



# Cloud Computing

Full strategic report at:

[www.FCW.com/CloudComputingSnap](http://www.FCW.com/CloudComputingSnap)



## Inside:

Government Takes Lead in Cloud Adoption, s2

The Cloud's Standards Imperative, s5

Cloud Security Concerns, Best Practices, s7

Understanding Cloud Formations, s9

Town Halls and Other Online Constituent Services, s11

# Government Takes Lead in Cloud Adoption

In an unlikely role reversal, speakers at the recent Cloud Computing Summit in Washington D.C., agreed the public sector has taken an obvious lead in the adoption of cloud computing, stepping ahead of private sector organizations by embracing pay-per-use solutions for a variety of new services and applications.

Even though the majority of publicly acknowledged government cloud computing investments are still in early phases of implementation, industry suppliers, observers and government officials all said the promise of lowered costs and greater efficiencies has accelerated the pace of adoption despite obvious security, legacy systems integration and governance challenges.

The pay-as-you-go benefits are so compelling, the 2010 federal budget submitted to Congress expanded the use of cloud computing, and included a reduction in the number and cost of federal data centers. The White House advises agencies to launch cloud computing pilot tests for applications ranging from communications and remote access, to virtual data centers, analytics/reporting, web portals, collaboration as well as records and case management.

Industry observers cite the Open Government Directive and the apps.gov website as a prime cloud-based example. NASA, meanwhile, has launched Nebula, a home-grown cloud computing environment that allows outside scientists to contribute. DISA has the RACE program, which is being used to test cloud services. The National Highway Traffic Safety Administration (NHTSA) ran its highly publicized 'Cash for Clunkers' program on a cloud computing service. The City of Los Angeles outsourced e-mail to a cloud-based solution. Michigan opted for a storage-as-a-service solution.

And as a shared services provider, the Department of Interior's National Business Center (NBC) is busy rolling out cloud-based offerings for federal agencies. "The feds should be proud of the work they've done so far," said Jon Oltsik, a senior principal analyst for Milford, Mass.-based ESG. "Great leading-edge cloud implementations exist in government today, while many in the private sector still [seemingly] aren't getting the message."

Cloud computing "presents a new business opportunity, an understanding that we can take the knowledge housed inside government organizations and present that in a cloud-run service," said Susan Camarena, chief knowledge officer for the Transportation Department's Federal Transit Administration (FTA).

Driving an unusually speedy migration is the government's underlying budgetary constraints, as well as a desire to achieve greater flexibility, efficiency and support for new applications and users, who increasingly expect high-speed availability and greater functionality. In research conducted by Enterprise Strategy Group, Inc., only 13 percent of 700 users surveyed believe current IT personnel aren't capable of servicing the organization's needs. "Behind this statistic is the realization that cloud computing investments aren't technology-based, but absolutely business-driven decisions," said NBC's Oltsik.

Cloud computing also is attractive because it supports all users, no matter where they are located. Such services minimize inefficient infrastructure, while boosting initiatives such as Green IT, disaster recovery/COOP (continuity of operations) and Telework. The U.S. Marine Corps' virtualization initiative, started in 2007, was driven by requirements for greater security, availability and recoverability, said Chip Brodhun, senior technologist/project director of emerging technologies for the USMC.

