White Paper

Cloud Computing in the Public Sector:
Public Manager's Guide to Evaluating and Adopting Cloud Computing

Authors
Russell Craig
Jeff Frazier
Norm Jacknis
Seanan Murphy
Carolyn Purcell
Patrick Spencer
JD Stanley

November 2009

Cisco Internet Business Solutions Group (IBSG)

Cloud Computing in the Public Sector:
Public Manager's Guide to Evaluating and Adopting Cloud Computing

Executive Summary

Cloud computing—delivering infrastructure, services, and software on demand via the network—offers attractive advantages to the public sector. For example, it has the potential to reduce information and communications technology (ICT) costs by virtualizing capital assets like disk storage and processing cycles into a readily available, affordable operating expense.

Some public sector organizations have made early moves into cloud computing. For example, in Washington, D.C., all 38,000 city government employees have unlimited access to Google documents and services such as Gmail. The U.S. General Services Administration recently announced moving the government-wide portal usa.gov to the cloud and issued an RFI for cloud infrastructure services. In Japan, the Ministry of Internal Affairs and Communications has announced plans to shift all government agencies into a private cloud environment by 2015.

One of the most significant cloud computing opportunities for the public sector is the ability to share ICT resources among multiple agencies. While governments have tried hard to create frameworks geared toward shared services, these have not always been successful. Cloud computing offers an easier and less burdensome route to more efficient and effective public sector information management. This may be especially true for developing countries that do not have the technology, skilled personnel, or resources to create world-class ICT infrastructures.

Of course, cloud computing is not without its challenges:

- A service provider residing outside of a government's legal or territorial jurisdiction may put access or security at risk.
- Open standards and interoperability may not be guaranteed, leading to the risk of vendor lock-in.
- Data privacy is a concern when using public clouds. This can be addressed by the development of private clouds.
- Business continuity will continue to be a concern. Cloud computing, however, may also mitigate this risk, as cloud vendors are likely to use more robust and better-maintained computing platforms that provide more redundancy and are less likely to fail.

Public sector ICT managers preparing for adoption of cloud computing should take these critical steps:

- **Identify all potential opportunities** for switching from existing computing arrangements to cloud services.
- **Assure that in-house infrastructure** complements cloud-based services. Virtualization will be a key element of a compatible infrastructure.
- **Develop a cost/benefit and risk-evaluation framework** to support decisions about where, when, and how cloud services can be adopted.
- **Develop a roadmap** for optimizing the current ICT environment for adoption of public and/or private cloud services.
- **Identify which data cannot be held in public cloud computing environments** for legal and/or risk-mitigation reasons.
- **Identify and secure in-house competencies** required to manage effective adoption of cloud services.
- **Designate a cross-functional team** to monitor cloud computing services, providers, and standards, and to determine if they affect the roadmap.
- **Evaluate technical challenges** that must be addressed when moving any current information or applications into a cloud environment. Experiment with and pilot various services—both internal and external—to identify where issues will arise.
- **Ensure that the networking environment is ready** for cloud computing.

Cloud computing is a natural evolution of the Internet, requiring careful consideration and planning.

Introduction

Recently, one of the hottest topics in information technology has been the emergence of so-called "cloud computing." Much ink and many bytes have been devoted to discussing this phenomenon. Public managers may find this information formidable to consume, and decisions about cloud computing difficult to make.

While clearly at an early stage of development, cloud computing is not "vaporware." Major companies are now offering cloud computing services. Prominent players to date include Google (initially through its Google Apps[1] offerings), Amazon (through its Web Services[2]), and Salesforce.com[3] (through its CRM software service and, more recently, its Force.com application development and deployment service). Major ICT vendors including IBM, Microsoft, and Cisco have cloud computing strategies, products, and services, and a plethora of smaller companies are also entering this market.

The Cisco® Internet Business Solutions Group (IBSG) believes that cloud computing is more than a fad and certainly something that governments should be exploring. Many in and around the ICT industry are clearly anticipating that cloud computing will become a dominant model of enterprise computing. As Nicholas Carr put it in *The Big Switch: Rewiring the World, from Edison to Google:*

1. http://www.google.com/apps/intl/en/business/index.html
2. http://aws.amazon.com/
3. https://www.salesforce.com/au/platform/

"In the years ahead, more and more of the information-processing tasks that we rely on, at home and at work, will be handled by big data centers located out on the Internet. The nature and economics of computing will change as dramatically as the nature and economics of mechanical power changed with the rise of electric utilities in the early years of the last century. The consequences for society—for the way we live, work, learn, communicate, entertain ourselves, and even think—promise to be equally profound. If the electric dynamo was the machine that fashioned twentieth-century society—that made us who we are—the information dynamo is the machine that will fashion the new society of the twenty-first century."[4]

This push by the ICT industry, coupled with the significant benefits that cloud computing promises to deliver, leads Cisco IBSG to believe that cloud computing will be widely used in government in the future. At the same time, we understand that the distinctive features of public sector information management mean that governments need to carefully evaluate whether, where, how, and when they might adopt cloud computing.

This paper seeks to help in that process. It provides a high-level overview of cloud computing, outlines some of the key benefits it could deliver to government, looks at some of the most important challenges cloud computing may pose for government, and suggests some early steps that can be taken toward its adoption. We plan to follow this with papers that examine various aspects of cloud computing in greater detail.

