

Making Your Agency Cloud Smart

INDUSTRY PERSPECTIVE



Executive Summary

For the federal government, adopting cloud is a question of when, not if. Cloud's flexibility, reliability and scalability is well-established, and agencies are eager to include the technology in their IT modernization efforts. Unfortunately, migrating to cloud is difficult when organizations are weighed down by legacy infrastructure and the plethora of vendor offerings.

Created in 2010, the federal government's Cloud First policy tried overcoming this challenge by requiring agencies to evaluate cloud options before making any new IT investments. Sadly, the result was that many government agencies misunderstood Cloud First – or leveraged the vague mandate to their advantage – and justified purchasing solutions without evaluating alternatives. Nine years later, many organizations have struggled with cloud migration due to the lack of adequate planning, analysis and cloud implementation strategy that aligns with their IT portfolio requirements. Hence, the White House Office of Management and Budget (OMB) has been busy developing a smarter approach to cloud to help agencies develop long-term, high-level strategies that drive successful, secure cloud adoption.

Draft Cloud Smart guidance was released in September 2018 for public comment and offers a more detailed roadmap to cloud than its predecessor. The Cloud Smart plan treats procurement, security and workforces as key components of moving to cloud during IT modernization. By providing more guidance on these major work streams, Cloud Smart aims to keep agencies safe while saving energy, money and time.

GovLoop partnered with Micro Focus Government Solutions, an IT software provider, to produce this report about choosing a cloud model based on the concepts introduced in the draft Cloud Smart guidance. In the following pages, we explain how Cloud Smart can guide agencies on how to establish a cloud framework that best fits their mission. We also share insights from David Wray, Chief Technology Officer (CTO); Steve Williams, Director of Sales Engineering and Customer Advocacy; and Chris Leffler, Sales Engineer, at Micro Focus Government Solutions.

From Cloud First to Cloud Smart

Cloud First debuted during a time when cloud computing was a relatively new technology in government. Although the policy was groundbreaking in federal IT, cloud's novelty left many agencies unprepared for how to maximize the technology's benefits.

"Cloud First attempted to force adoption of cloud services," Leffler said. "The result for agencies was often a lack of expected functionality or quality. In some cases, there were projects that needed to be completely decommissioned."

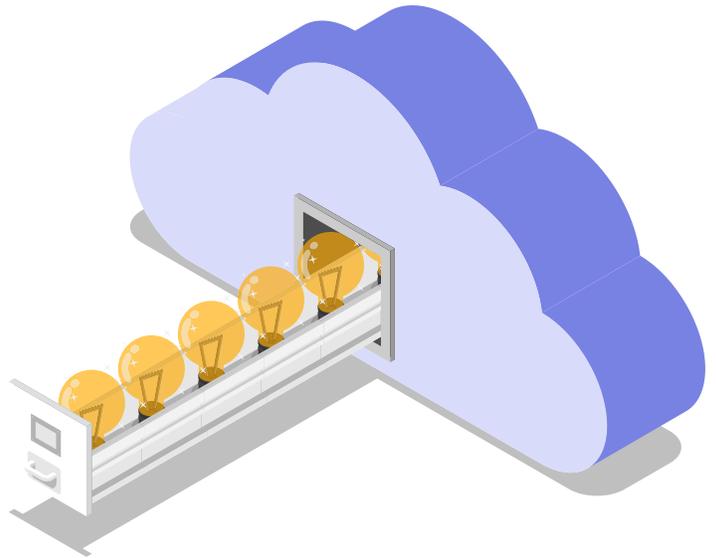
Upon releasing Cloud Smart in October 2018, the federal government admitted that Cloud First is too elementary to address the full scope of cloud transformation across its many agencies. Cloud Smart differs from its predecessor by focusing on adopting cloud effectively rather than deploying the technology by any means possible. The new strategy also expands on Cloud First by detailing how agencies can address cloud procurement, security and workforce reform to best meet their individual needs. Cloud Smart additionally accounts for the various cloud models that have emerged since Cloud First appeared.

Leffler said that Cloud Smart is a more nuanced strategy than Cloud First, as it recognizes that each agency successfully migrates to cloud differently.

"Cloud Smart is about using intelligence to evolve in a much more agile and capable manner versus just forcing someone into adopting cloud," he said.

Speaking at a December 2018 event, Federal Chief Information Officer (CIO) Suzette Kent, whose office is in the Office of Management and Budget (OMB), said that Cloud Smart builds on Cloud First instead of replacing the older policy.

"We transformed Cloud First to Cloud Smart," she said during the Advanced Technology Academic Research Center (ATARC) Federal Technology Modernization



Summit. "And that is in no way an invitation that we don't want people to look at Cloud First, but we want to enable very methodical decisions, and we want to link all the pieces together through policy."

Kent added that Cloud Smart tackles many aspects of cloud adoption that Cloud First didn't address.