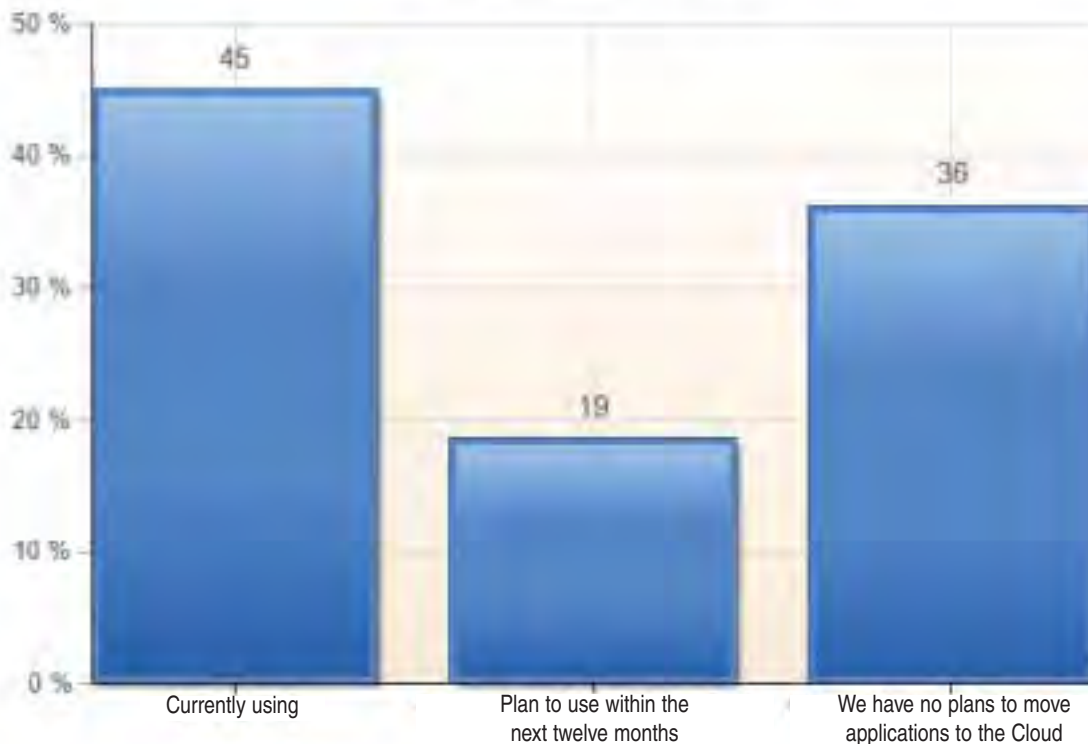
For instance, Brodhun said, "the COOP plan for Hurricane Katrina consisted of removable media, packed into rucksacks for a 17-hour truck ride to Kansas City." Now, after moving to a cloud-based disaster recovery service, "the Marines can be back up and running from almost any location, in just one to three hours," he explained.

Meanwhile, the Los Alamos National Laboratory's campus simply ran out of space for additional servers and had no further available power capacity, which drove the migration to virtualization, and then a cloud-based service now used to gather and report on energy consumption/savings, said Anil Karmel, a Solutions Architect for Los Alamos National Laboratory. In total, minus the power consumed by supercomputing operations, Los Alamos has realized a 25 percent reduction in power consumption, he explained.

Peter Mell, a senior computer scientist for the National Institute of Standards and Technology (NIST) and co-chair of the Cloud Computing Advisory Council, explained how high costs and hefty power consumption in traditional computing environments underscore the need to investigate cloud-based services. "Currently, \$800 billion is spent annually on the purchase and maintenance of enterprise software, and 11.8 million servers run at only 15-20-percent capacity in data centers," he said. "Meanwhile, the number of servers doubled



Is your organization currently using or do you plan to use the Cloud (hosted services across the Internet) for government applications within the next twelve months?



Source: Public Technology Institute

between 2001 and 2006, while power consumption per server actually quadrupled during the same period.”

As a result, market researchers predict public sector investment in cloud computing is likely to more than double in the next five years. According to research from INPUT in Reston, Va., as the federal government modernizes IT infrastructures, agencies are investing in cloud computing as a viable alternative to buying and maintaining additional servers and software. Also, agencies don’t want to pay more than other organizations for the same commodity products and services. The groundswell from early adopters, combined with momentum created by senior officials promoting the cloud is helping drive the cloud’s 27 percent compound annual growth rate, according to INPUT’s research.

**Obstacles Ahead**

While the migration to cloud computing seems inevitable, security and privacy concerns are still seen as prominent obstacles. Doubts remain that externally controlled cloud services can be adequately protected and federal agencies must carefully scrutinize industry offerings to ensure adequate security. “Each investment in a cloud-based solution requires proper due diligence,” Oltsik said.

The security required is daunting. The Treasury Department

was forced earlier this month to take down four public web sites for the Bureau of Engraving and Printing (BEP) after the discovery of malicious code on a cloud host site. The bureau began using a third-party cloud service provider to host the sites last year, according to a prepared statement. “The hosting company used by BEP had an intrusion and as a result of that intrusion, numerous websites (BEP and non-BEP) were affected.”

Meanwhile, the non-profit Cloud Security Alliance published a report on the biggest cloud computing security threats, based on information from security experts at 30 organizations involved in complex cloud environments.

