

THE DOWNLOAD

Cloud Computing Research Study



WHEN THE CLOUD MAKES SENSE – PAGE 2

Cloud computing could help the government become significantly more efficient. But is it always the right choice?



THE TRUTH ABOUT CLOUD SECURITY – PAGE 5

Several agencies are confidently wading through complicated cloud security concerns to help others feel better about releasing control of their data.



THE FUTURE OF CLOUD COMPUTING – PAGE 8

Although cloud computing will not completely replace on-site data centers in the federal government, the cloud will dominate new applications development.



WHAT ARE SAAS, IAAS AND PAAS? AND WHY SHOULD YOU CARE? – PAGE 10

Users should mix and match three different types of cloud computing.



THE ROI OF CLOUD – PAGE 13

If agencies carefully choose the right tactics at the right time for the right mission, they can reap significant financial savings with a move to cloud computing.

When the cloud makes sense

Cloud computing brings significant efficiencies to government, but is it always the right choice?

The twin pressures of reduced budgets and the need for greater efficiency have led the federal government to strongly promote cloud computing as a solution whenever possible. In fact, the Office of Management and Budget in December 2010 declared that government now operates under a cloud-first policy, meaning that agencies must first try to incorporate some type of cloud computing into projects. And if they choose not to use a cloud scenario, they must justify their decision.

“What this means is that going forward, when evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists,” said Jeffrey Zients, chief performance officer and deputy director for management at OMB, in November 2010.

According to a survey released in December 2010 by the 1105 Government Information Group, cost reduction, fast access to data and applications, and simplifying IT infrastructure and management are the top three reasons that federal agencies are moving to the cloud. Roughly half of the 460 respondents work for a civilian agency, while the other half worked for military agencies. And roughly half had non-IT titles but substantial roles in technology decision-making while the other half had IT titles.

The survey also found most government respondents indicated that private, public or hybrid cloud computing will become a vital element in federal IT activity during the next several years. Indeed, roughly one-third of respondents have already adopted or are in the process of adopting one or more cloud implementations.

Shedding even more light on the potential of cloud in government, a study released in April 2010 by Market Connections found that government users are willing to use cloud computing for core functions of their IT infrastructure. Nearly one-quarter use cloud computing for mission-critical data management and an even higher percentage is considering doing so.

Input, a government technology market research firm, validates these survey observations as well. It predicts that the government market for cloud computing will more than triple from 2010 to 2014, to \$1.2 billion.

What type of cloud makes sense?

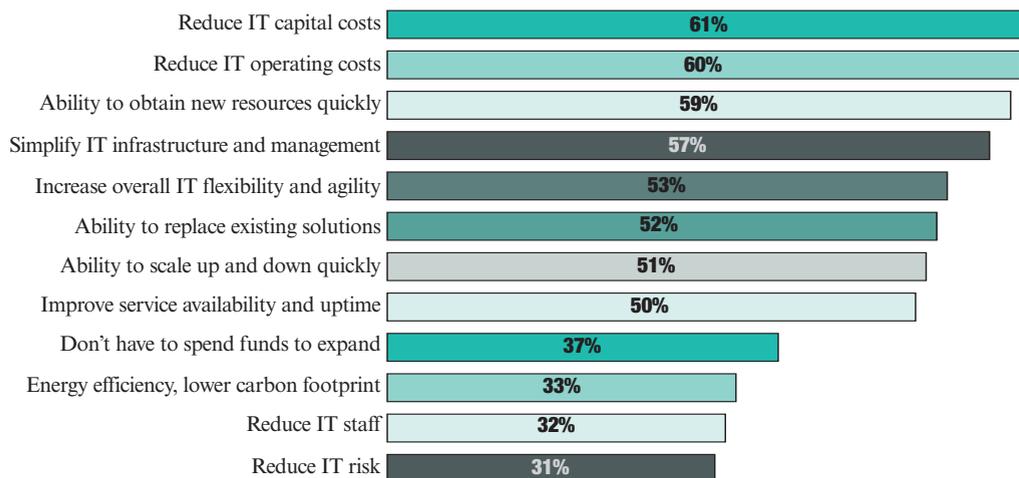
Moving to the cloud can bring many benefits, but one size doesn't fit all. The type of cloud you ultimately choose has a lot to do with the importance of the mission or application, in addition to the relative importance of issues such as time, availability, data portability, security, data transfer, high performance and rapid scaling.

