

# Program Managers, CxOs and the Cloud

## Applying the Cloud for Rapid Savings and Security

March 2011

The current tight budget environment puts Federal executives in a vital and strategic position to generate cost savings and free up increasingly scarce budget dollars for important mission functions.

One important tool at program managers' and CxOs' disposal is cloud computing. Cloud is not just a technology; it is an important budget savings mechanism that, if applied intelligently, can balance security and service while bringing down costs. Recent Office of Management and Budget policy requires agencies to act on cloud savings opportunities. OMB's federal IT management reform plan issued in December 2010 specifies that agencies "default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists."<sup>1</sup>

This issue brief provides a roadmap for program managers, CIOs, security officers, CFOs, and acquisition executives to use in applying cloud computing as a strategic financial stewardship tool to maximize savings and focus resources on mission activities. It also offers information to help these executives provide strategic guidance on budget issues and options when working collaboratively with peers in agency leadership to best apply cloud savings and the OMB "cloud first" mandate in their agency's context. To achieve these goals, this paper addresses three important financial questions concerning the cloud:

- What conditions can we look for that signal a real opportunity for practical cloud savings?
- How do we acknowledge and address real security concerns while making sure we don't leave potential savings on the table?
- How do we avoid running into unexpected additional costs that erode our savings?

### Watch for Five Key Triggers of Cloud Savings Potential

What conditions can I look for that signal a real opportunity for practical cloud savings?

Program managers and CxOs can keep an eye out for the following five key signs of potential savings from cloud computing:

1. **Systems scheduled to replace existing computer equipment.** Agencies can avoid the cost of purchasing new machines by moving a system to the cloud and save an estimated 15-20% on IT infrastructure costs due to three main areas of savings:
  - First, the agency leverages the cloud provider's global economies of scale in computer equipment acquisition, pooled expert IT infrastructure staff, and investments in IT service management technology and operating procedures.

### Five Key Signs of Potential Savings from Cloud

1. Systems scheduled to replace existing computer equipment
2. Planned new system implementations and system upgrades
3. IT infrastructure requests for system conversion, testing or development
4. Pilot projects and investments in new capabilities that are only used periodically
5. Investment requests for developing custom systems

### Two Different Security/Savings Situations

1. Systems housing public data subject to transparency
2. Systems supporting mission-critical operations and sensitive financial and procurement information

### Two Key Steps to Prevent Savings Erosion

1. Seek comprehensive service management
2. Plan and budget for integrating cloud systems with your enterprise

1. Office of Management and Budget, "25 Point Implementation Plan to Reform Federal Information Technology Management," <http://cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf>

- Second, the agency shifts to paying only for the computing power it needs at a given moment in time. For example, the agency can access the computing power it needs to run everyday operations, later add more scale for high-volume spikes, and then turn off the added resources when they are no longer needed (instead of leasing new computers to support peak operations and paying for unused computing power during lower volume periods).
  - Third, the agency can avoid the time and cost of infrastructure-specific security certification and accreditation activities. Instead, agencies can look to leverage certifications by the Federal Risk and Authorization Management Program (FedRAMP) for cloud infrastructure, and focus time and resources on certifying the security of the agency's applications running on that infrastructure.
2. **Planned new system implementations and system upgrades.** New system implementations and major upgrades also typically trigger a need for new computing equipment. Agencies can realize 15-20% savings by deploying these systems directly into an Infrastructure as a Service (IaaS) cloud environment<sup>2</sup> where they can rent, instead of buy, the required new machines.
  3. **IT infrastructure requests for system conversion, testing or development.** Acquiring testing environments for system updates/upgrades in the cloud can reduce the cost of creating and maintaining these environments. The agency can provision servers (and incur costs) in the cloud only when needed instead of paying for unnecessary continuous capacity.
  4. **Pilot projects and investments in new capabilities that are only used periodically.** If an agency doesn't require or desire ownership of a software package, the Software as a Service (SaaS) cloud approach provides access to new or additional functionality with minimal costs. This also applies to software required only on an as-needed or trial basis. For example, in advance of the next fiscal year budgeting cycle, an agency might want to pilot software that automates budget formulation. Using a SaaS cloud approach, the agency can acquire just the access it needs for the pilot, expand its use of the software during the peak budget preparation season, and then scale back to use by core budgeters during other times of the year.
  5. **Investment requests to develop custom systems.** For custom development needs, a Platform as a Service (PaaS) cloud approach provides the ability to develop custom applications or capabilities without having to purchase the necessary infrastructure or development software. The agency can rent a development platform in the cloud, build the capability it needs, migrate the application into steady state operation, and then turn off the development environment when the project is complete.