Top threats include:

- Malicious employees of cloud computing providers;
- Nefarious use – attackers who target cloud providers;
- Insecure interfaces and APIs;
- Shared technology vulnerabilities;
- Data loss or leakage;
- Account, service or traffic hijacking; and
- Unknown risks.

According to Oltsik, security, legacy systems integration and governance especially related to contracting and service level agreements remain nagging concerns. “Standards would help,” Oltsik said, as industry suppliers “would be

able to better respond if federal agencies worked together to define clear standards to delineate what and how services must be delivered.”

Early adopters said potential cloud customers must keep security, lifecycle management, chargeback, SLA and training issues uppermost in their minds as they negotiate cloud implementations. “It’s especially important to remember that there’s a much higher price tag associated with tier one systems that require 99.999 percent availability,” said Karmel from the Los Alamos Labs. He recommended a close inspection of current systems and applications destined for cloud deployments to ensure the applications that will function well at a tier two (90 percent uptime) are set to this level to avoid unnecessary expense in service level agreements.





USMC’s Brodhun said until data and users can be easily moved into and out of cloud environments, it’s unlikely the Marines will invest in public cloud solutions, which are still widely perceived to be too high risk. Another challenge Brodhun mentioned is training, which requires additional investment in personnel and engineering resources, he said.

For now, it seems obstacles from security to privacy, reliability, standards, regulatory or legislative hurdles have

all been “outweighed by the government’s overwhelming desire to reduce complexity and isolation and improve the sharing of information, applications, data and users,” said Javier Vasquez, director of Collaboration & Cloud at Microsoft Federal. In the coming months, Vasquez said federal customers should look forward to a FISMA-certified solution from Microsoft that has been designed to address at least some federal IT security concerns and further smooth the transition to cloud-based environments.

As complexity and risks have grown, federal IT security mandates – especially the Federal Information Security Management Act (FISMA) – have remained largely focused on testing, evaluation and the accreditation of security solutions. This has created a situation in which federal organizations spent time and effort on filing paperwork and providing documentation for compliance, without gaining much in terms of security benefits. FISMA currently is being modified to focus more closely on continuous monitoring and measurement. “Once we achieve certification, we expect to see an uptick in interest among customers of cloud offerings,” said Vasquez, “as so much of the government’s business is predicated on FISMA accreditation.” ▼

### A Shift to the Cloud

OPPORTUNITY	CLOUD SOLUTION	
	<p>Support doctors and healthcare providers in implementation of Electronic Health Records (EHR)</p>	<ul style="list-style-type: none"> <li>▪ Nationwide solution for 2,000 users in 6 weeks</li> <li>▪ Track and coordinate EHR implementations</li> </ul>
	<p>Consolidate more than 12 email systems serving 80,000 users</p>	<ul style="list-style-type: none"> <li>▪ Moving 80,000 mailboxes to the cloud</li> <li>▪ 66% expected cost savings</li> </ul>
	<p>Modernize enterprise data centers</p>	<ul style="list-style-type: none"> <li>▪ Halted procurement of up to \$1.5 billion in data center efforts</li> <li>▪ Reevaluating enterprise strategy in context of “Cloud First”</li> </ul>
	<p>Provide scientists and researchers on-demand access to raw data storage and computing resources</p>	<ul style="list-style-type: none"> <li>▪ \$32 million investment</li> </ul>

Source: Economic Gains of Cloud Computing Presentation, Federal CIO Vivek Kundra

# The Cloud's Standards Imperative

A general lack of government-wide standards – especially related to establishing common security practices for cloud computing – has hindered broader federal adoption, sources said at the May Cloud Computing Summit in Washington D.C.

Sharing information and trying to standardize anything across the various military branch services is still limited, according to Chip Brodhun, Senior Technologist/Project Director of Emerging Technologies for the U.S. Marine Corps (USMC). “With each military branch in a separate stage of implementation, while there has been greater collaboration and note sharing, there’s not much agreement or standardization yet,” as each unit considers its use case unique, he explained.