The most common type of cloud environment in government today by far is the private cloud. Private clouds are operated solely for one organization, can be managed either by the organization itself or by a third party, and can exist either on-site or off-site.

In general, federal agencies and departments opt for private clouds when sensitive or mission-critical information is involved. Private clouds are hosted on an agency's own dedicated hardware,

WHAT DRIVES CLOUD COMPUTING

(% OF RESPONDENTS, MULTIPLE ANSWERS ALLOWED)



and services and infrastructure are maintained on a private network. This increases security, reliability, performance and service. Yet like other types of clouds, it's easy to scale quickly and pay for only what is used, making it an economical model.

Here a few examples of private clouds throughout government.

- NATO's Allied Command Transformation, in concert with IBM, is developing a private, on-premise cloud for testing and developing network solutions for command, control, intelligence, surveillance and reconnaissance projects.
- Last year, the Customs and Border Patrol agency started moving its collaboration software and e-mail services to a private cloud inside of one of the Homeland Security Department's data centers.
- Los Alamos National Laboratory has implemented a private cloud with HP technology that allows researchers to use servers on demand.

Many vendors provide private clouds to government, including IBM, Lockheed Martin, Hewlett-Packard and Oracle.

The public cloud

Unlike private clouds, public clouds are usually made available to the general public or other government departments or agencies. Like all clouds, they are pay as you go, meaning that agencies pay only for the computing power they need at a given time for the number of users. Public clouds are more secure than accessing information via the Internet and tend to cost less than private clouds because services are more commoditized. Research by the 1105 Government Information Group found that for federal agencies interested in public clouds, the most popular functions are:

- Collaboration;
- Social networks;
- CRM;
- Storage.

Public clouds are an ideal solution for the burgeoning cost of managing internal storage. They provide a

cost-effective alternative to operating and maintaining agencies' storage area networks. Although some agencies are wary of the public cloud because of security concerns, others have overcome those concerns and are moving forward. One example is the Treasury Department, which has moved its website, Treasury.gov, to a public cloud using Amazon's EC2 cloud service to host the site and its applications. The site includes social media such as Facebook, YouTube and Twitter to communicate with its constituents. Another example of public cloud adoption is the Agriculture Department's Food and Nutrition Service. It uses Amazon's cloud to support an application to help people locate retailers that accept Supplemental Nutrition Assistance Program benefits.

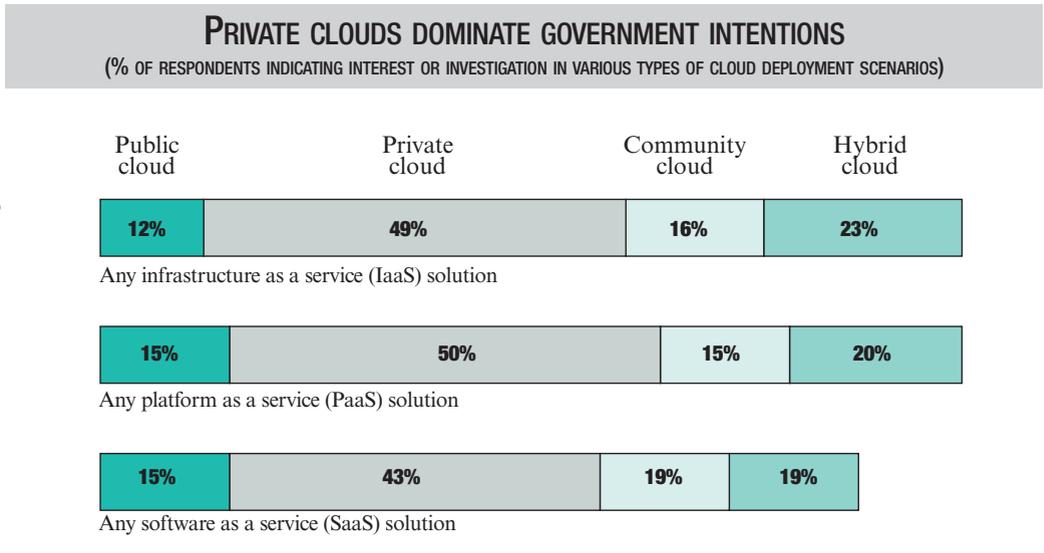
Even DHS can embrace the public cloud in the right circumstances. CIO Richard Spires stated in October 2010 that the department plans to contract with a public cloud provider to host its public-facing websites.