Five Key Signs of Potential Savings from Cloud	Recommended Actions for Program Managers and CxOs
1. Systems scheduled for hardware renewal or refresh	Avoid the cost of purchasing new machines by moving a system to cloud Infrastructure as a Service, where you can rent instead of buy required new machines and save an estimated 15-20% on IT infrastructure costs.
2. Planned new system implementations and system	Consider deploying a new system or upgrade directly onto cloud infrastructure, and realize similar 15-20% savings.
3. IT infrastructure requests for system conversion, testing or development	Acquire servers (and incur costs) for conversion, test and development environments from the cloud as needed instead of assuming equipment ownership costs.
4. Pilot projects and investments in new capabilities that require only periodic use	Pilot use of Software as a Service—software housed in the cloud and provided on a per-use/per-user basis—for functions with periodic spikes in usage needs (e.g., budget formulation).
5. Investment requests for developing custom systems	Pilot use of Platform as a Service (PaaS) to develop custom applications or capabilities without having to purchase the necessary infrastructure or development software.

2. For more information and definitions of cloud terminology and concepts, please visit [www.cgi.com/cloud](http://www.cgi.com/cloud)

Two Different Security/Savings Situations	Recommended Actions for Program Managers and CxOs
<ol style="list-style-type: none"> <li>1. Systems housing public data subject to transparency</li> <li>2. Systems supporting mission-critical operations and sensitive financial and procurement information</li> </ol>	<p>Look to leverage the maximum savings using public clouds.</p> <p>Take advantage of virtual private clouds to establish the security necessary while still realizing meaningful savings by leveraging the cloud provider's economies of scale.</p>
Two Key Steps to Prevent Savings Erosion	Recommended Actions for Program Managers and CxOs
<ol style="list-style-type: none"> <li>1. Seek comprehensive service management</li> <li>2. Plan and budget for integrating cloud systems with your enterprise</li> </ol>	<p>Consider all of the services required to deliver your systems, and verify potential providers' experience delivering those services within federal constraints.</p> <p>Include specific incremental projects to integrate systems migrated or deployed in the cloud into your agency's broader ecosystem.</p>

### Seize Potential Savings While Seriously Addressing Security

How do we acknowledge and address real security concerns while making sure we don't leave potential savings on the table?

According to the National Institute for Science and Technology (NIST), the number one reason agency managers cite for not migrating specific systems to the cloud is security. NIST has identified security as a "major issue" that will "define how we adopt and deploy cloud computing solutions." And yet, potential for savings from cloud techniques still exist even for systems requiring moderate or high levels of security.

Program managers and CxOs can seize on opportunities for savings by rapidly assessing potential cloud models and the savings they can achieve, even if a given system requires moderate or high security. To focus such efforts, executives can consider different savings optimization approaches for the following two major types of agency systems.

1. **Systems housing public data subject to transparency.** These systems may be the first to leverage the cloud and can achieve maximum savings using public clouds. For example, the Recovery Accountability and Transparency Board deployed Recovery.gov in the cloud, and NASA has leveraged the cloud for public information. When programs use the public cloud for public-facing information and systems, the agency should demand that cloud providers deliver a security level that prevents data tampering or disruption of service.
2. **Systems supporting mission-critical operations and sensitive financial and procurement information.** Many mission critical program systems house data (for example, personal identifiers captured by agencies with financial or health-oriented programs) that require tighter security than a public cloud is intended provide. Other systems also fall into this category. For example, federal financial systems manage multiple types of sensitive data, including budget information, procurement information, purchase card numbers, banking information for payments, or Social Security numbers. These systems are not simple commodities, and therefore are not good candidates to deploy in public clouds. Instead, mission systems and financial systems containing sensitive data are better suited to virtual private clouds, where agencies can deploy higher levels of security.

