

# Capturing And Sustaining Cloud Solutions

Agency technology teams should be having continuous conversations with the mission leaders and their specific vendor community about future state needs to marry the technology capability with the right configuration for mission.

Recently, I had a conversation with a cloud service provider and the individual asked if I believed that government leaders “get” the value proposition for cloud. My immediate response was “yes”, but I wondered what observations prompted that question. As we talked further, I realized that the true question was about why government agencies do not always achieve the results that maximize the value of cloud capabilities.

From a policy perspective, Cloud First<sup>1</sup> was about changing thinking inside government. Cloud Smart<sup>2</sup> was intended to evolve usage of cloud capabilities using a framework to make the right cloud services choices for the specific need of the agency initiative. In my personal experience, federal technology leaders have a clear understanding of the value of cloud-based solutions but capturing and sustaining that value in a federal operating environment is a very different challenge. This article



## Suzette Kent

Federal Chief Information Officer of the United States  
(retired)

Chief Executive Officer  
Kent Advisory Services

is a reflection on today’s challenges and ways that federal teams might achieve mission and technology goals, but also create a pathway for sustained improvement.

## The State Of The Union:

Starting with the highest-level point — the basic value proposition of cloud — there are many federal success stories. Agencies who have measurably improved security, significantly expanded capacity, achieved resiliency, and modernized legacy technology. Even better outcomes have been achieved where agencies rationalized their workloads and optimized the compute, storage, and security to achieve multiple improvements while making the end-to-end process more efficient.

The challenge today is choosing the right cloud capabilities for the specific purpose. Often, the hardest part of that equation is anticipating the future needs for the purpose. As agencies have progressed with digital transformation, the access protocols and data needs have changed.

As automation grows across all parts of government, performance and security demands have changed. One of the most obvious areas driving significant change in business and mission needs is the remote workforce. Today, most federal agencies use multiple cloud providers and use varying service models. This demonstrates that there is not a one-size-fits all purposes and emphasizes that the “fit for purpose” must be continually reassessed.

## Scaling The Enterprise:

So, if one considers the clear evidence of wide-scale government agency use as acceptance of the core value proposition and confirmation of the maturity of vendor offerings, what are the next steps?

The next phase is about operating at secure scale and maturing business operations to sustain effective performance.

Goals for a single application or initiative might not be difficult to achieve. The sophistication and complexity of getting the real value from cloud occurs when an agency begins to scale the agency “enterprise”. This is the point where hybrid cloud operational models, new resiliency protocols and enterprise network visibility are required. As agencies look at the key characteristics of their workload needs such as security, performance, compute capacity, they often have multiple provider options.

To take advantage of those options, they must be able to manage hybrid environments without sacrificing visibility of their entire enterprise operations and they must have pathways to achieve needed interoperability. Add on to these activities understanding the economics of the specific cloud environment and the workload dynamics. This is a complex set of variables to manage, but important to effectively operating at scale.

Evaluating workloads from a rubric combining mission needs and economics is difficult to achieve in a federal operating model. Acquisition approaches that seemed appropriate for the initial projects may not scale well for enterprise utilization. One might choose to train AI models using synthetic data in a public environment because it is less costly and more scalable while a production model running with real data requires a private cloud, augmented with significant security.

Another example might be that data utilization patterns were assumed at specific levels and pathways at the beginning of an initiative but those patterns changed substantially a few years after implementation. In many recent situations

the use of image, voice and other unstructured data vastly changed; therefore, the utilization demands, and compute capacity needed changed drastically, very rapidly. Some agencies have invested significant time into updating their data models separating data that requires different treatment for privacy or security reasons so that they have more flexibility and potentially lower costs when aligning workloads to cloud environments.

Another challenge in scaling an agency enterprise is creating the functional and architectural vision for what components of an agency require a level of connected, interoperable capability and which pieces can function independently. Today, agency technology leaders must have visibility of the enterprise and be able to observe data and activity across providers and environments. Initially, this visibility was about security and resiliency, but it must now extend to operational efficiency and cost. This need for broadscale visibility and richer operational data that can span an enterprise has created new needs for security tools or interoperability of security tools embedded in some cloud environments. Given the cybersecurity environment, this is a time for many agencies to invest in enterprise capabilities that support their hybrid environments.

