Federal Cloud Computing: The Vendor Perspective

Cloud computing has emerged as the federal government’s answer to major information technology challenges, such as infrastructure sprawl, strained budgets and a flat IT workforce. Although many in both government and industry argue that cloud computing has been in practice for awhile, the current iteration has been positioned as a new innovation that will change how the federal government procures and utilizes information technology. The current administration, under the tutelage of former Federal CIO Vivek Kundra, has made cloud computing the underpinning of the future federal IT landscape by attaching it to technology, acquisition and budgetary requirements.

The benefits of cloud computing are clear: easier to manage IT environment, pay only for what is used, on-demand computing resources, reduced time to provision technology and deploy applications, consolidated IT infrastructure with a smaller carbon footprint, etc. The challenges associated with cloud computing have been touted widely and consistently across federal IT decision-makers; the “Big Three” are security, interoperability and portability. However, the prevailing view of most cloud discussions is from the government perspective. While demand-side understanding is critical, what is often missing from the conversation are the challenges that Cloud Service Providers (CSPs) must face as they decide if, when and how to play in the cloud computing market, especially at a time when the stakes are so high.

Cloud Computing Adoption

In general, adoption has been slow; federal agencies have been gun-shy about migrating capabilities – especially mission-critical capabilities – to “the cloud.” While there are clearly some early adopters, nearly all agencies have ventured into the cloud in some capacity. Along the Roger’s bell curve, which classifies people or organizations along a technology readiness continuum, there are numerous agencies that have adopted cloud computing in “low risk” areas or as private cloud solutions:

Roger’s Bell Curve (Technology Lifecycle) – Agency Examples

<table>
<thead>
<tr>
<th>Agency Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovators</td>
</tr>
<tr>
<td>Early Adopters</td>
</tr>
<tr>
<td>DOD</td>
</tr>
<tr>
<td>DOE</td>
</tr>
<tr>
<td>NASA</td>
</tr>
<tr>
<td>DOI</td>
</tr>
<tr>
<td>GSA</td>
</tr>
<tr>
<td>Early Majority</td>
</tr>
<tr>
<td>Army</td>
</tr>
<tr>
<td>NSF</td>
</tr>
<tr>
<td>EPA</td>
</tr>
<tr>
<td>USDA</td>
</tr>
<tr>
<td>DOL</td>
</tr>
<tr>
<td>Treasury</td>
</tr>
<tr>
<td>Late Majority</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>Laggards</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
</tbody>
</table>

Source: Evert Rogers, Diffusion of Innovation Model
Most technology adoption happens after a few bold early adopters have tested the solvency of a new technology, so the bulk of federal cloud computing demand has yet to emerge.

While cloud computing is clearly entrenched in the future vision of federal IT, where does it sit now on the evolution path? While there are early adopters and agencies are moving forward with cloud computing (either voluntarily or by mandate), cloud computing as a federal market is unclear. Most agencies are still in the discovery phase – at least in terms of identifying broad or enterprise-level targets. There are numerous proponents of cloud within the federal government, yet momentum has been slowed by concerns such as security, portability, and interoperability.

There are competing forces that influence cloud computing and limit the level of predictability of adoption:

**Cloud Computing Competing Forces**

- **Drivers**
  - Policy (e.g. “Cloud-First,” Federal Data Center Consolidation Initiative)
  - Long-term Cost Savings
  - Administration “Evangelists” (e.g. Vivek Kundra, CIO Council)

- **Inhibitors**
  - Budget Constraints
  - IT/Mgmt Expertise
  - Technology Barriers (e.g. security, interoperability, etc.)

Key mandates, such as the “Cloud-First” policy introduced in Kundra’s “25-Point Implementation Plan to Reform Federal Information Technology Management,” add momentum to the numerous agency-driven implementations, as does its creator and other federal CIOs serving as cloud computing “evangelists.” The potential cost savings are attractive to all stakeholders, especially agency leadership and Congress.

However, the days of unfettered spending are long gone; agency leaders are working within tighter budget constraints and spending levels that may no longer keep pace with technology needs. This requires reprioritization, and the position of cloud among the list varies by agency. Agencies also lack the required IT and acquisition personnel to build, procure and manage
internal or external private clouds, and the technology concerns about security, portability and interoperability persist.

