Cloud Computing Concerns in the Public Sector

How Government, Education, and Healthcare Organizations Are Assessing and Overcoming Barriers to Cloud Deployments

White Paper

Authors
Fernando Macias, Solutions Architect, Cisco Global Government and Security
Greg Thomas, Senior Manager, Cisco Global Government and Security
What You Will Learn

Public sector organizations have much to gain by taking a cloud computing approach to service delivery in their information and communications technology (ICT) environments. But they must have confidence that the benefits can be achieved without compromising core requirements and institutional values.

This paper briefly examines issues that often present barriers to public sector cloud implementation. In particular, it focuses on reliability and resilience, privacy and security, and standards and development. We’ll discuss how hybrid clouds are helping to overcome many objections to cloud deployment. We’ll also touch on financing models that are making cloud computing more affordable.

Common Cloud Computing Concerns

Cloud computing is a recent stage in the ICT evolution of the last several decades. Many of the advances in ICT service delivery have been the result of networking innovations. Initially, the new breakthroughs were disruptive. But in each case, the uncertainty, doubts, and technological barriers were eventually overcome.

So it is with cloud computing. Government, education, and healthcare organizations are embracing clouds as a way to increase their operational efficiency and productivity, while at the same time maximizing investments and lowering costs. Cloud computing offers these public sector entities the opportunity to be more agile and innovative by consolidating, virtualizing, and automating their ICT resources. (For a more detailed discussion of cloud computing benefits, see the Cisco® white paper Cloud Computing Advantages in the Public Sector.)

Several issues may arise when public sector organizations consider transitioning to cloud computing. Here are some prominent concerns:

- **Control:** Managers naturally want to determine how and where elements of the ICT system are deployed and used. Cloud computing raises questions of ownership and accountability within ICT groups, across the organization, and extending to service providers and other vendors.

- **Security:** Organizations must keep systems safe from intrusions, and they need to safeguard information, privacy, and, in the case of research institutions and universities, intellectual property.

- **Reliability:** An ICT group must be able to trust in the reliability and resilience of its cloud implementation, especially when it supports mission-critical applications.

- **Quality:** CIOs are concerned that consistency and quality should not be compromised and that service-level agreements (SLAs) can be maintained.

- **Ownership:** When ICT is arranged in a new way, there are questions about who should manage which resources and who should pay for services that are shared. Data governance becomes an issue in cloud deployments when data is stored in locations outside institutional and territorial boundaries.

- **Interoperability:** A traditional reliance on separate system infrastructures makes cloud technology an unfamiliar option in the public sphere. At the same time, the cloud model must be integrated with legacy solutions.

- **Portability:** Adopting a cloud approach should not lock the organization into applications, equipment, or services from a narrow spectrum of vendors and providers.

- **Standards:** Because cloud technology is relatively new, industry standards and best practices are still being developed.

- **Vendors:** Competing platforms and proprietary approaches complicate the cloud marketplace. In addition, there is a perception among some CIOs that cloud-oriented vendors still do not fully understand the needs of public sector organizations.

- **Governance:** The ICT group must decide what new organizational approaches are needed, including the need to focus more on integrating services and supporting interactions among business groups.

- **Culture:** Public sector organizations may resist approaches that make it appear that they are giving up or privatizing their resources. Cloud-related innovations may also stir institutional opposition among those who resist change or fear that well-established procedures could be compromised.

- **Compliance:** Organizations must be sure they can comply with all relevant government regulations. Examples include regulations pertaining to privacy, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the European Data Privacy Directive; accountability laws, such the U.S. Sarbanes–Oxley Act; and legislation concerned with security, such as the U.S. Federal Information Security Management Act (FISMA).

- **Risk:** Assessment of risks needs to include anticipating a course of action if a cloud service provider fails to deliver services or goes out of business.
Many of these concerns have to be addressed by public sector ICT groups based on their organizations’ own individual missions, structures, and needs. However, the following concerns are particularly pressing, and they are common to nearly every organization contemplating a cloud implementation.