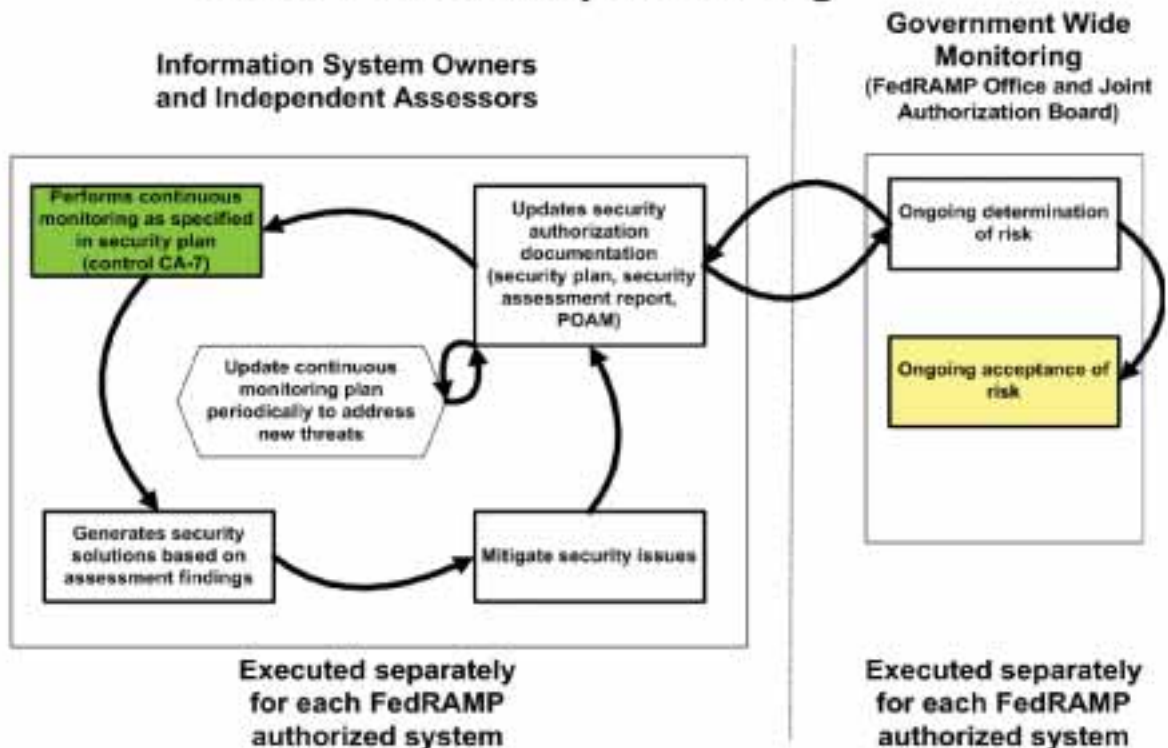
The lack of consistent requirements standardization is frustrating for industry suppliers, such as Microsoft, which must satisfy a raft of security requirements for each agency’s cloud deployment. Javier Vasquez, director of Collaboration

& Cloud at Microsoft Federal, said the company fully understands there’s no security without accreditation and established trust. “But requirements must be normalized,” he said. “When regulations and controls remain fragmented, it’s difficult to go back to corporate to support each agency’s separate, individual compliance requirements.”

The situation is changing however, with the advent of the NIST-promoted Federal Risk and Authorization Management Program (FedRAMP) to help mitigate risks to public sector cloud adoption. The program has been in the works for months, originated by the Cloud Computing Advisory Council. Federal CIO Vivek Kundra formed the council, co-chaired by Peter Mell, a senior computer scientist at the National Institute of Standards and Technology (NIST).

Mell explained the FedRAMP program’s primary advantages to attendees at the Summit. Industry suppliers will be able to work with one security assessment and authorization body for risk management and no longer will be forced to meet all of

## FedRAMP Ongoing Risk Management and Continuous Security Monitoring



Source: NIST

---

## FedRAMP Benefits

Benefits of this government-wide risk management program include:

- Agreed upon security standards for all federal organizations
- Security authorization and continuous monitoring
- Agencies participate by leveraging the results for covered products

Industry suppliers gain:

- Government-wide authorization and security compliance cost reduction

Agencies gain:

- Cost savings through reduced duplication of efforts
  - Rapid acquisition
  - Improved security assurance
- 

the security requirements of many differing agencies, he said.

FedRAMP will provide joint authorizations and continuous security monitoring of shared IT services for federal departments and agencies that enter contracts with outside providers, including cloud computing solutions. A joint authorization board will review the certification and accreditation work for a cloud service. Once approved (which could happen by the end of this month), the service would be available for use government-wide.