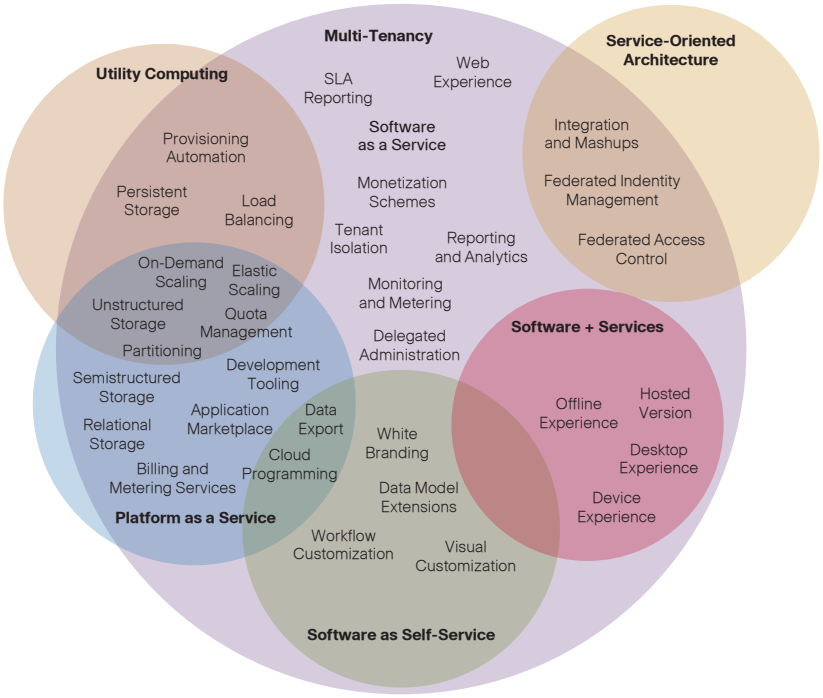
What Is Cloud Computing?

Figure 1 shows the emerging topology of cloud computing, and how cloud computing maps to the array of public and commercially available services. Figure 2 shows that the roots of cloud computing can be traced to the early 1990s and the concept of grid computing, through which many computing devices were networked together to work on a single problem—usually scientific in nature and requiring exceptionally high levels of parallel computation. Grid computing led to utility computing, which attempted to provide metered computing services as though they were a utility. Utility computing led to Software as a Service (SaaS), which allows users to access commercially available software online instead of using it locally, charging service fees instead of selling licensed applications.

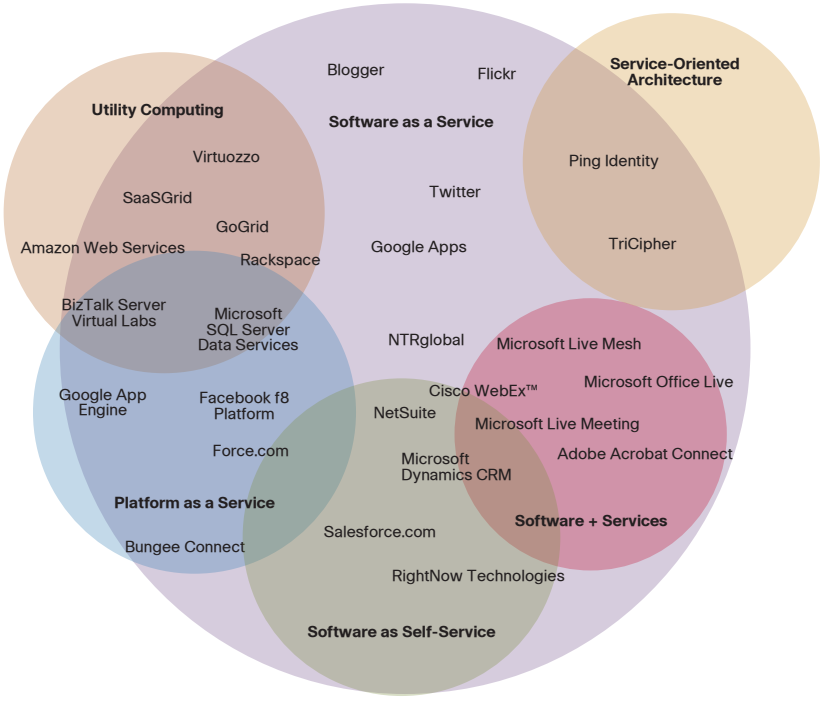
Growing out of grid computing, cloud computing transforms once-expensive capital assets like disk storage and processing cycles into a readily available, affordable commodity. The major driver of cloud computing has been the recognition that large data centers have thousands of servers that generally do not operate at full capacity, creating a surplus of computing resources. By using these resources more efficiently, cloud computing enables greater returns on data center investments.

4. *The Big Switch: Rewiring the World, from Edison to Google*, N. Carr, W.W. Norton & Co., 2008.

Figure 1. The Emerging Topology of Cloud Computing Products and Services



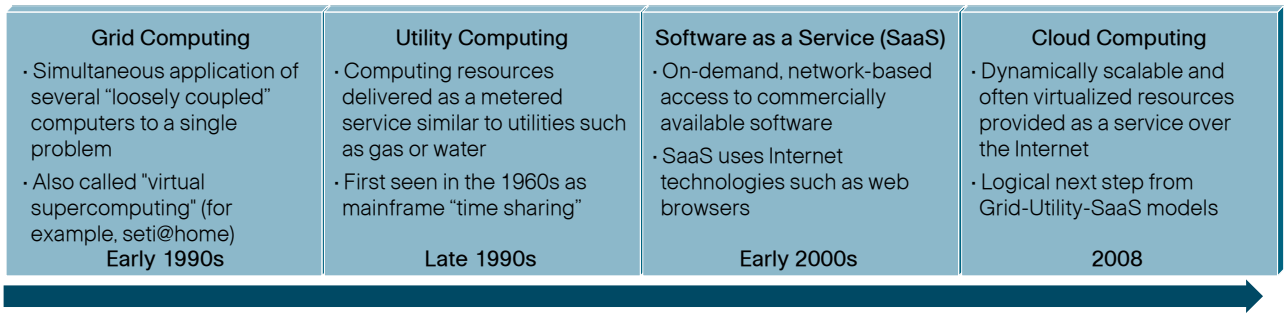
The top figure delineates the categories of cloud services available, and specific services within each category. The bottom figure shows the services available commercially in each category.



