

Practical Cloud Infrastructure for Federal Executives

Seek Service, Not Just Servers

By Ralph Tufano

The Obama administration's push for cloud computing offers federal agencies the potential for real gains in efficiency and effectiveness. At the same time, it raises challenging considerations for information technology and program executives. On the one hand, moving infrastructure, software applications, and software development out of agency IT shops carries the promise of savings on equipment, facilities, power, and staffing. On the other hand, it brings up questions about performance transparency, integrated management, service levels, cost visibility, security, standardization, and procurement.

Cloud computing is not an either-or proposition, but rather a set of techniques applied to add flexibility, speed, scalability, and efficiency to deliver infrastructure, software applications, and application development. Cloud techniques can be applied outside an agency by a company offering excess capacity on its infrastructure, or by another agency that procures capacity on the government's behalf. They can be applied by a company that hosts software applications and provides them as a service, or by an agency doing so as a shared-service provider for others. Alternatively, one or more agencies could decide to offer such services agencywide or across agencies as a private cloud provider.

When considering cloud solutions, agencies can get the most value by taking a holistic view, including the challenges they face, the data they manage, and their business needs.

In creating a business case, agencies must keep in mind that cloud computing is not a one-size-fits-all solution, especially to the many unique, sensitive, and enterprise-level computing challenges federal agencies face. When considering cloud solutions, agencies can get the most value by taking a holistic view, including the challenges they face, the data they manage, and their business needs. This method will lead to the best possible decision not only about which cloud approaches to use, but also which IT systems to consider for migration to the cloud.

Many agencies already take advantage of cloud computing's efficiency, increased capacity, economies of scale, and enhanced effectiveness by partnering with managed-services providers such as CGI. CGI is applying cloud techniques on behalf of the General Services Administration (including its more than 40 government financial management customers), the Administrative Office of the U.S. Courts and all 94 federal courts, the Interior Department's National Business Center, the National Transportation Safety Board, the Broadcasting Board of Governors, Corporation for National and Community Service, the Architect of the Capitol, and the Federal Communications Commission.

Executives seeking ways to practically apply cloud computing to more effectively achieve their agencies' missions can address these challenges by:

- Knowing the origins of the cloud computing initiative
- Understanding the characteristics of cloud computing in the federal setting
- Building a solid business case that balances potential efficiencies to be gained with

the imperative of achieving real business results

- Carefully reviewing their operations for data sensitivity and mission criticality in order to migrate only those best suited for the cloud
- Analyzing seven key considerations to help them make smart decisions when contemplating the cloud.

Origins of the Federal Cloud Computing Initiative

The Obama administration launched its cloud computing initiative in the 2010 budget proposal, which announced an Information Technology Infrastructure Modernization Program. The aim of the program is to eliminate duplicative IT operations at the agency level by identifying and consolidating enterprisewide common services and solutions. The plan is to transform IT infrastructure first by virtualizing and consolidating data centers — the building blocks of the cloud — and ultimately by adopting a cloud computing business model.

It's important to recognize that the push for infrastructure consolidation is not new; it's simply gaining power as technology evolves. The cloud computing initiative builds upon the information technology infrastructure line of business (ITILOB) begun in 2002. The ITILOB's goal is to drive federal IT practices that improve infrastructure support for agency missions and service delivery; that operate in a secure, standardized, interoperable, extensible, resilient, adaptive, and cost-effective manner; and that encourage collaboration and resource sharing.

The push for infrastructure consolidation is not new; it's simply gaining power as technology evolves.

The 2010 budget proposal defines cloud computing as “a convenient, on-demand model for network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Cloud resources and services can be scaled up and down easily and quickly without altering the infrastructure hardware, generally are Internet based, and relieve users of the cost of maintaining IT infrastructure.

In the proposed budget, the administration suggests that the General Services Administration become the government's cloud computing services provider, supporting implementation through seven pilot projects:

- End-user communications and computing — secure provisioning, securing and supporting (via help desk) of applications across a spectrum of devices addressing telework
- Secure, virtualized data centers
- Portals, collaboration, and messaging for secure data dissemination, citizen and stakeholder engagement, and improved productivity
- Content, information, and records management

- Workflow and case management
- Data analytics, visualization, and reporting
- Enterprise software as a service.

In a June 2009 address to a federal IT conference, Vivek Kundra, federal chief information officer, outlined what he sees as GSA's enhanced role. GSA should become the government's IT services provider to free agencies from worrying about business certification and procuring hardware and software, letting them focus on their missions, he told participants at the American Council for Technology-Industry Advisory Council's Management of Change Conference in Norfolk, Va. He suggested that one day, GSA will centrally provide everything from e-mail services to infrastructure.

