WHITE PAPER

CDW PEOPLE WHO GET IT™

CRITICAL CLOUD DECISIONS FOR FEDERAL I.T.

Federal technology leaders must make the right choices regarding what services to move to the cloud and which provider to use.

EXECUTIVE SUMMARY

The toughest job a federal CIO has is making the business case for an agency IT deployment. With the advent of cloud computing, IT leaders now have three options to choose from: hosting IT services in an agency-owned data center, hosting them in a private cloud or migrating them to a public cloud provider.

The first step in deploying IT services effectively is to decide which of these options should be used for each service an agency runs. This requires decision-makers to determine if a move to the cloud will allow the agency to achieve its mission more quickly and effectively, while saving money. If an agency chooses the public cloud, it must determine which provider best meets its specific needs. A trusted partner can help with each of these types of deployments and provide assistance with everything from planning and implementation to maintenance and support.

The Cloud Decision

Federal IT leaders face an industry at a crossroads. The private sector is rapidly embracing cloud computing models, and citizens expect their government to leverage this private-sector innovation for the public good. At the same time, government technology leaders must also balance unique security concerns and ensure that any adoption of cloud computing technology takes place in a deliberate, careful manner.

Agencies seeking guidance on selecting cloud solutions may first turn their attention to Federal Information Processing Standard (FIPS) 199. This standard provides technology leaders with a three-pronged categorization scheme for information and information systems. Following FIPS 199 requires assessing services on three factors:

- **Confidentiality** requirements, which mandate that federal agencies implement appropriate restrictions on access to sensitive information to prevent unauthorized disclosure
- **Integrity** requirements, which dictate the use of controls that protect against the improper modification or destruction of government information
- **Availability** requirements, which mandate the implementation of systems that ensure timely and reliable access to government information

With these assessments in hand, federal IT leaders may turn their attention to specific business requirements and evaluate the options available for traditional data centers as well as private cloud and public cloud computing. Most likely, agencies will find that a combination of these approaches meets the varied needs of federal computing.

55%

The percentage of federal IT professionals who believe cloud computing makes data management easier*

Decision Points for Cloud

As agencies consider deploying solutions in either a public or private cloud platform, IT leaders should weigh several key points that may influence their decisions. Answering these important questions will not only help IT leaders reach a decision in the best interest of their agency, but also provide them with the talking points they need to communicate the importance of cloud computing initiatives to agency executives.

Some of the key questions that IT leaders should ask about any cloud computing plans include:

- Is the cloud solution mission-effective? Can it support the agency mission as well or better than a traditional data center infrastructure?
- Is the solution cost-effective? Will the agency achieve direct financial savings as a result of the initiative?
- Does the solution provide time savings? Will the agency be able to recapture staff time due to IT efficiency or increased office productivity as a result of the deployment?

When it comes to making cloud decisions, there's no flowchart that agencies can follow. But answering these key questions will provide a strong foundation for the cloud decision-making process.

Traditional Data Center Infrastructure

Most federal spending on computing still takes place in traditional data center environments. While IDC estimates that the federal government spends approximately $3 billion on cloud computing services, this is a relatively small portion of the estimated $80 billion that the government spends on IT resources. Agencies are certainly increasing their spending on cloud computing services, but traditional data centers will remain a large portion of the federal computing strategy for years to come.

Building and maintaining traditional data centers requires substantial capital investments, ranging from physical infrastructure to IT equipment. Agencies operating traditional data centers must ensure that the facility has appropriate physical security and environmental controls to maintain a secure environment conducive to operating sensitive electronic equipment. This requires deep expertise in IT facilities management that may not exist in some agencies. For this reason, many federal agencies choose to partner with vendors who specialize in the construction and operation of data center facilities.

Agencies operating traditional data centers must also procure, install and manage the IT infrastructure necessary to operate a computing environment. This includes the rack-mounted servers and storage arrays that provide basic computing services to the agency, as well as the specialized routing and switching equipment necessary to maintain the flow of information to, from and within the data center.