**Learning to Trust Cloud Technology**

Public sector ICT strategists are placing their trust in cloud computing by:

- Realizing that the cloud model is really just the latest in a series of ICT innovations that have extended and improved upon previous models
- Learning from the experiences of the public sector organizations that have already planned and implemented a cloud approach
- Studying and evaluating all the implications of moving to a cloud environment
- Choosing a cloud model that best fits the organization’s business and risk tolerance
- Partnering with trusted vendors who have a successful track record in helping customers deploy cloud technology and deal with technological transitions

**Reliability and Resilience**

In April and May of 2011, some well-publicized outages called the reliability and availability of public clouds into question:

- Serious technical difficulties struck Amazon Web Services (AWS), affecting a public cloud that serves thousands of businesses. Reported problems included the inability to access data, as well as service interruptions and website shutdowns. AWS offers customers the option of spreading applications across multiple “availability zones” to protect against failures, but this did not prevent problems for some customers. (Amazon’s SLA provides 99.95 percent availability during a service year for each region, but not for each availability zone within a region.)
- Google’s Blogger blogging service and Microsoft’s BPOS Exchange service both experienced significant outages that inconvenienced users, and in the case of Exchange, embarrassed ICT managers whose organizations count on reliable email communications.

- A new VMware public platform-as-a-service (PaaS) offering for web developers called Cloud Foundry suffered sporadic downtime over two days due to a power outage and subsequent remedial activities.

Obviously, no ICT implementation is 100-percent problem free. But are these particular problems causing CIOs and other stakeholders to rethink the wisdom and efficacy of a cloud implementation? To some extent, yes. However, instead of questioning the basic premise underlying cloud computing, most ICT professionals regard such incidents as lessons in how best to implement cloud computing.

The best strategy for overcoming misgivings about a cloud services model is to design an infrastructure that ensures reliability and resilience. Many public sector organizations are questioning the reliability of public-only cloud infrastructures. Of course, there is the option to increase robustness by using multiple public-cloud vendors to provide redundancy. But applications that cross disparate public clouds raise interoperability issues and can add the sort of complexity that ICT organizations are trying to avoid in the first place.

As a consequence, organizations are turning to private and hybrid cloud deployments to mitigate risk and still satisfy their business requirements. These infrastructures give CIOs more control in terms of both design and operation. (For more information, see the section “Infrastructure for Hybrid and Community Clouds.”)[[waiting for the link for this item]]

A recent Norwich University survey (April 2011) of nearly 650 ICT professionals in municipal, state, and federal agencies and higher-education institutions in the United States found that 36.1 percent of respondents believe that a hybrid cloud model will best meet their needs in five years, while 28.2 percent anticipate moving to a private cloud and 16.2 percent favor a community cloud. Federal employees are more likely than state or local employees to favor private-only implementations. Only 7.3 percent of the respondents think that a public cloud will work best for them. (The remaining 12.2 percent don’t foresee a cloud implementation or don’t know.)

Because cloud deployments are well suited for distributing operations to multiple locations, cloud service providers will likely offer more sophisticated business-continuity and disaster-recovery services in the future. However, many public sector organizations with their own private clouds, and those that host cloud services for other agencies or business groups, will want to take the initiative by implementing an infrastructure specifically designed to reliably support a virtualized, multitenant computing environment and cloud-driven network traffic loads.
Building a high-availability cloud infrastructure does not have to be a laborious, costly proposition. Most ICT groups can use their existing infrastructure, which is likely to be underused at present. Transitioning to a cloud environment may be more about new thinking than it is about new technology.

Case Study: Municipal Government in the Paris Suburbs

Communauté de Communes de l’Aéroport du Bourget, three municipal governments in the Paris suburbs, decided to virtualize their 27 physical servers. It worked so well that they went on to virtualize 1000 desktops. Storage requirements are kept to a minimum with a linked clone deployment that stores only the changes that users make to the basic desktop template. “Our 6-terabyte SAN is easily big enough for our needs,” says David Larose, head of the IT infrastructure group. “Before the linked cloud technology, I would have needed much more.” For more information, download the case study.