Managing Market Risk

As agencies move along the adoption continuum, CSPs face challenges from within and without. Externally, competition continues to increase as both traditional federal IT contractors and new, commercially-based providers enter the federal market. CSPs are also challenged with gaining buy-in among its target customer base. Cloud computing is a market that contractors must actively engage in creating, and although policy and regulation aimed at increasing cloud adoption supports this, CSPs must fuel a level of market demand and momentum investment that will justify their investments.

Internally, all federal IT contractors must examine the impact of cloud computing on the other parts of their business. For example, how does Infrastructure-as-a-Service (IaaS) impact hardware pricing? How does Software-as-a-Service (SaaS) impact software licensing models? How do single tenancy requirements impact our strategy? Most importantly, how does cloud computing in general change business models? For those organizations that answered this early and have invested in cloud solutions, they must now answer a different question: will the investment be worth it?

The biggest concerns around cloud computing across the cloud vendor community relate to cloud’s staying power, models of delivery and opportunity identification.

**Will Cloud Computing “Stick?”**

All indicators suggest that the Obama administration has made its case regarding cloud computing. The benefits are clear, there are numerous success models to prove the impact of cloud computing on both budgets and technology environments, and both NIST and GSA are working on addressing the key concerns limiting momentum by developing standards, use cases, security certifications, and contract vehicles.

There are some risks, however. There could be a new administration in office in 2012, which could take a new approach to reducing federal IT infrastructure costs. This scenario is likely one reason for the aggressive approach being taken by OMB; Kundra needs to leverage his current window of influence to propel cloud computing to a level of adoption that would solidify it as a tactic even within a new administration. In other words, if he can push cloud computing far enough down the road, reversal would be cost-prohibitive or have negative impacts on agency performance and delivery of services.

Continued success in cloud computing implementations (and an absence of security issues) will provide an argument for cloud regardless of leadership. But that success could be undermined if the administration pushes implementation too far ahead of policy and strategy, in essence driving agencies to implement cloud solutions before they a) have a solid understanding of where cloud is appropriate and where it is not, and b) have standardized IT environments to a degree that will maximize the impact of cloud investments.

According to several government IT executives, the stickiness of cloud computing will rest on ROI. While agencies are wondering if vendors can help them prove cloud ROI, perhaps the better question is, “Can we define cloud ROI?” There is no consistent government-wide definition, but at a minimum, clear cost savings is a good place to start. But it must be relatable ROI, e.g. cost savings that are feasible within a particular agency’s environment and circumstances.
What Will Federal Cloud Computing Look Like?

The fiscal battles being waged in Congress have the potential to change the tone of the cloud computing dynamic in a way that has a tremendous impact on CSPs. While the preference continues to be private or hybrid clouds, the ongoing security debate raised issues about whether CSPs could secure government data as well as the government could itself. That debate continues, but anecdotal evidence suggests that budget constraints may be overtaking security as a top concern (which Vivek Kundra believes was overdramatized to begin with), and giving private outsourced clouds a larger role in the discussion. The idea of CSPs bearing the infrastructure costs is much more attractive than buying or reconfiguring their own infrastructure, with the assumption that security requirements will be met.

This transition can be seen in both policy and procurement discussions:

- **NIST “Draft Cloud Computing Synopsis and Recommendations”** - published in May 2011, this document discusses many of the drawbacks of the various cloud computing models: on-site private clouds; outsourced private clouds; on-site community clouds; outsourced community clouds; and hybrid clouds. It is interesting to note that this latest NIST publication begins to distill the conversation from simply “public cloud,” “private cloud,” “community cloud,” and “hybrid” down to the level of infrastructure ownership, i.e. on-site and outsourced. Each agency’s risk acceptance, willingness and capacity to innovate, and budgetary pain threshold will determine the approach. However, the NIST document presents an analysis of several key areas that help CSPs identify some of the branches of the decision tree driving cloud computing investments and the tradeoffs under consideration by agencies, such as:
  
  - How reliable is the network? What kind of performance risks exist?
  - Do I have the right internal skill-set to manage a private cloud, regardless of whether it’s on-site or outsourced?
  - How much control do I want/need over geographical location of workloads?
  - What risks does multi-tenancy (internal or external) introduce?
  - How much control over network capacity for data import and export does my organization require?
  - How much control over security does my organization require?
  - What is our cost threshold for upfront investment?
  - How much capacity do we need?

To answer these questions, agencies are looking to CSPs to provide greater information on their operations.