Mell said FedRAMP conforms with existing Office of Management and Budget and NIST IT security guidance, including Special Publication 800-37 Revision 3, which is aimed at applying risk management to federal IT systems. FedRAMP is expected to promote development of common security requirements for specific systems, provide ongoing risk assessments, encourage better system integration and dramatically reduce duplication and associated costs.

Suppliers and industry observers applauded NIST's standards efforts via FedRAMP. "We fully support NIST's FedRAMP," said Microsoft's Vasquez. "This program definitely has momentum, and the right people in charge to influence reciprocity and accreditation."

In a blog following the May cloud summit, Jon Oltsik, a senior principal analyst for the Enterprise Strategy Group, Milford, Mass., said, "If FedRAMP works, cloud service providers can deliver to a single set of standards. This will encourage innovation and bolster competition."

On the agency side, FedRAMP could spur a wave of cloud computing consumption over the next few years. But what if it doesn't work? "If FedRAMP fails, the federal government becomes difficult to service, so most cloud service providers [will likely] treat it as a market niche," Oltsik explained. "If this happens, the federal government could lose its cloud computing leadership and momentum very, very quickly." ▼

---

## How FedRAMP Is Structured

FedRAMP consists of three entities:

- Security Requirement Authorities to create government-wide security requirements.
  - A Joint Authorization Board to perform authorizations that can be leveraged by agencies.
  - The FedRAMP Office manages the program and conducts technical analysis of authorized solutions.
-

# Cloud Security Concerns, Best Practices

‘Caveat emptor’ was the key advice from industry observers and early adopters of cloud computing at the recent Cloud Computing Summit in Washington D.C. And if a recent survey is accurate, 70 percent of government technology decision-makers are indeed concerned about data security, privacy and integrity in the cloud.

The Cyber Security Alliance partners released the results of a collaborative cloud computing and cyber security survey in late April. Results reflect input from 198 respondents from all military branches and a variety of federal government agencies. The alliance commissioned an online survey to measure awareness and attitudes about cloud computing and cyber security. Established in 2009, the Cyber Security Alliance’s mission is to address key cyber security concerns. Led by Lockheed Martin, alliance members include: APC by Schneider Electric, CA, Cisco, Dell, EMC Corporation and its RSA Security Division, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, Symantec and VMware.

The best way to address cloud security, according to NIST officials, is to play close attention to the following elements when working with cloud services providers:

- Work with the provider to determine its attention to security. Compare the vendor’s security precautions to current levels of security to ensure the provider is achieving parity, or better security levels.
- Assessing risk is paramount. Require cloud computing partners to provide risk assessments and information on how to mitigate uncovered security issues.
- If the provider doesn’t have a seasoned client-facing CSO, CISO, or equivalent security professional, proceed with caution. This is a sign the vendor doesn’t take security seriously.
- Understand cloud security should be equal to the most risky client the provider supports.
- A cloud provider should be able to map policy and procedures to any security mandate or security-driven contractual obligation an agency faces.
- Pay attention to the provider’s adherence to secure coding practices. If the vendor doesn’t provide a strong story about the discipline used to write code, run away.

*(Source: NIST)*

Meanwhile, the Cloud Security Alliance also published a

list of best practices advice for securing SaaS and PaaS environments, including:

1. At minimum, authenticate users with a user name and password, along with stronger authentication options depending on the risk level of the services being offered.
2. Enterprise administration capabilities are required, especially the administration of privileged users for all supported authentication methods.
3. Self-service password reset functions should be used first to validate identities.
4. Agencies must define and enforce strong password policies.
5. Consider federated authentication, which is a means of delegating authentication to the organization that uses the SaaS application.
6. User-centric authentication (such as OpenID) can allow users to sign in using existing credentials that need not be stored by the consuming site.

## Questions to Raise...

Separately from the Cloud Security Alliance, a list of security-related questions for federal agencies to keep in mind when negotiating a cloud-computing contract include:

- What access control model is used and how well does it meet agency requirements?
- Are the authoritative sources of access control policy and user profile information chosen by the cloud provider, the individual user, or a third party such as the organization a user belongs to?
- Where do user accounts reside? How are they provisioned and deprovisioned? And how is the integrity of information protected?
- What authentication mechanisms are supported? And are they appropriate for the sensitivity of information in the service?
- What single sign-on model(s), if any, are supported? And who can select the external authentication services allowed for users? (This influences the integrity of data used for access control.)
- Does the supplier support the retrieval of access control policies and user profile information from external sources? If so, what formats and transmission mechanisms are accepted?