As agencies make capital investments in new and ongoing traditional data center operations, choice is essential. IT staff must identify the services that best fit the traditional data center model and then choose vendors that offer the best solutions for each of these services. Working with partners allows agencies to augment their internal expertise with teams of subject matter experts who possess extensive experience in the design and operation of data centers.

Private Cloud

Federal IT leaders often understand and desire the benefits offered by cloud computing models but have legal or operational constraints that prevent the use of public cloud providers.

***SOURCE:** MeriTalk, "Cloud Control: Moving to the Comfort Zone," September 2014

Private cloud models provide agencies with the benefits of cloud computing, including rapid elasticity, pooled resources, agility and cost savings, while remaining within a secure, private data center. Agencies that have security concerns or availability requirements that exceed the capabilities of a public cloud provider may choose to include private cloud operations in their computing mix.

In a private cloud model, an agency or vendor builds a single-tenant cloud solution that delivers a scalable, flexible computing infrastructure on hardware dedicated to a single agency. Each organization's private cloud uses a sole-purpose hardware stack that includes servers, storage and networking gear serving a single tenant. Private cloud platforms use automation orchestration technology that allows agencies to rapidly shift resources between competing IT needs and scale solutions to meet changing demand on a dynamic basis.

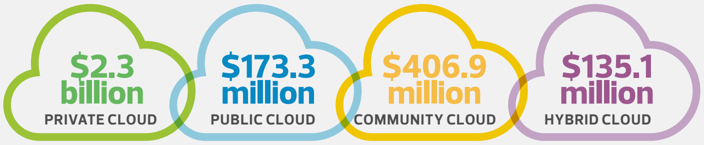
For example, agencies involved in tax collection may see a surge in website traffic during times of major tax deadlines. In a private cloud model, automation software may shift memory, processing and network resources to the website, providing it with additional capacity to meet the seasonal demand. After the tax deadline passes, website traffic may drop, but back-end systems may be busy processing taxpayer information. Automation solutions may see this new demand and then shift resources away from the website to increase the computing capacity available for processing tax returns. In a private cloud model, all of this can take place without requiring any hardware reconfiguration.

2,900+

The number of contracts the federal government has for cloud-based office productivity software*

Building a private cloud infrastructure requires assembling a variety of components, including servers, storage and networking equipment. CDW·G can help agencies put together all of these components more quickly, efficiently and cost effectively than agencies can achieve on their own. CDW·G private cloud services include configuration, orchestration, auditing and security. CDW·G delivers all of these services through a secure supply chain.

Federal Cloud Spending



$2.3 billion PRIVATE CLOUD

$173.3 million PUBLIC CLOUD

$406.9 million COMMUNITY CLOUD

$135.1 million HYBRID CLOUD

***SOURCE:** IDC Government Insights, "U.S. Federal Cloud Forecast Shows Sustained Growth Through 2018," September 2014

Public Cloud

The public cloud offers undeniable benefits by pooling the computing needs of public- and private-sector organizations on an unprecedented scale. Major cloud providers offer rapid innovation and scalability that often far exceeds the capabilities of both traditional data centers and all but the largest private cloud implementations. The innovation and economies of scale offered in the public cloud make it an attractive option for agency IT leaders.

While the public cloud does offer attractive benefits, federal IT leaders must approach this decision with caution. A survey conducted by MeriTalk in 2014 found that 89 percent of federal IT pros feel some apprehension about losing control of their IT services. Despite these concerns, those surveyed said they wanted to double their use of cloud services.

Some organizations have made incorrect decisions to migrate services to the public cloud that wind up being costly mistakes. Security and uptime are two of the most important factors that agency IT leaders must consider when determining

FedRAMP Certification

In the early days of cloud computing, agencies struggled to find service providers that met basic standards for confidentiality, integrity and availability. This led agencies to develop their own security assessment processes that produced inconsistent and redundant results.

As federal cloud adoption grew, the General Services Administration worked in partnership with security and cloud subject matter experts from across government to develop the Federal Risk and Authorization Management Program (FedRAMP). The program provides a standard approach to security assessment and monitoring of cloud service providers. Providers seeking to work with the federal government must implement FedRAMP requirements and then hire a third-party assessor to validate their compliance. Providers that achieve FedRAMP certification appear on a central list of FedRAMP-compliant cloud service providers and may be used across the federal government.