- **GSA Request for Quotation (RFQ) for Cloud Computing Services** - released on May 9, 2011, the RFQ establishes five lots, each with options for a Government Community Cloud; Vendor-Furnished Equipment Private Cloud; Secret Enclave Private Cloud (for High Impact Systems); or Public Cloud. Both the community and vendor-furnished equipment private clouds require single-tenant servers.

“People are still thinking in a stovepipe mentality. Let someone else worry about the hardware refresh and security.”
---Government IT Executive
In a time when outsourcing has been under tremendous scrutiny, it seems that when it comes to cloud computing, agencies are receptive to the idea of outsourced private clouds. The option of shifting the capital expenditure to a CSP and having it build the entire solution on the agency’s behalf cannot be dismissed in the current fiscal environment.

Where Will Federal Agencies Invest?

This is the million dollar question, and although it undoubtedly varies by agency there is a definite preference for hybrid clouds. Interestingly, this is based more on acknowledgement of future needs and limitations vs. current implementation trends. Many of the early adopters, such as NASA, DISA, and Energy, created private clouds, which confirms the widely acknowledged view that mission critical or high performance computing needs will likely be handled in-house, at least until federal agencies reach a higher comfort level with vendor security.

The challenge for CSPs is identifying where their target agencies or bureaus lie on the technology adoption spectrum, which can be particularly difficult in an environment where most cloud implementations have been piecemeal and narrowly focused. While there are some examples of enterprise-wide implementations, (e.g. Army, USDA, etc.), most agencies are utilizing cloud “on the fringe” rather than deploying large scale cloud migrations. However, cloud requirements are increasingly embedded within infrastructure modernization or enhancement projects.

Considering the competing forces and other internal drivers, there are indicators of cloud readiness that, as agencies begin to ramp up cloud efforts, CSPs can seek out:

- Agency is highly virtualized
- Agency has already embarked on small pilots
- Agency has already invested in some infrastructure modernization. Without it, some applications might need to be redeveloped or redesigned to be cloud ready.
- Agency has a solid outsourcing history.

In addition, the Federal Cloud Computing Strategy outlines numerous points for agencies to consider before migrating to the cloud:

- Security ramifications have been analyzed and addressed
- Service characteristics defined (e.g. SLA elements such as availability, performance, reliability, COOP, etc.)
- Vendor/market characteristics defined (e.g. market maturity, portability capabilities, technical standards, etc.)
- Network infrastructure, application and data readiness (bandwidth, legacy applications, etc.)
- Management expertise (e.g. experience negotiating and managing SLAs, technical expertise, etc.)
- Technology lifecycle (e.g. recently upgraded vs. nearing refresh)
Should We Build, Buy or Partner?

For many large federal IT contractors, the answer is “yes.” Major contractors that can afford the investment are doing all three: building private clouds or leveraging existing data center space to dedicate to federal customers (e.g. IBM, Microsoft, Terramark, Harris); acquiring niche cloud providers (e.g. Verizon acquisition of Terramark, Dell acquisition of Boomi, HP acquisition of 3PAR); and developing partner programs specifically for cloud computing vendors (IBM, HP, Cisco).

Business circumstances will determine the approach, but positioning within this space in any capacity will be critical. It is clearly an emerging market with tremendous growth potential. CSPs have the opportunity to shape the federal cloud computing market, but flexibility is important. “Build it and they will come” does not apply; CSPs must be able to keep ahead of demand without overextending resources. Ultimately, this will require deep market intelligence, solid customer relationships, superior business development skills and a little luck.

Conclusion

The federal government is entering an interesting phase in its evolution under unprecedented market circumstances. The convergence of tight budgets, aggressive market players, and increasing acceptance of the cloud computing model will fuel an uptick in demand for cloud computing solutions. However, CSPs must have the capability to overcome perceptions and barriers, articulate benefits and ROI, and maximize competitive positioning to cultivate federal cloud computing demand.

About Federal Industry Analysis (FIA)

This report was developed by Deltek Information Solution’s Federal Industry Analysis (FIA) team. FIA analysts harness Deltek Information Solution’s wealth of data, interviews with government and industry decision makers, and other strategic resources to provide a comprehensive view of the federal IT marketplace and the trends, drivers, priorities, budgets and legislative issues influencing it. With a top-down perspective on all of Deltek Information Solution’s information and analysis capabilities and resources, FIA is able to provide broad, long-range strategic insight on the federal contracting industry and its various sectors that focus on technology.