- What support is provided for delegated administration by policy administration services?
- What log information is provided, and can it be accessed so it can be imported into internal operational analysis and reporting tools?
- Can a user specify external entities with which to share information? If so, how is that accomplished?

For more information, read the white paper at:

[www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf](http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf)

### Contracting Pitfalls

Finally, and equally worrisome, according to recent research conducted by Yankee Group analyst Camille Mendler, is a troublesome lack of customer service on standard cloud computing contracts. “Cloud vendors offer poor service guarantees and limited financial redress if their service fails,”

she said. “Get-out clauses are rife, and robust privacy policies are rare, potentially exposing organizations to litigation.”

Mendler’s analysis is based on an investigation of 41 software, infrastructure and platform-as-a-service (SaaS, IaaS and PaaS) providers that collectively market 46 different services. Included in the research were standard service terms, service-level agreements (SLAs) and privacy practices. Yankee Group found only half of service providers offer SLAs, and none offer financial compensation when they fail to perform against the SLA. Timelines to fix problems are often not listed and customers can expect limited reparation other than service credits or the ability to terminate the contract, according to the Yankee Group report.

Mendler said as cloud service outages (such as the one suffered by the Treasury Department) regularly hit the headlines, focus must be sharpened, “on the minutiae of cloud service commitments.” ▼



# Understanding Cloud Formations

There are a number of ways agencies can leverage the technological tools, services and expertise available to help consolidate and modernize data center operations and smooth the migration to cloud-based solutions.

Investments in virtualization, high-speed networking, automated tools for management, monitoring and capacity planning all can be used as stepping stones in the move to cloud-based services. Federal organizations are leveraging cloud-related technologies such as virtualization and service-oriented architecture (SOA) to build on-demand web services.

“Virtualization enabled us to reduce servers by 66 percent, and physical data center requirements by 12,000 square feet,” said Chip Brodhun, senior technologist/project director of emerging technologies for the U.S. Marine Corps (USMC). The USMC was able to transition from simple consolidation via virtualization into cloud services by implementing greater automation in the management of its IT environment. Without additional budget or personnel, cloud services can be used help alleviate some IT management chores, he explained.

Although cloud computing is still evolving, it has been defined by NIST as a pay-per-use model for enabling convenient, on-demand network access to a shared pool

of configurable and reliable computing resources. These resources include “networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction,” NIST said.

The elastic, shared, self-managing and self-healing utilities inherent in cloud computing are so attractive because they support all users, no matter where they are located. Also, these services can minimize inefficient infrastructure, while boosting initiatives such as Green IT, disaster recovery/COOP (continuity of operations) and Telework. Cloud computing also can help federal agencies create unified, reliable, available infrastructures, comprised of interchangeable industry-standard components.

There are three primary cloud service models federal agencies can choose from, including:

**Infrastructure as a Service (IaaS)** – this provides the ability to provision processing, storage, networks and other computing resources, offering the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts IT operations in the hands of a third party, with options available to minimize impact if a cloud provider has a service interruption.

Visual Model Of NIST Working Definition Of Cloud Computing

<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>



Source: NIST

**Platform as a Service (PaaS)** – offers the capability to deploy onto a cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider.

**Software as a Service (SaaS)** – delivers the ability to use a provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

Another important choice to make involves selecting a deployment model for a cloud solution. Here's a brief description of the four primary models:

- **Private clouds** – operated solely for an organization, this option creates the least risk. A private cloud may be managed by the organization or a third party and may exist on-premise or off-premise. On the downside, a private cloud may not provide the scalability and agility of public cloud services.
- **Community clouds** – shared by several organizations, this type of cloud deployment supports a specific community with a shared mission or interest. Community clouds may be managed by the organizations involved, or by a third party, and may reside on- or off-premise. Data may be stored with the data from other organizations.
- **Public clouds** – owned by industry suppliers that sell cloud services. Public cloud services are made available to the general public or a large industry group. Data may

be stored in unknown locations and may not be easily retrievable.

- **Hybrid clouds** – Two or more clouds (private, community or public) that remain unique entities, but are bound by standardized or proprietary technology that enables data and application portability, such as cloud bursting for load balancing between clouds. This model can be used to reduce inherent risks to data by merging different deployment models. Hybrid clouds work best in environments that already use classification and labeling of data to ensure data elements are assigned to the correct cloud type.