Other cloud computing models

Hybrid cloud computing is exactly what it sounds like: a combination of both public and private clouds. In this scenario, two or more clouds coexist in the same environment – the private cloud containing sensitive information and applications and the public cloud containing less sensitive information and platforms.

This model allows organizations to combine everything under one infrastructure, facilitating collaboration and management, while maintaining the desired level of security and privacy.

NASA is one federal agency that has embraced the hybrid model. Its Nebula open-source cloud computing



Federal Cloud Initiatives

- Data.gov: An open-government initiative from the Executive Office of the President that provides a centralized federal cloud providing easy public access to datasets generated by federal agencies.
- The Defense Information Systems Agency's Rapid Access Computing Environment: A cloud-based solution that allows users to purchase a basic computing environment and use it on demand.
- NASA Nebula: An open-source cloud computing project and service that provides infrastructure on demand and a way for NASA scientists and researchers to share large, complex datasets with external partners and the public.
- The General Services Administration's Info.Apps.gov: A website where agencies can research how cloud computing can enable them to provide more cost-effective IT services for federal government.
- Interior Department's National Business Center: Infrastructure as a service, platform as a service and software as a service offerings via the cloud for other federal agencies.
- Federal Risk and Authorization Management Program: An interagency initiative spearheaded by the National Institute of Standards and Technology to provide a governmentwide certification process to ensure security of cloud products and services.
- The Standards Acceleration to Jumpstart Adoption of Cloud Computing: Run by NIST, it aims to drive the formation of cloud computing standards by providing working examples that show how key use cases can be supported on cloud systems that have implemented a set of specifications.

project uses a private cloud for research and development as well as a public cloud to share datasets with external partners and the public.

State governments are turning to hybrid clouds as well:

- Colorado's plan includes a private cloud for highly secure, line-of-business data and systems; a virtual private cloud for archival storage and disaster recovery; and a public cloud for e-mail, office productivity applications and websites.
- Michigan also plans to provide cloud services via a hybrid model to its agencies, cities, counties and schools.

Yet another type of cloud is a community cloud. Shared by several organizations, this type of cloud deployment supports a specific community with a shared mission or interest and can be shared by several departments or agencies.

Examples might include a community dedicated to compliance considerations or a community focused on security requirements policy. There may be a community cloud for health-related concerns throughout government, or one for everything related to immigration.

Community clouds can be managed by the organizations involved, or by a third party, and may reside on-site or off-site. Data may be stored from several organizations on partitioned servers and disks. Several vendors are getting in on the community cloud trend, including IBM, which said two agencies have signed onto its Federal Community Cloud so far. Although there are many types of cloud scenarios, there probably is one that is right for every environment. It's just a matter of finding the right fit.

The Truth about Cloud Security

Security is areal issue, but the feds are on the case

Although the cloud provides many benefits for government, it also exposes data and systems to risk. Before any federal government agency moves to the cloud, it must be 110 percent sure that every possible security precaution is taken.

Agencies are serious about cloud security. According to The Download on Cloud Computing in Government, a December 2010 survey by the 1105 Government Information Group, the most critical cloud computing security worries are potential data loss or leakage, robust identity authentication and credential management, and secure and timely identity provisioning. Other concerns include effective data encryption; physical security; insecure application programming interfaces; and account, service and traffic hijacking.