Source: Matias Woloski, 2008[5]

5. http://blogs.southworks.net/mwoloski/2008/08/19/cloud-computing-taxonomy-map/, August 19, 2008.

Figure 2. The Evolution of Cloud Computing



Source: Cisco IBSG, 2009

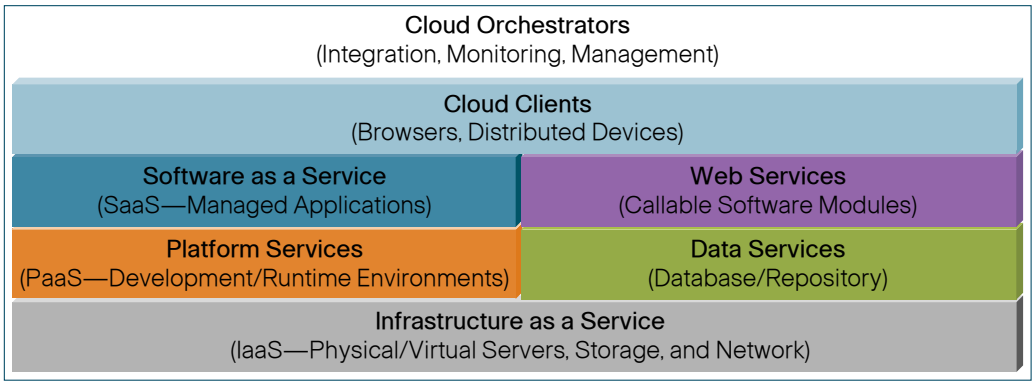
A multitude of simple definitions emphasize the delivery of computing services over the Internet. Cloud computing is, however, more complex than this. IDC suggests that definitions should be given to both "cloud services" ("consumer and business products, services, and solutions that are delivered and consumed in real time over the Internet") and "cloud computing" ("an emerging IT development, deployment, and delivery model, *enabling* real-time delivery of products, services, and solutions over the Internet").[6]

With this in mind, we believe the best definition is the one currently used by Cisco:

"Cloud computing is a broad term, but in our view maps to methods that deliver infrastructure, services, and software via the network on demand, and at scale. Cloud is based on a foundation of virtualization, in which pools of (virtualized) resources are dynamically organized for the benefit of software applications and services. This will change the way that applications are written and delivered."

In 2008, the authors of another Cisco IBSG paper on cloud computing ("Casting a Ray of Sunshine on Cloud Computing"[7]) observed that it is more useful to talk of "cloud services," as there are many more services offered in the cloud than simply computing. The authors presented a framework of seven main services that can be found in the "cloud services stack" (shown in Figure 3).

Figure 3: Cloud Services Stack



Source: Cisco IBSG, 2008

6. http://blogs.idc.com/ie/?p=190
7. "Casting a Ray of Sunshine on Cloud Computing," Jim Cooke and Shaun Kirby, Innovations Practice, Cisco Internet Business Solutions Group, November 2008.

Drilling further into these services reveals a wide array of solutions already being delivered in the rapidly developing cloud computing marketplace, as illustrated in Figure 1. We believe it is essential that public managers monitor this market closely, as it is likely to have a profound impact on the way government makes best use of ICT in the future. In 2008, Gartner stated that:

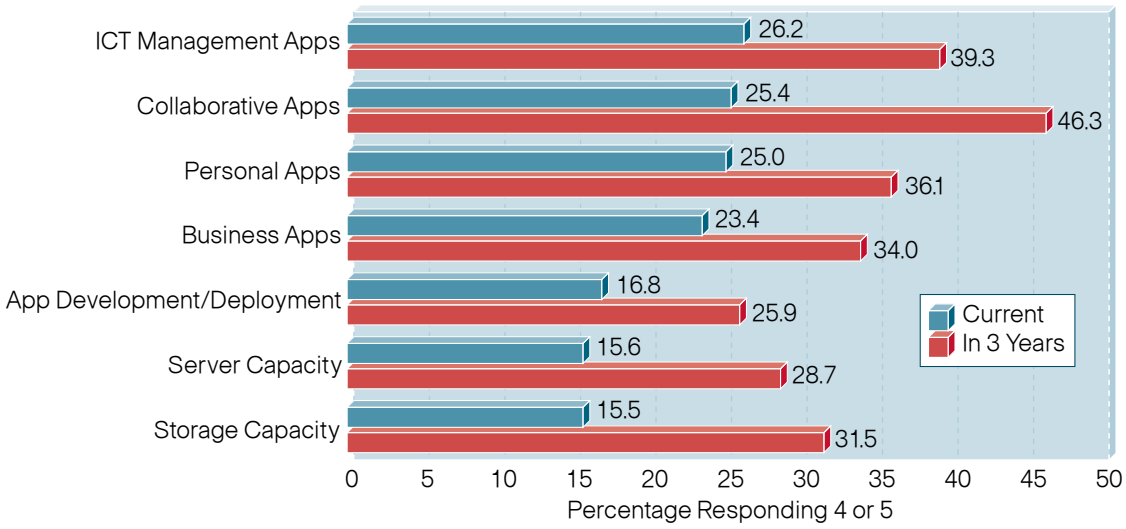
"... cloud computing heralds an evolution of business that is no less influential than ebusiness..."[8]

Benefits of Cloud Computing

Cloud computing can profoundly change the way organizations access and use ICT products and services. Instead of owning and managing ICT products and services, or using a "traditional" outsourcing approach built around dedicated hardware, software, and support services, organizations employing cloud computing services can meet their ICT requirements using a flexible, on-demand, and rapidly scalable model requiring neither ownership on their part, nor provision of dedicated resources by the cloud services provider. Both parties stand to benefit from the considerable economies of scale and scope that are possible under such an arrangement.

Cloud computing is being used or considered by many organizations, as demonstrated by an IDC survey[9] of current and future use of cloud services. Figure 4 shows the percentage of survey respondents whose organizations occupied the higher end (4 or 5) of the usage scale, or will be there in three years. It is worth noting that the three areas of strongest intentions are those in which organizations face major cost and management pressures (servers and storage) or have the most limited experience (collaborative applications).