Privacy and Security

Keeping data secure and personal information private is critical for any ICT implementation today, but particularly for those that serve large numbers of citizens.

As ICT systems are extended and merged, there is growing fear that sensitive data that is collected and held by public entities will be vulnerable to criminal hackers or other types of unauthorized disclosure. This threat is magnified when a piece of crucial identity information, such as a social security number, can be linked to other information about that individual residing on the network, such as a financial or health record.

A security breach is inconvenient for individual users, but it can be a catastrophe for an organization whose reputation, credibility, and legal standing is at stake. Public sector organizations are especially vulnerable because their operations are tied so closely to the public’s trust. When the relationship between organization and citizen is damaged, it is very difficult to repair. And lawsuits arising from assaults on privacy not only taint public perceptions, but can also deplete public funds.

The legal definition of “personal data” can be much broader in some countries and jurisdictions than in others, making it difficult for international providers to obey what amounts to a patchwork of inconsistent statutes. Because the data centers that support clouds may be located anywhere, the technology has run into obstacles in regions with strict regulations concerning information that is transmitted across borders.

For example, rigid limits have been placed on the movement of information beyond the borders of the 27-country European Union (EU). Companies that want to process data in unapproved countries must negotiate and enter into binding legal agreements to ensure that the personal information of EU citizens will be handled in accordance with regulations. Privacy concerns and a complicated legal landscape in Europe have hampered the implementation of cloud-based computing in both the public and private sectors. Companies with a stake in cloud computing, including Cisco, are working with European political leaders and regulators to streamline the continent’s fragmented data protection laws and reform the statutes to reflect recent technological developments.

The situation is similar in some other regions. An Australian commissioner has instructed state government organizations to use only those cloud service providers that agree to comply with the state of Victoria’s information privacy laws. Locally based data centers are preferred. By the same token,
the New Zealand government issued a revenue alert in 2010 stating that any organization in that country wanting to utilize cloud computing must either use cloud services that have data centers located within the country, or they must keep local copies of all records.

In the United States, the Federal CIO Council has issued guidelines for maintaining privacy when a government agency employs cloud computing. The document states: “Federal agencies need to be aware of the significant privacy concerns associated with the cloud computing environment where personally identifiable information will be stored on a server that is not owned or controlled by the Federal government.” The guidelines also note that “privacy and security risks are magnified when the [cloud provider] has reserved the right to change its terms and policies at will, which is a common provision in some terms of service.” The CIO Council calls for agencies to conduct a privacy impact assessment before deploying a cloud solution.

A Frost & Sullivan report (May 2011) based on a survey of organizations in the Asia Pacific region found that government concerns about the security and location of data centers have led these organizations to adopt private and hybrid clouds to a greater extent than public clouds. In countries like India and China, where cyber protection for individuals is relatively weak, some people are leery of trusting their personal data to any institution that keeps information in a cloud.

However, public sector ICT professionals should bear in mind that maintaining privacy in clouds that cross jurisdictional borders is not unlike taking similar measures in an outsourcing environment. For example, financial call centers and organizations that outsource healthcare insurance claims generally make privacy an essential part of the contractual obligations that they impose on their vendors. These contracting organizations often limit or curtail secondary outsourcing because the legal obligations may not carry over to subcontractors hired by the primary vendors. Taking care to oversee and monitor the data’s “chain of custody” within cloud environments may be one way to prevent confidentiality breeches and to limit liability.

Civilian and military organizations involved in national security need to maintain strict control over sensitive data, and must also retain the ability to delete or destroy the data when required. There is also the matter of physically securing storage devices. However, in addition to decentralizing operations, cloud models can also distribute risk. So, for instance, several agencies with similar security requirements might share a community cloud that implements extremely stringent protections, giving them the advantages of cloud-based data portability without exposing them to additional risks.

As the technology matures and regulatory standardization proceeds, privacy and security concerns about cloud computing should eventually subside. In the meantime, public sector CIOs can make the case that information residing in a private or hybrid cloud is generally as safe as it is in a conventional data center.

Standards and Development

Standards are critical to making sure cloud computing technologies can interoperate with each other and with legacy systems. For example, an organization that is running an application on an internal cloud or a provider’s cloud should be able to transition to another cloud infrastructure without having to rewrite the application. The industry is working to provide open-source software for cloud-based computing, and to develop standards and interfaces for the interoperability of various types of software that support cloud computing.

Several groups are involved in cloud standards and development efforts:

- The Open Cloud Manifesto has established a core set of principles to help ensure that organizations will enjoy freedom of choice, flexibility, and openness as they take advantage of cloud computing. More than 400 supporters are listed on the Open Cloud Manifesto website.
- The Open Cloud Consortium is managed by the Center for Computational Science Research, Inc., a corporation in Illinois that has applied for not-for-profit status. It manages cloud computing infrastructure such as the Open Science Data Cloud to support scientific research, and cloud computing test beds such as the Open Cloud Testbed. It also develops reference implementations, benchmarks, and standards, and sponsors workshops and other events related to cloud computing.
- The Distributed Management Task Force (DMTF) spans the ICT industry with 160 member companies and organizations, including Cisco, and more than 4000 active participants in 43 countries. DMTF’s Cloud Management Working Group is developing a set of standards to improve cloud management interoperability between service providers and their customers, including public entities.
- OpenStack is a global collaboration of developers and cloud computing technologists that focuses on an open-source cloud computing platform (infrastructure as a service [IaaS]) for public and private clouds. The technology consists of a series of interrelated projects
delivering various components for a cloud infrastructure solution. All the code for OpenStack is freely available under the Apache License, and anyone can run it, build on it, or submit changes back to the project.

• In the United States, the National Institute of Standards and Technology (NIST) is leading the development of cloud computing standards for the government, including high-priority security, interoperability, and portability requirements. Under the auspices of the Federal CIO Council, NIST is defining a consistent technical process that can be used by the Federal Risk and Authorization Management Program (FedRAMP) to assess the security posture of specific cloud service implementations. In addition, the Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) is facilitating the development of cloud computing standards, with the aim of increasing confidence in government cloud adoption.

• In Europe, the Standards and Interoperability for e-Infrastructure Implementation Initiative (SIENA) is working to break down the interoperability barriers that impede implementation of clouds by coordinating among various national and pan-European initiatives, policy bodies, and enterprises. The group will also define scenarios, identify trends, investigate innovation, and assess the impacts of cloud and grid computing.

A new cloud model called network as a service (NaaS), which is now under discussion, would empower the service provider to deliver virtualized networking components such as firewalls, load balancers, and wide-area acceleration services, as well as monitoring and management resources and future capabilities such as SLA management. As proposed, NaaS would give OpenStack developers the capability to create and manage virtual networks using simple APIs.

Case Study: District Police Force in England

Gloucestershire Constabulary, a police force covering six districts across southwestern England, currently faces tight budget constraints and has had to restructure to increase efficiency and lower costs. A new cloud computing approach to ICT enables higher levels of automation and integration. Through virtualization, the organization was able to consolidate the number of servers from 200 physical machines to just two chassis. The constabulary was also able to lower power requirements by implanting smart meter technology, and to reduce file server requirements by centralizing storage and domain access to a small number of sites. For more information, download the press release.

Infrastructure for Hybrid and Community Clouds

Instead of choosing between public and private clouds, many public sector organizations are combining the two. That way, ICT groups can use the cloud infrastructure to extend the boundaries of internal resources and take advantage of new public service offerings without giving up central control of services and security.

Furthermore, a hybrid infrastructure allows the ICT group to establish a community cloud by making services available to other agencies or related organizations, rather than transferring that role to outside vendors. If an institution has developed software and would like to share it with kindred organizations, they can create a template in the cloud and allow others to use it. A community cloud can also become a profit center if the hosting organization charges for the services.

By using a hybrid strategy that integrates with existing ICT management technologies, organizations can avoid the “lonesome cloud” syndrome—that is, a cloud implementation that is cut off from the rest of the organization’s critical systems. A comprehensive plan for unifying cloud services should be in place before cloud implementations multiply to the point where the services become fragmented and redundant.