"So [it's] security, workforce, FedRAMP, how we get authority to operate and strongly encouraging all agencies to complete the application rationalization," she said, referencing the Federal Risk and Authorization Management Program. "If you haven't looked at your whole landscape and know where you're going, you're not going to be making the best long-term strategic decisions."

Ultimately, many agencies struggled with Cloud First when they realized that cost was not the only factor to consider when planning cloud adoption. Some of their legacy technology couldn't migrate to cloud despite being critical to their mission, and new strategies for procurement, security and workforce training were required for success. Most agencies have realized that an IT portfolio assessment is required first to help provide a prescriptive blueprint for cloud migration as part of an overall strategy for IT modernization. In the next section, we explain the potential solutions Cloud Smart offers for this problem.

Finding Your Agency's Perfect Cloud Model

Cloud Smart differs from Cloud First by discussing specific cloud models that are the most effective for public sector organizations. The policy also clarifies the definitions that the National Institute of Standards and Technology (NIST) has approved for the Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) cloud models. These are:

- **Anything-as-a-Service (XaaS)** – Industry has moved to a more finely differentiated set of capabilities at different layers. The rapid development of both open source and proprietary offerings has made possible almost any combination of vendor and government ownership of these various layers.
- **Hybrid cloud** – Hybrid clouds mix cloud and legacy IT infrastructures to deliver services. They can be created using IaaS, PaaS, SaaS or other cloud frameworks.
- **Multi-cloud** – Multi-cloud environments are those that have more than one cloud vendor. This style can occur as a hybrid, IaaS, PaaS, SaaS or other cloud models.

Wray said that Cloud Smart improves on Cloud First by admitting that different agencies must juggle their modern and legacy technologies in different ways.

“I don't think agencies realized early on that they're never going to be 100 percent in the cloud,” he said of Cloud First. “The reality is that you're going to have applications and infrastructure in multiple clouds and on-premise. It has to be part of your strategy to be capable of managing all your IT regardless of how or where it is physically located.”

Several hurdles, however, have slowed down agencies transitioning to cloud since Cloud First. One is assessing which legacy applications to migrate to the cloud and how much this transition costs. Another obstacle is gauging the security risks of cloud migration. A third barrier to successful cloud adoption is how workers adapt to their technology changing.

“Almost 50 to 60 percent of the cost of agencies' operations maintenance is for the use of mainframe and legacy applications that may sometimes be 20 to 40 years old,” Wray said. “When agencies analyze the cost of cloud migration, they must understand it's to improve the long-term support cost for those applications and measure the potential risks of being in a community cloud environment.”

A community cloud is a cloud where several organizations with common concerns share the infrastructure. Wray added that agencies that successfully adopt cloud are those that factor their budget, security needs and workforces into their migration efforts.

“You can't separate execution from your cloud strategy,” he said. “Resources and security are part of your execution. And if you separate execution and strategy, you'll fail at adopting cloud.”

In the next section, we explain how Cloud Smart helps organizations factor procurement, security and workforce changes into their cloud migration plans.



Cloud Smart's Best Practices for Cloud Adoption

Picking a cloud model isn't the only chapter in an agency's migration story. Organizations will also need to consider procurement, security and their workforces while writing their cloud adoption narratives. Cloud Smart offers agencies a valuable outline by making all three steps foundations of the IT modernization process.

The following best practices are inspired by Cloud Smart and will help your organization successfully adopt cloud most effectively. They are:

1. Comply with federal cybersecurity standards

Cloud Smart urges agencies to continuously monitor their data in real time to protect against cyberthreats. The policy also suggests that organizations practice a risk-based approach to cybersecurity. This approach revolves around agencies carefully governing their systems to strengthen their cybersecurity.

Subsequently, organizations must choose cloud vendors that comply with federal law regarding continuous, risk-based cybersecurity.

For example, vendors that are certified as secure government cloud providers must adhere to the Federal Information Security Management Act (FISMA) and NIST Risk Management Framework (RMF) standards. Leveraging FedRAMP-certified cloud providers that align with FISMA Moderate, meanwhile, can speed adoption of a cloud framework that can deliver the cybersecurity protections Cloud Smart seeks.

Industry has made significant advances in enabling technologies and frameworks for cloud that allow agencies to comply with security standards as well as innovate faster by leveraging secure, trusted components as part of a cloud architecture framework. This new approach can greatly aid in reducing risks, improving innovation and lowering the cost of security compliance.

2. Look before leaping on cloud procurement

Cloud Smart acknowledges that governmentwide, federal procurement guidance on cloud adoption doesn't exist. Because of this, Cloud Smart recommends that agencies carefully consider which cloud vendor they choose.

Subsequently, Cloud Smart encourages agencies to examine their peers and the private sector for examples of successful cloud procurement. The policy also pushes organizations to

recruit talent that's knowledgeable about effectively buying cloud services.