Figure 4. Private Sector Intentions To Adopt Cloud Computing



Source: IDC Enterprise Panel, August 2008

8. http://www.gartner.com/it/page.jsp?id=707508
9. http://blogs.idc.com/ie/?p=205

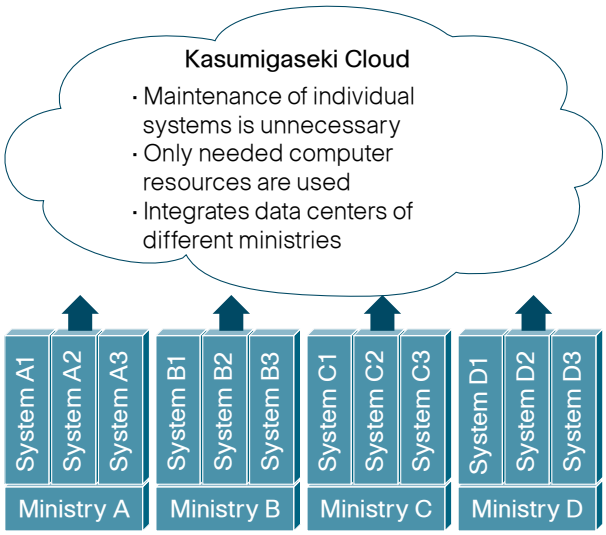
While businesses likely will adopt cloud computing more rapidly than the public sector, there are some notable early moves occurring in government. For example, in Australia, the New South Wales Department of Education and Training decided to use Gmail for 1.5 million students. In Canada, Ontario Centres of Excellence is involved in a pilot to deliver software development tools as a service to Canadian universities. In Washington D.C., all 38,000 city government employees have unlimited access to Google services and Gmail. This last example is particularly important, as it was initiated by Vivek Kundra, the former CTO of the District of Columbia who, in March 2009, was appointed CIO of the U.S. federal government. In this new role, he has already stated that he will push government to adopt cloud computing.[10] The U.S. General Services Administration recently announced that it moved the government-wide portal usa.gov to the cloud.[11]

Cloud computing is gaining momentum in other areas of government:

- The U.S. National Institute of Standards and Technology formed a new team focused on helping federal agencies determine how to proceed in this area, with a particular focus on standards—especially those that can help address security and privacy concerns.[12]
- The U.S. General Services Administration issued a request for information about IaaS offerings.[13]
- The Government of Japan's Ministry of Internal Affairs and Communications (MIC) announced plans to build an all-of-government cloud computing infrastructure as part of a wider "Digital Japan Creation Project."[14] To be built in stages from now until 2015, MIC intends that the new infrastructure (called the Kasumigaseki Cloud; see Figure 5) will consolidate all government ICT systems into a single cloud to improve operational efficiency and reduce costs.[15]

10. http://bits.blogs.nytimes.com/2009/03/05/the-nations-new-chief-information-officer-speaks/
11. http://techinsider.nextgov.com/2009/05/gsa_sends_usagov_to_the_cloud.php
12. http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf
13. https://www.fbo.gov/index?s=opportunity&mode=form&id=d208ac8b8687dd9c6921d2633603aedb&tab=core&_cview=0&cck=1&au=&ck=
14. http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Topics/pdf/090406_1.pdf
15. http://www.greentelecomlive.com/2009/05/13/japan-to-build-massive-cloud-infrastructure-for-e-government/

Figure 5. The Kasumigaseki Cloud



Source: Ministry of Internal Affairs and Communications, Japan, 2009

Cloud computing delivers major benefits to both private and public sector organizations, as detailed in Figure 6.

Figure 6. Significant Benefits of Cloud Computing

Benefit	Comment
Cost Savings	Organizations can reduce or eliminate ICT capital expenditures and decrease ongoing operating expenditures by paying only for the services they use and, potentially, by reducing or redeploying their ICT staffs.
Ease of Implementation	Without the need to purchase hardware, software licenses, or implementation services, an organization can deploy cloud computing rapidly.
Flexibility	Cloud computing offers more flexibility (often called "elasticity") in matching ICT resources to business functions than past computing methods. It can also increase staff mobility by enabling access to business information and applications from a wider range of locations and/or devices.
Scalability	Organizations using cloud computing need not scramble to secure additional, higher-caliber hardware and software when user loads increase, but can instead add and subtract capacity as the network load dictates.
Access to Top-End IT Capabilities	Particularly for smaller organizations, cloud computing can allow access to higher-caliber hardware, software, and ICT staff than they can attract and/or afford themselves.
Redeployment of IT Staff	By reducing or eliminating constant server updates and other computing issues, and by cutting expenditures of time and money on application development, organizations can focus ICT staff on higher-value tasks.
Focusing on Core Compentencies	Arguably, the ability to run data centers and to develop and manage software applications is not necessarily a core competency of most organizations. Cloud computing can make it much easier to reduce or shed these functions, allowing organizations to concentrate on critical issues such as (in government) the development of policy and the design and delivery of public services.
Sustainability	The poor energy efficiency of most data centers, due to substandard design or inefficient asset utilization, is now understood to be environmentally and economically unsustainable. Cloud service providers, by using economies of scale and their capacity to manage computing assets more efficiently, can consume far less energy and other resources than traditional data center operators.

Source: Cisco IBSG, 2009

It is important to note that the scale of such benefits, the ability to capture them, and the cost/benefit ratio achieved depend on many unique factors and will vary significantly. These include where an organization sits in its ICT capital expenditure and systems development cycle, its current hardware and software architecture (for example, many existing applications may not be "cloud-ready"), and its staff and management capabilities. In the public sector, legal and policy constraints will be especially important.