GSA Chief Information Officer Casey Coleman told *Computerworld* in May 2009 that the advantages of cloud computing "are so compelling, I don't think there is any going back." Kundra told *InformationWeek* in June that "the cloud computing investment in the 2010 budget reflects the administration's desire to drive down costs, drive innovation across the federal government, [and] make sure we're making available technologies to the workforce that may be available to them elsewhere."

Cloud computing is not an either-or proposition, but rather a set of techniques applied to add flexibility, speed, scalability, and efficiency to deliver infrastructure, software applications, and application development.

Cloud Computing Characteristics

In May, in concert with the ITILOB, GSA issued a request for information about Infrastructure as a Service (IaaS) cloud computing offerings. The RFI is based upon a working definition still under development by the National Institute of Standards and Technology. (See "Cloud Computing: The Working Definition," below.) NIST's final version is due this summer in a special publication on cloud computing and security.

Cloud Computing: The Working Definition

The National Institute of Standards and Technology is developing a definition of cloud computing for use throughout the federal government. Here is NIST's working definition; the final is due this summer:

Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five **key characteristics**, three **delivery models**, and four **deployment models**.

Key Characteristics:

On-demand self service. A consumer can unilaterally provision computing capabilities,

such as server time and network storage, as needed, without interacting with each service's provider.

Ubiquitous network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by many devices, e.g., mobile phones, laptops, and PDAs.

Location independent resource pooling. Provider's computing resources — storage, processing memory, virtual machines, bandwidth, etc. — are pooled to serve using a multitenant model. Physical and virtual resources are dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for rent often appear to be infinite and can be purchased in any quantity at any time.

Pay per use. Capabilities are charged using a metered, fee-for-service, or advertising-based billing model.

Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

Delivery Models:

Cloud Software as a Service (SaaS). Use of the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). Ability to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g., Java, Python, .Net). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). Ability to rent processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy software, including operating systems and applications. The consumer does not manage or control the underlying infrastructure but controls operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).

The focus of cloud initiatives should be on meeting the diverse and unique business needs and solving the business problems of government agencies.

Deployment Models:

Private cloud. Cloud infrastructure owned or leased by a single organization and operated solely for that organization.

Community cloud. Infrastructure shared by several organizations and supports a specific community with shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

Public cloud. Infrastructure owned by an organization selling cloud services to the public or a large industry group.

Hybrid cloud. Infrastructure composed of two or more clouds (internal, community, or public) that remain unique entities but are bound by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting).

Each deployment model can be internal or external. Internal clouds reside within an organization's network security perimeter, and external clouds reside outside it.

Source: Infrastructure as a Service Offerings Request for Information Synopsis, May 13, 2009, QTA-0-09-MH-I-0003

GSA's request to industry for Infrastructure as a Service information is a strong indication that cloud computing offers a unique opportunity for government/contractor collaboration. That partnership will refine an appropriate definition of cloud computing for the federal arena. Companies and agencies will work together to develop a mature business model and security standards and practices, and to share best practices from cloud projects in government and the private sector, as well as from the pilot projects set forth in the 2010 budget. The first step in realizing the promise of this collaboration is building a practical, powerful, and comprehensive case for applying cloud techniques.

Build a Business Case that Balances Efficiency and Results

The federal government spends \$70 billion annually on information technology, nearly half of it on infrastructure alone. The Obama administration wants to consolidate, modernize, and rationalize IT infrastructure to improve the return on this huge investment and reduce its size. Cloud computing is advertised as producing savings in computing capacity and infrastructure, so it appears to be an especially appealing solution to the problem of infrastructure sprawl.

Agencies should differentiate between the tangible benefits available from traditional infrastructure modernization — e.g. server upgrade or consolidation — and the benefits available from applying cloud approaches. Real infrastructure savings are possible via the cloud, but its great promise lies in the services and capabilities it can

provide. The focus of cloud initiatives should be on meeting the diverse and unique business needs and solving the business problems of government agencies.

Focusing on the business application of services provided in the cloud can offer much more than reduced infrastructure and application costs. Those services can improve IT agility, enabling greater responsiveness to agency customers. By lifting the burden of managing IT infrastructure, cloud approaches can help agencies reallocate resources to apply directly to mission accomplishment.