The choice of deployment model is tied to each agency's specific requirements. According to Jon Oltsik, a senior principal analyst for the Enterprise Strategy Group, Milford, Mass., the most popular choices are SaaS and IaaS. SaaS is popular because it provides a 'commodity' method for achieving better services, such as customer relationship management, he said. Meanwhile, IaaS is used for development purposes and laptop backup services. Oltsik recommends if internal resources or skills are scarce, cloud-based services may provide a viable alternative to resolve agency-specific challenges.

Meanwhile, he added, it's far less appealing to consider cloud services for highly customized applications or services deemed sensitive or mission critical. ▼

# Town Halls and Other Online Constituent Services

Microsoft Details Government Cloud Services

---

With the onset of the upcoming election season fast approaching, Microsoft officials are optimistic current and future prospective politicians will want to leverage cloud computing via the company's CampaignReady to set up and run their campaigns.

According to Javier Vasquez, Director of Collaboration & Cloud at Microsoft Federal, CampaignReady social media was used by candidates during the recent Massachusetts political campaigns. Cloud computing services "are a perfect fit for politicians during election season," he explained. "This is a quick and easy way for politicians to setup and run their campaigns, and even take down operations, based on election results."

One of the initial applications inside CampaignReady is Microsoft TownHall, an online tool that organizes, moderates and houses online conversations, driving discussions on crucial issues and concerns. Politicians can use TownHall to engage voters online, scale communications, aggregate feedback and gain voter insight. The most popular or relevant questions rise to the surface, so participants can readily see timely topics at any moment. Because it's hosted on Windows Azure, TownHall is ideal for politicians who don't want to manage bulky technical infrastructure. Because CampaignReady is a service available using a pay-only-for-usage model, customers won't be required to purchase hardware and bandwidth that might sit idle. Nor do they worry about handling a crush of traffic around a spike in activity. A typical campaign can connect with more than 100,000 constituents, 24 hours a day using this online, always-available vehicle.

The CampaignReady service and TownHall are not just for political candidates. NASA also is using TownHall for its Be a Martian Web site, which enables the public to participate as citizen scientists to improve Martian maps, take part in research tasks and assist Mars science teams studying data about the Red Planet. In less than six months, Be a Martian participants have earned more than 2.2 million points.

Beyond political campaigns, TownHall can also be used to engage:

- Customers of a brand
- Attendees at an event
- Customers seeking support
- Fans of a sports team, TV show, film or other topic
- Disaster victims seeking to connect with resources
- Virtual teams that include internal and external resources.

For more information, please visit:

[www.microsoft.com/campaignready](http://www.microsoft.com/campaignready)

Meanwhile, the City of Miami wanted to improve applications that use mapping technology and required a cost-effective, scalable solution to fit its shrinking IT budget. Mapping applications are typically processing-power intensive, and the IT department was unsure it had the compute power to handle new mapping applications.

After evaluating several cloud offerings, the city chose Microsoft's Windows Azure platform, along with Bing maps, to deliver a 311 application, which takes advantage of sophisticated mapping technology. The City of Miami teamed with Microsoft Gold Certified Partner ISC, a provider of interactive mapping software for geospatial visualization and analysis, to develop the 311 application hosted on the Internet. Windows Azure provided developers with on-demand compute and storage to host, scale, and manage Web applications on the Internet through Microsoft data centers.

Now, with near limitless storage and processing power, the city expects the new system will eliminate much of its need to procure, host and manage physical servers – representing a 75 percent savings in the first year. It also does not need to redirect valuable developer resources or hire additional staff to deploy and manage a server infrastructure. One additional bonus - by relying on hosting at Microsoft data centers, the hurricane-prone city improved its disaster-recovery strategy.

Developers plan to add more functionality, including the ability for users to submit service requests with photos, global positioning system location, and a description directly from their Windows phone or Apple iPhone. In addition, the city could send status updates and notifications to users by e-mail message or short message service (SMS). ▼

**Security is in.**  
**Compliance is in.**  
**Privacy is in.**

**Microsoft has spent billions on increasing the capacity and security of its system infrastructure and data centers. We're all in.**



Microsoft has over 25 years of experience working with government agencies. Find out more at [microsoft.com/cloud/gov](https://microsoft.com/cloud/gov)

**Microsoft®**