Benefit realization will also depend on the chosen cloud computing model. At this point in the evolution of cloud computing, two models are available: the "public cloud" model typified by the offerings of Google, Amazon, and Salesforce.com; and the "private cloud" approach, where organizations develop or procure their own dedicated cloud computing environments (either alone or in groups) rather than simply using the existing multi-tenant offerings of third-party providers. Discussions are starting about a hybrid option where an organization might use a public cloud for some functions (such as basic business applications or nonsensitive data processing) and a private cloud for others (for example, data storage). This is an important development, making it clear that the choice of a cloud model is not an all-or-nothing proposition. In the short to medium term, we believe that selection of a cloud computing model is one of the most important decisions public managers will face.

Cloud Computing and Shared Services: Key Public Sector Opportunities

The most significant cloud computing opportunities for the public sector may arise at the multi-agency or all-of-government levels. Around the world, public sector information management is clearly dominated by a "silo" model that sees most government organizations operating largely stand-alone information systems. One of the more intractable challenges faced by governments has been effective sharing of information technology resources. This is true in core e-government programs, and in areas such as public health/education and public safety/security.

Governments have invested enormous effort into tackling this challenge over the past decade. For example, they have developed coordination mechanisms such as enterprise architectures and interoperability frameworks. They have also enacted laws, policies, and budgetary frameworks geared toward shared services, and implemented a wide range of multi-agency ICT assets. Despite all this effort and cost, however, progress toward shared services has generally been slower and less widespread than many in government had hoped. As a result, governments pay too much for ICT and realize fewer benefits than they could—especially in regard to the performance of the public sector as a whole. Explanations for this poor progress may include:

- Lack of appropriate incentives and sanctions
- Inadequate design of funding and governance arrangements
- Difficulty harmonizing the ICT requirements of multiple organizations conducting disparate operations
- "Overprotection" of budgets and resources, excessive control of access to information, and erection of barriers to organizational change

While these are real challenges, it is also understandable that, when faced with imperatives to achieve discrete objectives within tight political, legal, and funding constraints, many government organizations have been reluctant to participate in shared ICT services initiatives.

In many cases, organizations have been rightly concerned about the implications shared services may have for costs, staffing, and their ability to flexibly and reliably meet business ICT needs. They have often found that government-wide enterprise architectures are too abstract and reductive to fit into their real-world operations, and that interoperability frameworks can be complex, restrictive, incomplete, and technologically outdated. They have seen that the costs of using shared services can often exceed those of self-provisioning, or that the projected savings are either not realized or inaccessible.

It is reasonable to anticipate that as cloud computing matures, and if it is used wisely, it may address many of the real or perceived barriers that have prevented widespread adoption of shared services in public sector information management. This is not to suggest that mechanisms such as enterprise architectures, interoperability frameworks, and the like will not be of ongoing importance. Rather, Cisco IBSG believes that the emerging cloud computing models and services may represent enterprise ICT finally reaching the point of maturity, sophistication, and flexibility needed to realize shared services objectives, resulting in more efficient and effective public sector information management.

In the longer term, due to its inherent flexibility and potential to reduce the rigid structural dependencies between government agencies and the ICT infrastructures underlying their data and services, cloud computing may play an important role in enabling the ongoing reform and transformation of the public sector in the 21st century. In a context of accelerating government adoption of Web 2.0 tools and business models that are increasingly linked to cloud computing as an underlying computing paradigm, cloud computing may also provide for greater conceptual coherence between ICT investment decisions and decisions about how best to organize the business of government. More pragmatically, it may also help the public sector cope with the explosion of network traffic and data storage requirements driven by Web 2.0.

Cloud Computing for Developing Countries and Regional / Local Governments

Cloud computing will deliver benefits beyond the public sectors of developed countries. Its advantages may be even more pronounced in developing countries that have not yet achieved high levels of public sector computerization, lack people with adequate ICT skills, or do not have firm legal or cultural requirements regarding data security and privacy. On the positive side, developing countries face less of the entrenched resistance to new computing paradigms that government agencies in developed countries often exhibit. Cloud computing may enable them to leapfrog a whole generation of government computing, bypassing many of the costly and debilitating challenges discussed above.

A similar logic applies at subnational levels of government in developed countries where many agencies are small enough to qualify as small and medium-sized businesses (SMBs). Given their generally greater financial and human resource constraints, these organizations may find the low capital and in-house skill requirements of cloud computing models particularly appealing.

Also, many regional or local governments work closely with SMBs as a major part of their economic development efforts. If cloud computing offers a way for these SMBs to be more efficient and effective, these governments should consider facilitating the use of cloud computing by SMBs to accelerate economic development.