These procurement practices are important, as they keep agencies from getting stuck with costly, inefficient or inconsistent cloud services because they've signed a long-term contract with a vendor that's not the best fit for their needs. Agencies should exercise caution when building custom solutions or investing heavily in integration of shared services that have proprietary technology stacks that lock in vendors for future services. Shared services may or may not be based on cloud architectures.

Modern cloud architectures based on open technologies that enable more choices for agencies are preferred, thus enabling competitive contract awards and fair competition that yields better performance and cost structures over time. One goal of Cloud Smart is to define the best-of-breed cloud approaches and negotiate governmentwide acquisition vehicles to help streamline acquisition and reduce cost.

3. Make workforces cloud-savvy

Cloud Smart calls on agencies to examine the impact that cloud migration will have on their workforces. The policy suggests, for example, that organizations communicate to their employees how cloud adoption may change their workforce.

Another tip Cloud Smart provides agencies is identifying the cloud-related skills their current employees lack. Agencies can then train their workers in those areas, hire new ones with those abilities or both. Workforces that are knowledgeable about cloud are more capable of acquiring and using the technology effectively.

Cloud Smart additionally encourages agencies to streamline their hiring processes for top cybersecurity and IT talent related to cloud. The policy recommends that organizations use the federal government's hiring authorities, recruitment and student loan repayment incentives to successfully compete with the private sector for talent.

How Micro Focus Government Solutions Helps

Agencies whose procurement methods, security and workforces are ready for cloud will still fail to adopt it without an efficient migration strategy. Organizations that don't carefully plan their move to cloud will waste energy, time and resources.

Tools like Micro Focus Government Solutions' IT Operations Management (ITOM) suite, however, can help agencies maximize their return on cloud investments. ITOM is a PaaS offering that lets agencies govern their infrastructure effectively, whether it involves hybrid cloud, multi-cloud or other cloud environments.

"When it comes to IT management, agencies are realizing they need a cloud platform that's agnostic," Wray said. "ITOM is a platform that runs on open source technologies that are freely available. It's already cloud-ready and Cloud Smart, as it's built on cloud architectures."

Another advantage of ITOM is its PaaS format. Typically, agencies have used SaaS cloud services since Cloud First debuted because they provide only their data to vendors in exchange for the functionality and capabilities that they use. Unfortunately, many organizations have realized that the SaaS model is not without drawbacks, especially when agencies have heavily invested in customizing SaaS offerings for their needs but don't own the technology.

An agency using the SaaS model is dependent on its vendor for the new capabilities and services it wants. If the SaaS vendor doesn't offer them, the agency might be stuck waiting – or

worse, paying to customize the offering that they don't own or control. This introduces future risks and vendor lock-in and restricts competitive choices.

"You're extremely limited by the capabilities that the SaaS vendor has made available," Williams said. "It restricts agencies that are looking to move new functionalities beyond what is provided by that SaaS vendor."

In contrast, Williams said, PaaS offerings like ITOM give agencies a platform for their cloud services that they can develop, manage and run new applications on as their needs change.

"PaaS is a toolbox that an agency can utilize to take the rich set of critical mission and citizen services that are being delivered and evolve those capabilities closer to their cloud delivery model," he said. "It doesn't restrict them on configuration, integration and even customization requirements so they can make progress on re-factoring, re-platforming or sometimes completely rewriting the applications that they deliver as services."

A third advantage of PaaS systems like ITOM is that they let agencies quickly add new applications and services to their platform. ITOM, for example, doesn't sacrifice consistency and reliability while scaling to meet agencies' latest needs.

"We're well prepared for the cloud of the future," Wray said of ITOM.

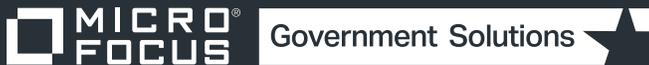


Conclusion

Cloud Smart takes Cloud First to the next level, as it includes cloud procurement, security and workforces in the IT modernization discussion.

Though agencies currently have numerous cloud options, some are better than others for balancing legacy and modern technology. For example, the PaaS framework is especially adept at governing an organization's hybrid cloud and multi-cloud ecosystems. PaaS is a more versatile option for cloud than SaaS because it avoids cloud service vendor lock-in for agencies by enabling them with more choices on their cloud providers.

Pairing Cloud Smart's guidance with PaaS infrastructure in either a hybrid cloud or multi-cloud environment is a winning combination for agencies. By working together, these tools help agencies focus less on upgrading their technology and more on serving citizens and driving more value to their mission priorities faster.



ABOUT MICRO FOCUS GOVERNMENT SOLUTIONS

Micro Focus Government Solutions is a purpose-built, mission focused company that serves US public sector clients. A company anchored by success in the IT industry, Micro Focus Government Solutions is uniquely positioned to help your organization bridge the gap between legacy systems and modern innovation. Backed by one of the largest pure-play software companies in the world, Micro Focus, we help solve critical IT challenges with software solutions in Hybrid IT, DevOps, Security & Risk, and Predictive Analytics.

www.microfocusgov.com



ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.



1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop