrics to measure on an ongoing basis.

Optimize resource cost and utilization

To boost efficiency and achieve cost savings, government agencies need to continuously optimize their infrastructure. Optimization can take several forms, such as decommissioning idle or unused infrastructure, rightsizing assets, and identifying opportunities to take advantage of pricing discounts offered by cloud service providers.

An easy way in which organizations save money is by finding and decommissioning actively running cloud resources no longer being used. Referred to as zombie infrastructure, these assets can include unused virtual machines, storage volumes no longer attached to a compute instance, old snapshots, and disassociated IP addresses, just to name a few.

In a growing cloud environment, organizations using manual analytic models across tens of thousands of resources often find it difficult and overwhelming to rightsize their environment—a challenge that worsens as they increase their use of cloud services or adopt a multi-cloud strategy. By analyzing performance metrics (such as CPU, memory, network and disk) on a regular cadence, government IT teams can identify and make adjustments to these assets, and reclaim funds that can be reallocated to other mission-critical projects or initiatives.

Additionally, agencies can optimize costs by leveraging flexible pricing structures. For example, the leading cloud providers all offer some form of upfront monetary commitment to utilize specific asset types in return for a discount on compute costs. Known as Reservations, Savings Plans, and Committed Use Discounts, many organizations get caught up in the complexity of purchasing these discounts due to the number of options and the limited resources at their disposal for optimization. A cloud management platform can be a trusted source to help with identifying purchase opportunities and managing these discounts throughout their lifecycle.

Centralize cloud governance

With restrictive budgets and lean hiring plans, it's critical for government agencies to maximize the resources at their disposal. Defining policies is the most efficient way to manage scaling cloud infrastructure. Cloud governance policies can proactively alert on any irregularities, such as cost spikes, tagging compliance issues, security vulnerabilities, and more, across the different business units and departments that consume cloud resources. The CCoE often defines and enforces policies and governance throughout the agency.

Depending on the cloud management platform, the sophistication of policies can range from a simple email notification to an automated action, such as terminating unused infrastructure. Taking the initial step from governance alerting to governance automation can be daunting. It's advised to begin with automation within an approval workflow before action is taken and progress to full automation over time. Tanzu CloudHealth provides the ability to add approvers or authorizers to governance policies for initiating change requests. Members of the CCoE team, for example, may be great candidates for authorizers within a cloud environment. Implementing cloud governance policies will free up staff for more mission-critical projects and can yield immediate cost savings.

Integrate cloud and organizational KPIs

The ultimate goal of cloud management is to fully integrate the cloud into your business, with the key being to embed cloud management processes into the day to day of users both inside and outside of IT. Organizations can begin by integrating with existing business systems, such as a governance risk and compliance solution or accounting software. It's important to note that integration goes beyond the technical components and extends to driving a cultural change across an organization.

To measure the impact of cloud consumption, agencies need to align cloud and operational KPIs with the organization's business KPIs. These KPIs may include time to bring new services to market, compliance issues open, citizen satisfaction, and more.

At this phase, the CCoE should make it apparent how the cloud is:

- Reducing the dependency on legacy systems by minimizing data center footprint, hardware and operating costs
- Enabling new service delivery models and offering new digital experiences for employees and constituents
- Enhancing citizen engagement and satisfaction with government services
- Strengthening the organization's security posture
- Contributing to the attraction and retainment of technology talent while improving the skillsets of the current workforce

Conclusion

The adoption of public cloud within the public sector continues to accelerate as more government agencies act on the mandates from U.S. federal initiatives. To successfully transition from legacy systems to the cloud, government agencies need to establish a cloud center of excellence and develop a comprehensive cloud strategy.

Government agencies do not need to be hesitant to migrate to the cloud due to compliance controls or a lack of in-house cloud expertise. Tanzu CloudHealth helps government organizations deliver new and improved services to their constituents by accelerating migration to the cloud, ensuring effective use of IT funds, and improving operational efficiency.

Copyright © 2023 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001
VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at vmware.com/go/patents.
Item No: 1703106aq-wp-state-us-pub-sec-cld-mgmt-a4 2/23