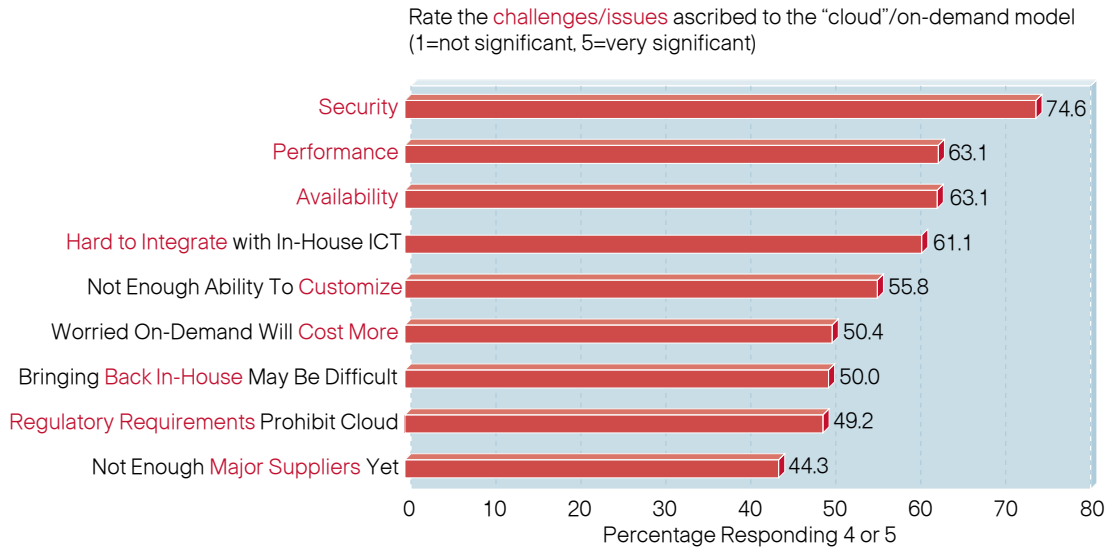
Challenges of Cloud Computing

Many challenges of cloud computing for the public sector relate to its apparent newness and the relative underdevelopment of the marketplace for cloud services. For government, decisions to adopt cloud computing will be driven by more than technical and cost considerations.

Information is the lifeblood of government, and decisions on how to manage that information can have far-reaching political, social, and economic considerations. Adoption of cloud computing presents many of the same risks and challenges as deciding to use a more traditional outsourcing arrangement. The increased possibility that the service provider may reside outside of a government's legal or territorial jurisdiction, however, can make some of these issues more acute.

A useful overview of some of the challenges businesses face in adopting cloud computing is provided in Figure 7. The public sector will confront the same range of challenges, though it may weight them differently. Some of these challenges will be unique to the government environment.

Figure 7. Cloud Computing Challenges



Source: IDC Enterprise Panel, August 2008

One area of challenge pertains to **open standards** and **interoperability**. As noted above, many governments have invested heavily in the development of enterprise architectures and/or interoperability frameworks. These are designed to reduce the risk of individual government organizations building ICT systems or managing information in ways that lead to duplication of ICT assets or an inability to flexibly combine information held by different agencies to support collaboration and user-centric service delivery. Many governments are also committed to using ICT systems that conform to so-called open industry standards to reduce the cost or performance risks that can occur when using nonstandard systems. Governments also want to make sure they avoid **vendor or technology lock-in**.

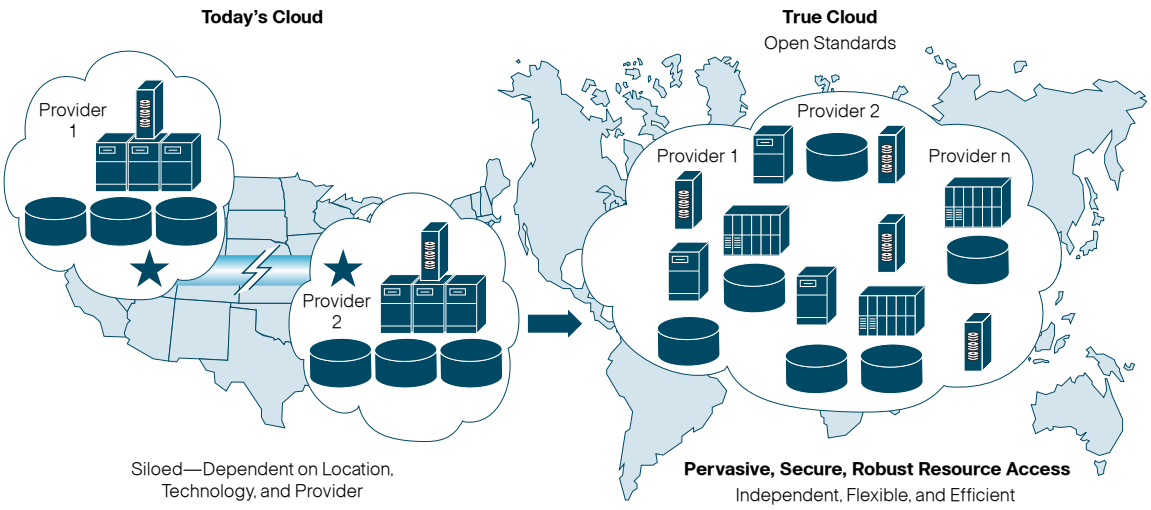
Open standards, interoperability, and the avoidance of lock-in continue to be important issues in a cloud computing environment. To date, cloud computing services have developed as largely proprietary offerings, and the overall market has not yet adopted standards that make it easy for different clouds to interoperate. Clearly, cloud interoperability standards will need to emerge as users of cloud services increasingly demand the flexibility and choice that standards enable. They will expect that their applications and/or data are easily portable among cloud environments, or can be moved back onto their own premises if required.

As shown in Figure 8, today's cloud environments resemble siloed enterprise ICT environments. We anticipate that there will be an evolution to what we call a "true cloud" environment, based firmly on open standards. This process is under way and, in March 2009, became controversial with the publication of "The Open Cloud Manifesto"[16] under the auspices of an informal coalition of many cloud services vendors. This document articulates a set of principles that its authors say should guide development of cloud computing in the future. This process will take some time, however, as not all of the major cloud vendors were part of the initiative—at least at that time.[17] In the meanwhile, if using a public cloud, public managers should consider issues they may face if they decide to exit the arrangement—especially if that cloud is built on proprietary platforms that inhibit easy switching to an alternative service. In the short term, developing private clouds involving multiple agencies may adequately address these concerns.

One unique set of cloud computing challenges governments may face potentially impacts their **sovereignty**. Special consideration must be given to using cloud computing to handle information that is vital to national security, to maintaining public trust and confidence in government, or to managing certain core government functions such as foreign relations, maintenance of property rights, law and order, and defense. Whether cloud services are provided on- or offshore, governments will need assurance that their sovereignty is not threatened—for example, through the possible overriding effect of laws in the jurisdiction where a cloud services provider stores data or applications.