### Virtual Private Clouds – Balancing Security and Savings

Virtual private clouds provide agencies exclusive use of computing infrastructure and allow them to dictate specific security measures, while still realizing meaningful savings by leveraging the cloud provider's economies of scale. Agencies can confidently deploy systems with a "moderate" security classification (as defined by FISMA guidelines) in a virtual private cloud managed by a private sector provider with experience in federal IT security requirements. In fact, providers awarded positions on the GSA's Infrastructure as a Service blanket purchase agreement are required to offer cloud infrastructure that meets FISMA Moderate requirements. This approach makes it possible for agencies to directly leverage the environments being certified under the GSA IaaS BPA to support a large number of existing and planned federal systems. Additionally, agencies with security requirements higher than FISMA Moderate can work with the cloud providers to design and deploy a virtual private cloud that meets their more stringent security specifications.

## Act to Prevent Unanticipated Expenses or Costly Gaps in Service

How do we avoid running into additional unexpected costs that erode our savings?

1. **Seek out comprehensive service management.** Agencies can avoid unexpected costs and gaps in service by demanding a full accounting of all the services required to deliver their systems in the cloud, and verifying potential providers' experience delivering those services within federal constraints. Cloud management services that are important for federal cloud success include: system management, maintenance and security; backup and restore; access and user administration; operating system and application administration; capacity planning; change control; documentation and maintenance; help desk; disaster recovery and continuity of operations, and technology refresh management.

There is a significant difference between a "commodity cloud" provider that only delivers access to technology, and a full-service business solution provider that can shape services to meet client needs with a "fully managed cloud." Unless your agency is prepared to synthesize and manage multiple cloud components and service providers, you will benefit from demanding clear service agreements from your cloud provider to hold them accountable for service delivery. This step is vital in order to avoid gaps in service or security.

2. **Plan and budget for integrating cloud systems with your enterprise.** As agencies migrate systems to the cloud or add new cloud systems to their operations, it is important to plan and budget for integrating these systems, their workflows and their data into the agency's broader ecosystem. You can minimize the costs of interoperability maintenance by limiting the number of different cloud service providers you use to reduce the burden and cost of integrating across different clouds.

### CGI at a Glance

Founded in 1976, CGI is one of the largest independent information technology and business process services firms in the world. We deliver end-to-end services and solutions in application and technology management, systems integration and consulting, business process management and services, advanced engineering and technology services, and operational support services. CGI and its affiliated companies employ approximately 31,000 professionals in more than 125 offices worldwide.

Learn more about CGI's cloud services at [www.cgi.com/federalcloud](http://www.cgi.com/federalcloud).

### Why CGI?

- Built-for-government. CGI's powerful combination of cloud solutions are focused entirely on meeting government and enterprise-grade requirements.
- Readily accessible federal contracting options. Agencies can acquire CGI cloud services under GSA's new cloud Infrastructure as a Service blanket purchase agreement.
- Expert guidance. CGI has nearly 35 years of experience in providing infrastructure and managed services for complex organizations, and integrating those solutions with current environments. CGI's infrastructure services support more than 50 federal agencies.
- Rapid results. CGI has delivered entire applications to meet critical government needs (e.g., health care reform and American Recovery and Reinvestment Act) faster than agency data centers could deliver just the infrastructure.
- Proven approach. Our processes, governance, security and service levels enable government to focus on its mission rather than building and managing IT infrastructure.
- Full-service cloud portfolio. We also offer Software as a Service (SaaS) and are adapting our industry-leading applications to support the SaaS delivery model. In addition, our consulting services help clients create effective cloud strategies based on their mission priorities.