Taking full advantage of cloud approaches will require careful decisions about the business problems they might solve. Agencies must determine how using the cloud provides the best solution to those problems, as well as consider the potential agencywide impacts of turning to the cloud. Once the business case is made, applying cloud techniques requires a carefully crafted approach.

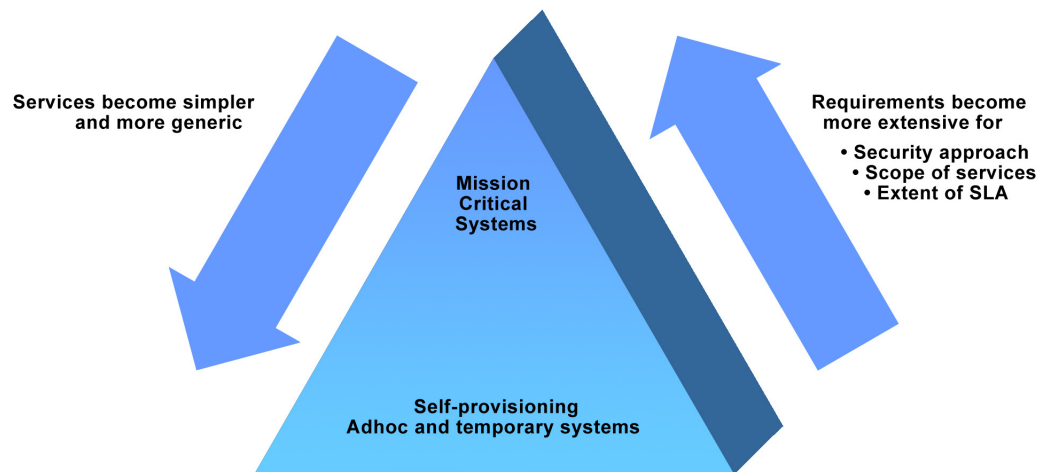
Carefully Review Operations for Data Sensitivity and Mission Criticality

Cloud computing techniques can be used for a range of systems, from those that deliver public and nonsensitive information, to those housing sensitive data, and even those executing mission-critical transaction processing tasks. However, unless cloud services are applied smartly across these systems, the overall price and risk to the government could be higher in the cloud, even for types of data and systems that appear well suited to pure-play cloud approaches.

To decide what's best suited for the cloud, determine where a system falls on the data spectrum (public, sensitive, or mission critical) and what business goals the system is involved in achieving. As the illustration below shows, systems become less amenable to pure cloud provisioning as they rise on the scale of mission criticality and require increasingly stringent security and involve broader scope.

EXHIBIT 1

Applying cloud computing smartly requires different approaches depending on the data involved, ranging from public information to sensitive data to mission-critical transactions.



Once an agency has decided which data and systems are suitable for initial migration to the cloud, the next critical step is selecting a provider. In approaching cloud computing, most agencies will seek support to analyze, develop, and deploy solutions as well as to understand and solve problems they encounter. However, typical cloud computing engagements focus solely on providing physical infrastructure for increased computing capacity. An effective cloud computing provider for the federal government will deliver management support and operational and maintenance services while offering a balance of cost efficiencies and agency results. This balance is vital to providing end-of-the-day value to agencies and to enabling and accelerating agency-by-agency adoption of a governmentwide initiative as ambitious as cloud computing.

Key Considerations When Contemplating the Cloud

Integrated management of cloud computing components — the application of management and governance frameworks to cloud projects — will ensure cloud efficiencies are tied to the achievement of agency-specific mission results. Cloud management services include refining processes; rationalizing and standardizing infrastructure, software, and the delivery model; and sharing infrastructure resources.

Unless cloud services are applied smartly, the overall price and risk to the government could be higher in the cloud, even for types of data and systems that appear well suited to pure-play cloud approaches.

As federal agencies contemplate the cloud, it will be critical to clearly define the key characteristics that apply in the federal arena and to outline the limitations of the approach if it is not managed wisely. Agencies considering cloud techniques should:

- Expect and require transparency into infrastructure and application services
- Demand integrated service management of cloud computing components to align efficiencies with the achievement of mission results — be prepared to synthesize and manage multiple components and service providers or find a partner that can
- Set service levels that matter — make sure they apply to both infrastructure and applications, regardless of who owns the applications
- Factor in all costs, with an eye toward those often not included in typical pay-per-use agreements
- Handle security holistically, being prepared to assume greater responsibility for assuring security for applications if using infrastructure-only providers because they typically offer less security than does a business solution provider
- Achieve savings and better service through standards
- Explore new procurement methods. Current rules would require contract modifications every time an agency sought to dial up or dial down cloud service.