Today, agency technology leaders must have visibility of the enterprise and be able to observe data and activity across providers and environments.

changed because there was not initiative funding or time allotted to effective skills transfer with the team designated to sustain the new operating environment. In circumstances like these, modernized applications could quickly stagnate again because the investment did not include the people investments necessary to support on-going improvements.

In the scientific agency areas and programs where state-local partnerships are critical, it is imperative that cloud solution approaches are vetted with the specific industry ecosystem to achieve more

secure, accurate data sharing. Examples might be how job information is shared, how weather data is shared, how research outcomes from grants are made public. These are current examples where improved, secure, cost-effective data sharing via cloud advances the mission goals because of alignment with the entity being served.

Governance processes should be designed to periodically revisit the cloud choices made to determine if any of the key variables have changed in a way that would suggest evaluation of other alternatives. This might include cost versus use changes, that might include significant growth in data volume or user demands and many other situations that can change the decision drivers which pointed to a specific cloud solution option.

There have been situations where use patterns of volumes have changed significantly, and agencies received a shock in the rapid rise of their costs. These types of examples make the point for continuous review of choices and contract terms with providers. It also demonstrates the importance of procurement flexibility and development of new models so that a vendor partnership can evolve as agency operating models evolve.

In closing, there is clear evidence that government agencies have embraced the value proposition for cloud services, but the operational processes to achieve and sustain that value must continue to be advanced in ways that span beyond technology infrastructure and across agency mission. ■

---

**Suzette Kent** served as Federal Chief Information Officer of the United States from January 29, 2018 until July 2020. As CIO, Ms. Kent was responsible for setting federal IT policy and leading the Federal CIO Council, which is composed of CIOs from various federal government departments and agencies. Prior to her appointment as Federal CIO, she was a principal of the banking and capital markets advisory team at the Ernst & Young Financial Services Office in Dallas. Currently Ms. Kent is Chief Executive Officer of Kent Advisory Services

In the rush to get legacy applications and data to cloud environments, agencies have to reexamine the end-to-end processes to harvest opportunities to transform. When agencies buy specific solutions, are they using all the features that are available?

There are often multiple solutions implemented in production environments that have duplicative capabilities. As agencies scale their connected enterprise, they should continue to evaluate opportunities to consolidate, shift or grow use of solutions to maximize their return on technical investments. It is also a time to understand vendor goals for interoperability or invest in tools that span solutions for security needs.

### Sustaining Improving Performance

As high performance compute becomes widely available, as digital transformation and automation continue to grow, processes to reevaluate solution choices must become more nimble. This means that the circle of change extends beyond the technology team. It requires continuous partnership with mission, investments in talent development, capability needs discussions with vendors, new procurement models and mature governance and cost modeling to ensure that operating environment is optimized.

Agency technology teams should be having continuous conversations with the mission leaders and their specific vendor community about future state needs to marry the technology capability with the right configuration for mission.

In a recent conversation with an agency CIO, he shared that although he had clear visibility about the fit and functionality of a certain technology capability, the hardware was too big and connectivity models needed were unlikely in the tactical environment of his mission team. This was an opportunity for a dialogue with vendor community about how cloud

might be used to decrease on-site device demands and address some elements of connectivity while achieving the mission needs of the team.

At times, I saw agencies choose cloud environments and tools not because it was the best fit for the workload, but because it better aligned with their mix of talent. It is very natural for a member of the workforce to prefer tools with which they are familiar, but that did not always equate to the best long term fit for the workload.

There were also situations where certain environments were not maximized because the agency investment in human capital or incumbent skills development had not been made. As agency cloud environments become more sophisticated and scale, funding talent upskilling or talent acquisition and retention is critical. Demand and demographics demonstrate that the need for talent in technology areas may become a major obstacle to achieving mission goals. Expanding technology capability can deliver great outcomes but only if the team responsible has the skills to use the capability properly beyond the initial implementation.

In situations where contractors were driving initial work efforts, workforce sometimes was short

As agency cloud environments become more sophisticated and scale, funding talent upskilling or talent acquisition and retention is critical.