

The Complete Cloud

Creating and preserving savings, security and service through solid transition planning and automated service management

The Office of Management and Budget has estimated that cloud computing offers the ability to provision IT services on demand at up to 50 percent lower per unit cost. The cloud also promises the benefits of:

- Greater transparency for planning and continuous improvement
- Better support for data-driven decision making and collaboration
- Greater flexibility to meet rapidly changing business needs
- Verifiable performance measures
- Reduced risk and improved security posture.

Creating and preserving cloud infrastructure savings, security and service, however, requires active engagement by agencies or their qualified cloud providers to prevent erosion of the benefits that drew them to the cloud in the first place.

Easy access to cloud Infrastructure as a Service by individual users and programs makes it difficult for organizations to track and manage these services holistically. Agencies can learn from lessons of the past to prevent their cloud services and costs from sprawling out of control while also making sure their systems run smoothly, their data remains secure and their service levels are maintained or improved.

Key success factors for a complete cloud approach include:

- Effective service management to ensure that critical processes are followed and that they deliver savings, security and service
- Automating those services to provide the greatest value
- Well-defined service levels that embed savings, security, service and scalability for the life of a cloud service
- Solid transition planning and implementation to maintain secure operations and prevent hidden costs.

Identifying the services required to get to the cloud

Seek service, not just servers

Good service management requires significant discipline to ensure compliance with an agency's standards, policies and objectives. In fact, lack of service management is often at the root cause of user dissatisfaction with traditional IT.

Creating and preserving cloud infrastructure savings, security and service requires active engagement by agencies or their qualified cloud providers to prevent erosion of the benefits that drew them to the cloud in the first place.

This issue paper is intended to help agency program managers realize even greater value from the cloud—and avoid value erosion—by planning and managing cloud solutions holistically to address service management and transition, not just technology management.

ITIL: the gold standard of service management

“The primary objective of Service Management is to ensure that the IT services are aligned to the business needs and actively support them ... If IT processes and services are implemented, managed and supported in the appropriate way, the business will be more successful, suffer less disruption and loss of productive hours, reduce costs, increase revenue, improve public relations and achieve its business objectives.”¹

The Information Technology Infrastructure Library (ITIL) is a public framework that describes best practices in IT service management

Typical “commodity” cloud offerings only provide physical infrastructure and do not include service management. They essentially follow a least-cost model that assumes customers will read the documentation, learn the provider’s unique language, and determine how to plug the services into the agency’s environment.

This “read the fine print” approach is not viable for most agencies that require support for analyzing, developing, deploying and troubleshooting their solutions. Agencies should not turn to cloud computing with high hopes of saving money on infrastructure and labor, only to take on time-consuming and expensive management and integration tasks. Seeking cloud solutions that include service management can fill the gap.

An important first step is to identify all of the service management components—including staff and equipment—that are needed to move an application to the cloud.

Key service management disciplines include:

Discipline	Purpose
Access Management	Who can use the cloud
Capacity Management	How much to buy and how to control it
Change Management	How to control changes without disrupting operations
Release & Deployment Management	How to control what gets added to the cloud
Configuration Management	Know what you have in the cloud
Event Management	Know what happens in the cloud
Incident Management	Know when something is broken and how to get it fixed
Knowledge Management	Know where all of information is about your cloud
Security Management	How to protect your agency and your data
Service Level Management	How to get the performance you need
Request Fulfillment Management	How to handle user requests for new things in the cloud

Agencies can also decide whether they want to manage multiple components and service providers, or prefer that a qualified partner manage their cloud services for them. A full-service cloud provider can deliver the personnel, management oversight, tools and processes to support the IT infrastructure and complete the security and other services for applications running on that infrastructure. Having the cloud provider manage these services frees internal agency resources to focus on other mission priorities.

Automating service management

Automated service management for cloud computing is an imperative. Embedding processes into the system removes the burden of enforcement and provides an easier path to adoption. By choosing the right cloud provider, agencies can achieve best practices in IT service management and still deploy to the cloud quickly.

¹ <http://www.itsmfi.org/content/introductory-overview-iti-v3-pdf>

Lesson Learned: The costs of technology without service management

Virtual sprawl is the proliferation of virtual servers without adequate IT control. Several years ago, when an enterprise found it had more than 5,000 virtual machines in its data center, it decided to learn which were no longer needed by shutting them down. The answer: 70% were obsolete but still consuming resources and software licenses. The virtual machines were so easily generated, IT had trouble tracking how many there were, and when and where they were deployed.