Expect and require transparency. Transparency is vital in managed services relationships. Agencies often require that their operations be conducted on dedicated infrastructure. But reaping the full benefits of cloud-based services means

relinquishing some of this control. In exchange, agencies should expect and require a high level of transparency into application and infrastructure services. Such transparency should include detailed service-level agreement reports with backup documentation to demonstrate how service-level agreements (SLAs) are met, access to providers' incident and change systems, and a view of the details of security events through the provider's portal.

Demand integrated service management. Governance drives success when trying to balance security, outcomes, and efficiency. Information technology governance — with its standardization, cost-saving vendor relationships, economies of scale for components and applications, and efficient labor management — becomes all the more important in a cloud-based environment. Agencies shouldn't turn to cloud platforms with high hopes of saving money on infrastructure, software maintenance, and labor only to be forced to take on time-consuming and expensive integration tasks. They can and should demand integrated service management of cloud computing components to align efficiencies with the achievement of agency-specific mission results.

Set service levels that matter. Measure IT in terms of its business value. Purchasing infrastructure as a service separately from applications makes measuring business value more difficult. Agencies should strive to achieve a service level — for availability and response time — that applies to both infrastructure and applications, regardless of who owns the applications. As government moves into the cloud, agencies will need to develop metrics to show the availability and performance of their business-related applications, not just the availability of the underlying infrastructure.

Success in the Cloud: National Business Center

The National Business Center (NBC), a federal shared-services provider, turned to cloud services for a more effective, less costly way to provide financial management services to agency customers. While NBC clients' hosted financial management applications remain independent from one another, CGI uses shared virtualized servers across the line of business, allowing NBC to create cost efficiencies for each customer. Pooling services on virtualized servers improves service for NBC clients as well as direct CGI customers. The cloud approach means NBC can easily add new customers with only incremental infrastructure expansion. By standardizing hardware, software, security protocols, and infrastructure management processes, CGI can distribute to customers the savings achieved by more efficient use of infrastructure and at the same time reduce their IT footprint and their power consumption. Partnering with a best-in-class provider created a single point of accountability and reduced the technology and management burden on NBC.

Factor in all costs. Visibility into costs that pure-play cloud providers typically leave out of their pricing structures is important to achieving agency goals. Such costs include:

- Licensing compliance management
- Change management and business process reengineering
- Disaster recovery testing
- Comprehensive monitoring across both infrastructure and applications
- Engineering components for optimal cost and service delivery
- Identity management
- Domain name management.

Agencies will need to factor in these costs and others as they weigh whether to acquire infrastructure and other services in the cloud.

Handle security collectively. Infrastructure-only providers typically offer far less security than does a business solution provider, which offers a holistic security view across an entire system. In an IaaS cloud, each agency must assume greater responsibility for assuring security for its applications.

Agencies also should guard against unnecessarily duplicating security efforts: for example, conducting repeated certification and accreditation reviews of cloud services providers. A better approach might be for GSA or another central authority to do certification and accreditation on the general support system once, so agencies don't have to repeatedly do it on their own.

To comply with OMB's effort to reduce Internet connections across government, GSA or another central agency could eliminate the need for every cloud provider to create its own Internet access by provisioning a public cloud with a Trusted Internet Connection (TIC).

Achieve savings and better service through standards. Leveraging standard hardware, software, and processes provides for efficient pricing. Agencies can squeeze out cost at the component level by choosing a cloud provider that has negotiated strategic relationships with hardware and infrastructure software companies. The cloud provider can use its relationships to achieve high-quality service delivery. The ability to synthesize and manage multiple components and service providers is essential to reaching agency outcomes. In the cloud, standardized processes are a must if a cloud provider is to take advantage of best-in-class technology and partners. To fully realize the savings potential of cloud computing, agencies also should consider standardizing their application portfolios when preparing to move to a cloud environment.

Success in the Cloud: Administrative Office of the U.S. Courts

In 2006, the Administrative Office of the U.S. Courts wanted to eliminate the stove-piped architecture in which each court hosted its own instance of the financial management system. Since early 2008, CGI has provided infrastructure services and application management for its Momentum financial management software, consolidating and replacing 94 separate servers with 13 state-of-the-art servers at CGI's shared-services center in Phoenix. In his 2008 year-end report, Chief Justice John Roberts underscored the courts' anticipated savings from using CGI's infrastructure services and software. "The judiciary is currently undertaking a consolidation of technology in its national accounting system, which is expected to achieve savings and cost avoidances totaling \$55.4 million through 2012," Roberts wrote. "Those at the Office of Management and Budget or the Congressional Budget Office may not be impressed by these numbers, but don't forget: The entire judicial branch accounts for only 0.2 percent of the nation's budget. For us, these are real savings."