For more information on FedRAMP and a list of cloud service providers with current FedRAMP certifications, see the program website at www.fedramp.gov.

***SOURCE:** Govini, "Insider Snapshot: Cloud," September 2015 whether the public cloud is a suitable option for meeting agency computing requirements.

Once an agency does make the decision to move to a public cloud service, IT leaders must then select an appropriate public cloud service provider. Agencies should first turn to the Federal Risk and Authorization Management Program (FedRAMP). Federal requirements dictate that agencies may use only FedRAMP-approved vendors for public cloud computing services. FedRAMP certification not only ensures that providers meet minimum security requirements, but also offers federal IT leaders a starting point for their evaluation of cloud vendors.

Starting from the list of FedRAMP certified providers, agencies may then vet providers against other business and technical requirements. Agencies should bring together a team of subject matter experts with deep understanding of project requirements to identify the vendors that best meet agency needs. During this process, leaders should take care to understand the different service delivery and pricing models offered by each provider, as they may vary significantly. Investing time in this due diligence process increases the likelihood that agencies will enter into long-term, mutually beneficial cloud computing partnerships.

➜ ***To learn more about how agencies of any size can take advantage of cloud computing solutions and services, check out the Cloud page of CDW's Experts Who Get IT blog.***

You and CDW

Microsoft

Microsoft Windows 10 is familiar and easy to use, with lots of similarities to Windows 7, including the Start menu. It starts up and resumes fast, has more built-in security to help keep you safe, and is designed to work with software and hardware you already have.

vmware®

VMware vCloud® Air™ Disaster Recovery is a new Recovery as a Service solution that introduces native cloud-based disaster recovery capabilities for VMware vSphere® virtual environments. Built on VMware's hypervisor-based replication engine, vSphere® Replication™, and new integration support with vCloud Air Disaster Recovery.

www.cdw.com/content/brands/vmware/vCloud-Air.

CDW·G: A Cloud Partner That Gets IT

CDW·G's solution providers serve as your agency's cloud computing partner. The CDW·G team can help you get to the cloud and integrate your solution seamlessly. We can even completely manage your day-to-day operations. CDW·G's highly trained security professionals possess elite certifications and can help you put plans in place to enhance your security and mitigate identified risks. CDW·G provides the risk management methodologies that you need to secure data, maximize continuity of operations and put disaster recovery plans in place.

CDW·G's Cloud Client Executives, account managers, solution architects and advanced technology engineers stand ready to assist you in every phase of your project as you select and implement the cloud technology needed to boost productivity, regulate IT costs, enhance flexibility and drive innovation. CDW·G will help you get started with a risk assessment that reveals vulnerabilities prioritized by risk, cost and impact and then guide you through the decision-making process to determine the best delivery method for your IT needs: traditional data center, private cloud or public cloud.

CDW·G takes a comprehensive approach to identifying and meeting the needs of every customer. Each engagement includes five phases designed to help you achieve your security objectives in an efficient, effective manner. These phases include:

The CDW Approach

ASSESS

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements

DESIGN

- Detailed vendor evaluations, recommendations, future environment design and proof of concept

DEPLOY

- Development of a migration and management strategy for cloud services

MANAGE

- 24/7 telephone support and ongoing product lifecycle support

To learn more about how CDW·G's cloud computing solutions can help you deliver the right mix of flexibility, scalability and innovation, contact your CDW·G account manager, call 800.800.4239 or visit cdwg.com/cloud.

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified
MKT5370— 150825 —

CDW® PEOPLE WHO GET IT™

ADDITIONAL WEB INFORMATION

[vanity url] CDWG.Com/federal-cloud-WP

[link to cdw solutions page]

https://www.cdwg.com/cloud

[seo hed] Critical Cloud Decisions for Federal IT

[seo dek] Federal technology leaders must make the right choices regarding what services to move to the cloud and which provider to use.

[seo keywords] cloud, cloud solutions, public cloud, private cloud, hybrid cloud, data center, security, cloud security

[Job number] MKT5370

[drop date] 12/30