16. http://www.opencloudmanifesto.org/
17. http://blogs.zdnet.com/BTL/?p=15341

Figure 8. Expected Evolution of Cloud Computing



Source: IDC Enterprise Panel, August 2008

This is more than a theoretical consideration. If information is held or processed in cloud environments that are legally and/or physically located offshore, governments will need to clearly understand how this may affect their ability to apply all relevant legal rights, restrictions, and sanctions that prevail in their own jurisdictions. Public managers should also think about challenges they might face in preserving the integrity or privacy of government information held offshore and in having it repatriated, if required, in instances of natural disaster, political instability, civil or industrial unrest, criminal activity, terrorism, or any instance of *force majeure*. Again, this risk can be minimized through the creation of a private cloud—particularly if that cloud resides in the government's own jurisdiction.

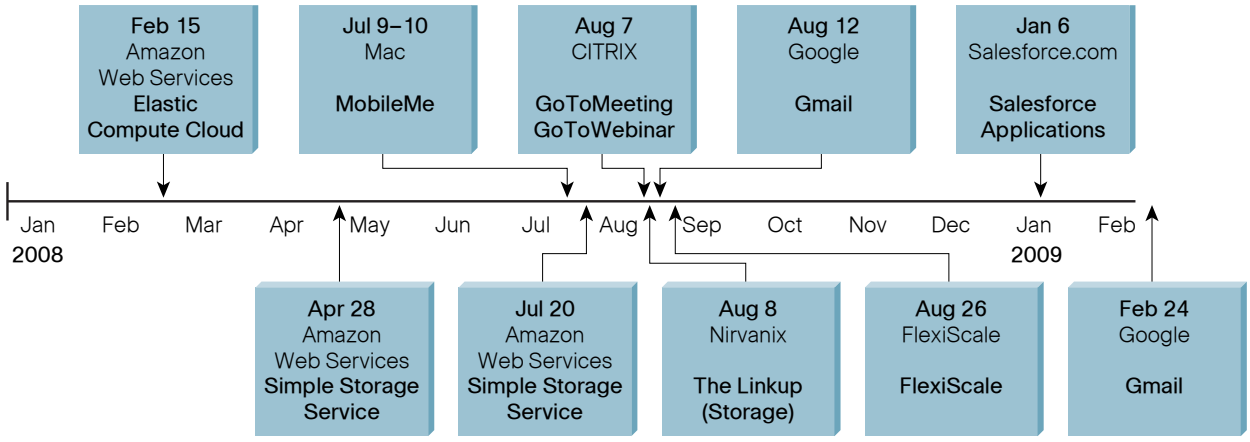
Security of information held in cloud computing environments will be another area of significant concern for governments. While, in principle, cloud computing is little different from more traditional outsourcing arrangements, public managers should assure themselves that the security surrounding cloud environments complies with laws, policies, and protocols. While there are strong arguments suggesting that cloud environments may actually be more secure than many enterprise ICT systems, one of the chief concerns will arise around the potential for a cloud environment to have multiple tenants. A government may not know or trust all of these tenants, or wish to share computing resources with them.

Closely related to security is the question of **privacy**. As with security, there is no real evidence that placing sensitive public information into a cloud environment, either on- or offshore, will risk breaches of privacy. Given the reduction of direct control over such information that cloud computing entails, however, public managers will need to thoroughly understand how privacy is assured in a cloud environment. In some cases, they may find that the operation of various national or international data protection laws and protocols prohibits them from using some cloud services. In this case, private clouds may again offer an alternative solution.

The public sector will also face a range of general **governance and management** challenges in adopting cloud computing. Again, these will be similar to the challenges of traditional ICT outsourcing. For example, there must be assurance that particular cloud computing arrangements comply with legal and policy constraints discussed above, and with others such as internal and external audit requirements. The possibility of greater geographical dispersion of computing resources and more limited in-house ability to manage relationships with service providers (at least temporarily) may make some of these challenges more acute. There may be increased performance monitoring costs or enforcement difficulties when rights must be asserted overseas and/or against offshore entities. As with other forms of outsourcing, one of the key ways of mitigating risks will be robust analysis and design of effective contractual arrangements that properly assure the nature, level, quality, and costs of services provided. As part of this, organizations will need to assure themselves that appropriate service-level agreements (SLAs) are in place, that they have adequate mechanisms and skills for assessing performance against those SLAs, and that they adopt effective means of addressing any non- or underperformance.

Another challenge will be assuring **business continuity**. Again, this challenge is more than theoretical, as the outages in 2008 and 2009 of Gmail[18] and a number of other cloud services demonstrate (see Figure 9). The public sector will need to understand the business continuity risks that this entails and be assured that effective remedies for those risks (such as strong contracts, effective SLAs, disaster recovery, and business continuity plans) are in place—especially if using offshore cloud services. Conversely, the public sector should also understand how cloud computing may mitigate some of these risks by, for example, providing access to more robust and better-managed computing platforms than most organizations can afford for themselves, or by enabling them to replicate data and/or business processes in the cloud, where they can be warehoused at minimal cost until needed.

Figure 9. Timeline of Major Cloud Service Outages



Source: "Envisioning the Cloud: The Next Computing Paradigm," J. Rayport and A. Heyward, 2009[19]

18. http://www.pcworld.com/article/160153/gmail_outage_marks_sixth_downtime_in_eight_months.html
19. http://www.marketspaceadvisory.com/cloud/

A final challenge in the public sector is that, as cloud services become increasingly easy for government organizations to adopt, clouds could present a further opportunity for organizations to defect from governments' shared services and cross-agency service integration efforts, thus jeopardizing the success of those programs. If this potential challenge does manifest, however, Cisco IBSG believes that public managers should examine it closely before concluding that it represents a strategic problem—it may instead indicate that cloud computing is ready to make a robust contribution toward achieving such goals.

What Should Public Managers Do About Cloud Computing?

In our view, public managers' interest in cloud computing is (or should be) essentially the same as for any other computing technology or architecture. At its simplest, cloud computing should be evaluated for its ability to enable government organizations to conduct business efficiently and effectively. At the multi-agency or all-of-government level, it should also be examined for its ability to enable achievement of e-government objectives and support increased public sector performance.