Operational Advantages of Hybrid Models

• **Workloads:** Applications and virtual machines can port between clouds in response to changing business conditions.

• **Performance:** Compute, memory, and storage resources may be dedicated to the organization’s specific needs, on shared or physically separated hardware.

• **Management:** A single dashboard can monitor the infrastructure, applications, operations, and processes.

• **Security:** Sensitive information can be protected by being located within the private cloud.
Organizations considering a hybrid cloud approach that do not already support an internal cloud environment will need to develop a virtualization strategy that includes servers, applications, storage, and network connections. Such an implementation moves functions closer together and integrates them into a fabric linked by high-speed interconnects. It requires a high level of governance and security, with the intelligence to handle diverse applications and the flexibility to adapt to new and changing demands.

Because cloud computing is really an operations model rather than a particular type of technology, applications do not encounter a “cloud layer” in the application execution stack. The only cloud-specific technology in the data center is in the management and security systems that provision, monitor, and otherwise operate the underlying compute, network, and storage infrastructure. The execution stack is thus able to remain consistent at various scales, provided that the infrastructure allows for sufficient interoperability and portability. Interoperability enables management of compute and storage images, instances, and network policy, while portability takes in both compute images and network policies.

Innovative Financing Models

CIOs in today’s public sector organizations are moving to align their policy, finance, and technology initiatives to achieve better overall results. Cloud computing has the potential to provide a positive return on ICT investment for organizations that need to respond proactively to the current budgetary environment.

Here are some ways that public sector ICT groups can modernize and economize at the same time:

- **Become a shared-service provider:** In this model, the organization helps defray costs by providing cloud services to other agencies or organizations. In other words, the cloud acts as a revenue center. Organizations also have the option of becoming brokers or resellers of the cloud services that they contract for.

- **Shift capital costs to operating expenses:** Paying for a major ICT upgrade upfront can be difficult when immediate funds are lacking, which is often the case when the technology cycle is not in sync with the budget cycle. By taking advantage of a shared infrastructure, ICT can spread out capital expenditures without turning to leasing or borrowing. Total cost can actually go down.

- **Finance the entire project:** Many public sector organizations are looking to public–private partnerships to help finance vendor services and hard-asset purchases. By financing an entire project, the organization can ensure that costs are tied to milestones and all facets of the project are covered, including installation activities.

- **Defer payments:** Future debt obligations may be justified if the project will save costs going forward and the implementation promises to offset financing charges. This approach would also be a good choice for organizations that need to meet critical deadlines.

- **Use tax exemptions:** In the U.S., the interest on bonds issued by state and local governments is generally exempt from federal income taxes, resulting in favorable financing arrangements and lowering the cost of borrowing. However, deferred costs will usually need to be paid in future appropriations periods. A nonappropriations clause relieves the government of the burden of payment if sufficient funds are not appropriated in the future.

- **Optimize end-of-year budget:** If budget dollars remain at the end of the year, this can be a good time to launch a modernization project, significantly reducing interest or other finance costs.

Conclusion

Cloud computing is the next step in ICT evolution, representing a transformative leap forward for today’s public sector networking and data centers. Despite some misgivings, public sector CIOs worldwide are placing their trust in cloud technologies. They are now thinking less in terms of silos and discrete data center functions, and more in terms of virtualization and integration.

By choosing their cloud models wisely and aligning them closely with their organization’s business model, ICT decision makers can deploy an effective, economical solution while also successfully addressing reliability, data management, and security issues. Regulatory issues that now stand as barriers to cloud implementation in some regions are in the process of being resolved. Standards continue to be developed that will make it easier for ICT groups to adopt cloud technologies and make sure they interoperate with both new and legacy resources.
For More Information

To find out more about cloud computing and how Cisco helps public sector organizations find their cloud advantage, visit:

- www.cisco.com/go/govcloud
- www.cisco.com/go/education
- www.cisco.com/go/healthcare