Fast-forward to the cloud. The agency responsible for one of the largest federal websites is having a similar experience. Due to a lack of governance, they cannot track who created what server and whether a server is still necessary. As a result, they are paying more and more each month for services, eroding the savings derived from the economies and elasticity of the cloud. They question whether they are getting any more value for their money.

Setting service levels that matter

Purchasing infrastructure separately from applications makes measuring business value more difficult. Agencies can develop metrics to show the availability and performance of their business-related systems, not just the availability of the underlying infrastructure. They can also benefit from service levels that apply to both infrastructure and applications, regardless of who provides them.

Key service-level considerations for each system an agency plans to run on cloud infrastructure include:

- How critical is the system?
- What are the acceptable availability, recovery time and recovery point objectives?
- What are the performance characteristics and needs of the system?

Agencies can compare their needs with the service levels offered by cloud providers to determine which will meet their requirements

Transparency is vital in all managed services relationships—and the cloud is no different. Agencies can require a high level of transparency into cloud infrastructure via detailed documentation of how SLAs are met, as well as access to the provider's incident and change systems and security event details.

Guidelines for setting service levels

- ✓ Distinguish between service levels, service requirements and reporting requirements
- ✓ Ensure service levels represent business impact
- ✓ Measure outputs not inputs
- ✓ Set service level targets that are achievable, measurable and auditable
- ✓ Distinguish between desired and contracted service levels
- ✓ Keep service levels to a number that is reasonable for the agency to manage
- ✓ Ensure service levels reflect risk associated with contract terms

*"Cloud Infrastructure as a Service (IaaS) providers differentiate themselves based on the quality of their service and support. Buyers must pay close attention to these aspects, as they are among the most significant contributors to the cost and agility of the solution."*²

-Gartner

² Gartner Research Note: "Cloud IaaS: Service and Support Models," Lydia Leong, 8 March 2011, ID Number G00210094, Page 1.

Solid Transition Planning

Control operational and security risks in moving applications

Once an agency has determined what systems it wants to move to the cloud, the next challenge is to ensure the move happens without service interruptions or security breaches. This process is called “transition.” Transition requires a disciplined process for deciding and planning the move in a low-risk, step-by-step way, with a solid business case for each move. A baseline discovery can be used to determine the best approach, including whether and how to phase the transition (similar to a traditional managed services project). Areas of transition to be addressed are:

- Migration of the system
- Migration of the data
- Ongoing operation and support of the system
- Responsibility for each aspect of the system (If an agency has different vendors for software, infrastructure, modifications and integration, how will their separate but tightly coupled responsibilities be synchronized?)

A solid transition process should reflect a keen understanding of the nature and purpose of the system and include:

- **A well-defined project plan** that is approved by the agency with a clear beginning and end, a relatively short timeframe, and key client-acceptance milestones
- **Clearly identified transition leadership** for both agency and cloud provider, with project management from the provider that is separate from service delivery management
- **A formal policy and common framework** for implementing all required changes so that no services, stakeholders, or events are missed, and service failures are prevented
- **A well-defined Knowledge Acquisition/Knowledge Transfer plan** that ensures the right person has the right knowledge at the right time to deliver and support the system.

Effective federal cloud transitions require providers with prior experience in complex federal system transitions. Full-service cloud providers can also help identify, manage and control the risks of failure and disruption across transition activities. In addition, they may be willing to wrap the price of transition into predictable cloud usage fees.

Starting with GSA’s BPA for Infrastructure as a Service

Agencies can begin by evaluating cloud providers on the General Services Administration’s Blanket Purchase Agreement (BPA) for Infrastructure as a Service³ as it provides a solid foundation for acquiring secure, robust and cost-effective services. As a standardized vehicle, the BPA represents current industry best practice and addresses key challenges around security, contracting and transparency. For example, it requires that awarded providers meet Federal Information Security Management Act (FISMA) moderate security standards, provide at least two data centers in the continental U.S. and offer tools for monitoring, control and reporting.

While the BPA has considered a number of service management issues, it is important to understand how each awarded provider is implementing service management and whether they offer transition services, as there are significant differences in approaches and capabilities. These are key factors behind price differentials between “commodity” and “fully managed” cloud services.