We are confident that as cloud services mature, they will offer significant flexibility, reliability, and cost-effectiveness benefits, although many hurdles must be overcome. It is important for public managers to gain a solid overview of how cloud computing is evolving, and the trends in its adoption. In the near term, Cisco IBSG expects rapid growth in third-party "public" clouds offering many different application, computing, and storage services. While public sector organizations may choose to use these services—especially, we suspect, for standard business applications such as email or document creation—we think it is more likely they will elect to create their own private clouds, either alone or in partnership with other agencies. Although public sector organizations will weigh the costs and benefits of each approach, we anticipate that a major driver of these decisions will be their level of trust in both the cloud model under consideration, and in the entity providing them. Figure 10 compares some of the key features of public, private, and hybrid clouds.[20]

We see these decisions being made in the context of three successive phases of cloud development and adoption in coming years:

- **Cloud 1.0:** Public and private clouds operating with no real interconnections
- **Cloud 2.0:** Hybrid environments in which public and private clouds work in conjunction in what might be called a "Cloud Network"
- **Cloud 3.0:** A rich cloud environment in which many external and internal clouds share workloads relatively seamlessly in what might be called "Intercloud" or "True Cloud" mode (see Figure 8)

20. A hybrid cloud computing environment is one in which an organization manages some resources in-house, but has other functions delivered via a cloud. For example, a government might choose to manage general computing in the cloud, but manages sensitive data on its private, secured servers.

Figure 10. Public Versus Private and Hybrid Cloud Computing Services

	Public Clouds	Private Clouds[21]	Hybrid Clouds
Characteristics	Often depicted as available to users from a third-party provider, "public" clouds are typically made available via the Internet and may be free or inexpensive to use. There are many examples, such as Amazon Web Services, providing services across open, public networks today.	Private clouds offer many of the same benefits as "public" clouds, but are managed within the organization. Private clouds are unburdened by network bandwidth and availability issues, or by potential security exposures that may be associated with public clouds.	Some ICT functions (for example, email, calendaring, document production, or business application runtime) may be handled in lower-cost public clouds. Other functions such as data storage or mission-critical business applications may be retained in-house.
Benefits	Commercial clouds in operation today provide best practices and examples for those considering cloud computing. **Key Benefit:** Tremendous elasticity and lowest cost.	Private clouds can offer the provider and user greater control, security, and resilience. **Key Benefit:** Gives users greater control than public clouds.	Hybrid clouds offer greater architectural flexibility. **Key Benefit:** Offers greater business choice and avoids all-or-nothing approach.
Risks	Potentially greater risks in terms of security, resiliency, transparency, and performance predictability (at least in the near term).	Potentially less risk—security, resiliency, infrastructure, and support processes will not differ significantly from current environment.	Risks and costs fall between public and private models.

Source: Cisco IBSG, 2009

There is no way of knowing how swiftly this process will unfold. It will be important for public managers—whether they are planning to adopt cloud computing now or waiting until it becomes mature—to constantly monitor the development of cloud computing and analyze how it might fit into their wider ICT plans and strategies.

There are several other important steps that can be taken now in preparation for cloud computing adoption:

- **Identify all potential opportunities** for switching from existing computing arrangements to cloud services. This should occur at both individual agency and all-of-government levels.
- **Ensure that in-house infrastructure complements cloud-based services**. The shift to cloud services isn't all-or-nothing, and some cloud services (for instance, infrastructure services) will support the ability of in-house ICT to extend into some clouds (for additional compute and storage capacity and so forth). **Virtualization** will be a key piece of a compatible infrastructure.
- **Develop a cost/benefit and risk evaluation framework** to support decisions about where, when, and how cloud services can be adopted.

21. For an excellent example of a private cloud in a public sector application, see http://www.cisco.com/webabout/ac79/docs/pov/Trust_Clouds_0115a_PrintedBooklet.pdf

- **Develop a roadmap** for optimizing the current ICT environment for adoption of public and/or private cloud services.
- **Identify which data cannot be held in public cloud** computing environments for legal and/or risk-mitigation reasons.
- **Identify and secure in-house competencies** that will be required to manage effective adoption of cloud services.
- **Designate a cross-functional team** to continually monitor which new services, providers, and standards are in this space, and to determine if they affect the roadmap.
- **Evaluate technical challenges** that must be addressed when moving any current information or applications into a cloud environment. Experiment with and pilot various services—both internal and external—to identify where issues will arise.
- **Ensure that the networking environment is ready** for cloud computing.

This last point is particularly important. We see cloud computing as a natural evolution of the Internet. Rather than regarding networks as mere plumbing, it is vital for public managers to understand them as the fabric "within" the cloud, and as the connection between the cloud and the user. In the future, networks will also be the fabric that connects and mediates between different types of clouds. The network must be a key part of providing security and quality of service at scale. It's not a matter of simply choosing either the endpoints or the network for a particular function.

Some industry participants believe that the majority of the intelligence that enables cloud computing should be driven by "endpoints" (clients, servers on the network, and so forth) rather than by the network itself. Each has an important role to play in providing enterprise-class cloud computing that is flexible and scalable. We believe there are numerous functions that should naturally be part of the network, just as router and firewall software originally ran on servers and clients but eventually migrated to the network. The driver here will be the vast proliferation of types of clients and servers (not to mention mobility). Because the network is the constant, not the endpoints, the intelligence driving these services is a network discipline.

For more information about cloud computing in the public sector, please contact:

Carolyn Purcell, Director
Public Sector Practice, Cisco Internet Business Solutions Group
Phone: +1 512 917 7448
Email: purcellc@cisco.com

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps CXOs and public sector leaders transform their organizations—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that address key CXO concerns.

For further information about IBSG, visit http://www.cisco.com/go/ibsg

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

KK/LW15967 1109