Explore new procurement models like GSA's highly flexible Alliant contract.

By design, Alliant's scope is comprehensive enough to enable the procurement of all current technology, and flexible enough to incorporate future technology as it becomes available. Alliant allows all contracting types, including firm fixed-price, time and materials, and cost-based orders; this makes for flexibility in solutions development.

Even Alliant's flexibility, however, cannot overcome the challenges of the current cloud computing model. Federal procurement regulations present a barrier to a chief cloud characteristic: the ability to dial capacity up and down at will. Under today's rules, such capacity changes would trigger a change in cost to the agency, thus requiring a contract modification before the change could occur.

GSA CIO Casey Coleman recently addressed cloud procurement challenges in an interview with *InformationWeek*. "Let's say [an agency has] a Website and you don't have ready-made capacity, so you need infrastructure as a service," she said. "You would typically have to prepare a statement of work and go through some kind of source selection, do an acquisition, make an award, conduct a FISMA [Federal Information Security Management Act of 2002] certification and accreditation, and continually monitor that environment, and you would have to replicate those functions every time more Web hosting is needed."

She said that GSA could make the process frictionless by acting as the cloud provider for agencies. "If GSA were to provide infrastructure as a service, and we pre-compete the vendors so that those vendors can compete only on price or on customer

satisfaction for past service, and if we do this business certification and accreditation, then an agency in minutes or hours could have hosting capabilities available,” Coleman said.

Conclusion

The question for senior government executives no longer is whether they will adopt cloud computing approaches, but how and when. Industry partners that already employ cloud techniques and deploy them on behalf of federal customers can support executives as they analyze and develop cloud strategies and deploy cloud solutions. Agency executives should be guided in considering cloud computing by the Obama administration’s goal for the approach: to eliminate duplicative IT operations at the agency level by identifying and consolidating enterprisewide common services and solutions.

The practical, measured approach to cloud computing involves taking a holistic view of the agency’s budget and IT challenges, the types of data it must manage, and its business needs. In determining which cloud approaches to use and which systems to consider migrating to the cloud, executives should weigh the sensitivity of data and the mission criticality of systems.

As with all IT decisions, business needs should drive determinations about appropriate applications of cloud techniques. Thus, building a comprehensive business case for using the cloud is critical, as is care in choosing partners to apply cloud approaches. The following criteria are useful measures in choosing cloud services providers:

- The degree of visibility they offer into application and infrastructure services
- The extent of governance they apply in managing cloud components
- Their ability to offer service levels — for availability and response time — that apply to both infrastructure and applications
- Whether their pricing truly reflects all costs of cloud computing
- Their ability to guarantee security for hosted applications
- The degree to which they can synthesize and manage multiple components and service providers.

Especially when moving forward on as new and rapidly evolving an initiative as cloud computing, agencies that factor these considerations into their decisions will be well positioned to reap maximum benefits.

Ralph Tufano is a director managing technology services for CGI Federal. Over the last 16 years, he has helped customers apply new technologies to solve complex business problems across a variety of industries, including public sector, health care, banking, and insurance. He is a member of the Tech America cloud computing committee and the IAC-ACT cross-SIG cloud computing group.

About CGI

Founded in 1976, CGI is a leading information technology and business process services provider with 25,500 professionals operating in more than 100 offices worldwide. In the public sector, CGI is a major partner to federal, state, provincial, local and municipal governments in the U.S., Canada, Europe and Australia.

CGI has helped more than 100 U.S. federal agencies improve program and back-office operations, allowing them to better fulfill their core missions. Our track record includes enhancing citizen information via healthcare services websites, optimizing IT infrastructure through managed services supporting more than 50 federal agencies, and modernizing financial management operations for more than 100 federal agencies.

Focused on helping government continually adapt and evolve, CGI created the CGI Initiative for Collaborative Government in 2008. In partnership with leading universities the CGI Initiative for Collaborative Government analyzes models of collaboration between government and the private and non-profit sectors, and provides recommendations on how government can best leverage these models to maximize mission results.

More information on the CGI Initiative is available at www.collaborativegov.org. More information about CGI is available at www.cgi.com.