(Note: Recognizing that additional services are needed for a complete cloud, GSA is drafting a template for agencies to use to acquire services for data migration, content management and application migration.)

³ <http://www.info.apps.gov/node/22>

Conclusion

A holistic approach to technology management, service management and transition implementation is necessary to realize the full promise of the cloud. Agencies can maximize savings, security and service by choosing providers with the capability and know-how to provide a complete cloud approach.

When evaluating cloud providers, agencies will benefit from asking:

- Does the provider follow ITIL, the gold standard of service management?
- Have they automated service management into the cloud solution?
- Can they extend the service management processes to the application to encompass the entire solution?
- Do they offer additional services such as management support and operational and maintenance services?
- Can they perform the needed migration and transformation?
- Do they have experience with complex federal environments?
- Do they offer a flexible transition approach that aligns to the agency's program objectives, constraints and cloud-readiness?
- Can they leverage the inherent savings of the cloud to spread costs over the life of the service, to reduce the total cost of ownership and eliminate upfront transition costs?
- Do their available SLAs meet the needs of the agency's system?

In short, agencies can achieve strong security and maximize savings by seeking GSA BPA vendors with: ITIL-based service management that is woven into an automated framework, solid transition planning capabilities and experience, and SLAs that match agency needs for availability and performance.

*"...all cloud IaaS offerings are not created equal, despite superficial similarities in the way the offerings are described. There is considerable variance in service provider design goals, the quality of technical implementations, and the cost-effectiveness and value for money of those implementations."*⁴

-Gartner

5

Why CGI

CGI has the global commercial infrastructure management expertise and federal IT experience to help you deploy on-demand, cost-effective and secure cloud services. Our nearly \$1 billion infrastructure business encompasses world-class data centers and IT equipment, allowing clients to delegate entire or partial responsibility for their IT functions. We follow global best practices in service management and transition planning to ensure that clients get results they can count on in the short- and longer-terms.

We are:

- Trusted by more than 180 CIOs to provide the efficient, secure and reliable technology infrastructure services that run their businesses and support their missions
- Experts in translating our commercial expertise and innovation for federal agencies
- Agile, flexible and technology independent, working with today's existing infrastructure and providing scalability for tomorrow's requirements
- Recognized in data center services, receiving a "strong positive" rating within Gartner's 2010 "MarketScope for Data Center Outsourcing, North America" research report⁵
- Members of the board of directors of the Uptime InstituteTM and members of The Green Grid[®].

⁴ Source: Gartner Research Note, "Cloud IaaS: Service-Level Agreements," Lydia Leong, 7 March 2011, ID Number: G00210096, Page 3

⁵ Gartner, Inc. MarketScope for Data Center Outsourcing, North America, R. T. Matlus, W. Maurer, March 10, 2010. * The MarketScope is copyrighted 2010 by Gartner, Inc. and is reused with permission. The MarketScope is an evaluation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the MarketScope, and does not advise technology users to select only those vendors with the highest rating. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CGI's ITIL v3-based processes and tools provide a cohesive set of best practices for IT services operations. Our thought leadership in service management has evolved into a fully integrated solution that enables IT organizations to quickly adapt to market needs and effectively support business priorities.

Our extensive qualifications in hosting and transitioning federal systems includes financial systems management for more than 50 agencies. As a full-service cloud provider awarded the GSA BPA for Infrastructure as a Service, CGI provides infrastructure, service management, transition, training, help desk and cloud integration and consulting services. In addition, as an industry-leading managed services provider, we can blend cloud solutions with traditional infrastructure to accommodate your needs.

With CGI, you do not have to worry about gaps in your service. We have what it takes to make your application and infrastructure work in the cloud. To learn more about federal cloud computing approaches, or to talk to a CGI cloud expert about your specific situation, contact your CGI Federal account partner or visit us on the web at www.cgi.com/federalcloud.

About CGI

A global leader in IT, business process, and professional services, CGI partners with federal agencies to provide end-to-end solutions for defense, civilian and intelligence missions. For 35 years, we have delivered quality services to help clients achieve results at every stage of program, product, and business lifecycle. We deliver end-to-end solutions in application and technology management, systems integration and consulting, business process management and services, advanced engineering and technology services, and operational support services. Our proven capabilities in high-demand areas include cloud, cybersecurity, biometrics, citizen services, data exchange, health IT and energy/environment. CGI has 31,000 employees in 125+ offices worldwide.