The Download survey found that 55 percent of the 460 government respondents don't think cloud solutions are secure enough, and 59 percent agreed that security risks associated with cloud computing implementation are greater than those for on-premise IT implementations. Roughly half of the respondents work for a civilian agency, while the other half worked for military agencies. And roughly half had non-IT titles but substantial roles in technology decision making, while the other half had IT titles.

The Cyber Security Alliance also posted dire numbers.

According to an April 2010 survey of federal agencies on collaborative cloud computing and cybersecurity, 70 percent of government technology decision-makers are concerned about data security, privacy and integrity in the cloud.

Although some of these concerns are valid, some may be due to a simple lack of knowledge, said Melvin Greer, senior fellow and chief strategist for cloud computing at Lockheed Martin.

"In a survey we did in 2010 focusing on cybersecurity in the cloud, we found that the more people are aware of the cloud, the less concerned they are about security, and the less aware they are, the more they are concerned about security," he said.

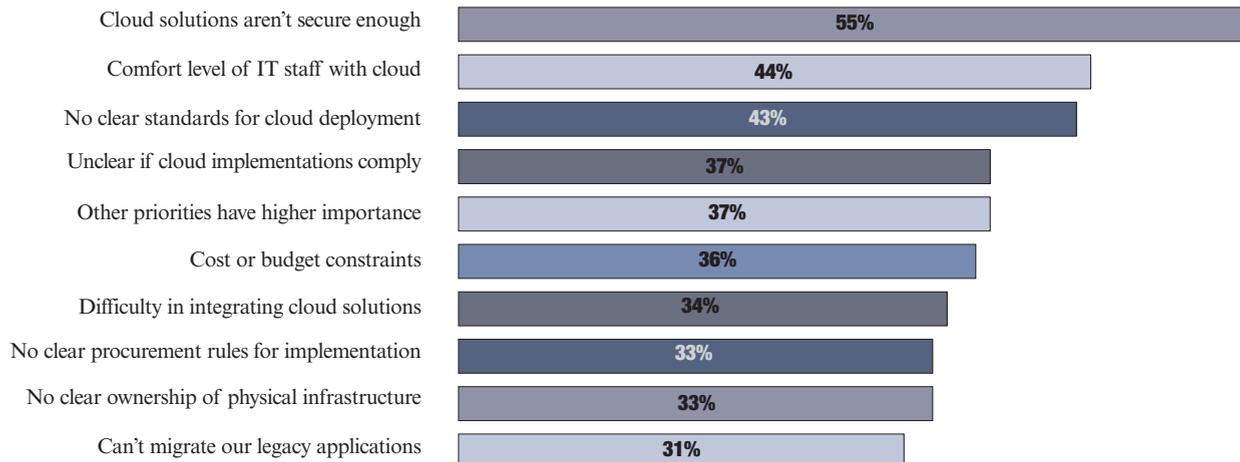
Indeed, other surveys beginning in 2009 have shown that the percentage of respondents extremely concerned about security of cloud implementations has been steadily declining as more information and experience provides reassurance.

Taking the right steps

Although the level of concern may have declined, it is not going away. The federal government has taken significant steps to ensure that cloud computing will not compromise security of government data or the private information of its people. Enough progress has been

SECURITY NOT THE ONLY CLOUD CONCERN

(% OF RESPONDENTS INDICATED THE FOLLOWING WAS A CONCERN OF THEIR AGENCY)



made during the past few years to prompt Federal CIO Vivek Kundra to say at a House committee meeting last summer:

“As we move to the cloud, we must be vigilant in our efforts to ensure the security of government information, protect the privacy of our citizens, and safeguard our national security interests. The American people must be confident that their information is safe in the cloud. Therefore, we are being deliberate in making sure the federal government’s journey to the cloud fully considers the advantages and risks associated with cloud technologies, by defining standards and security requirements.”

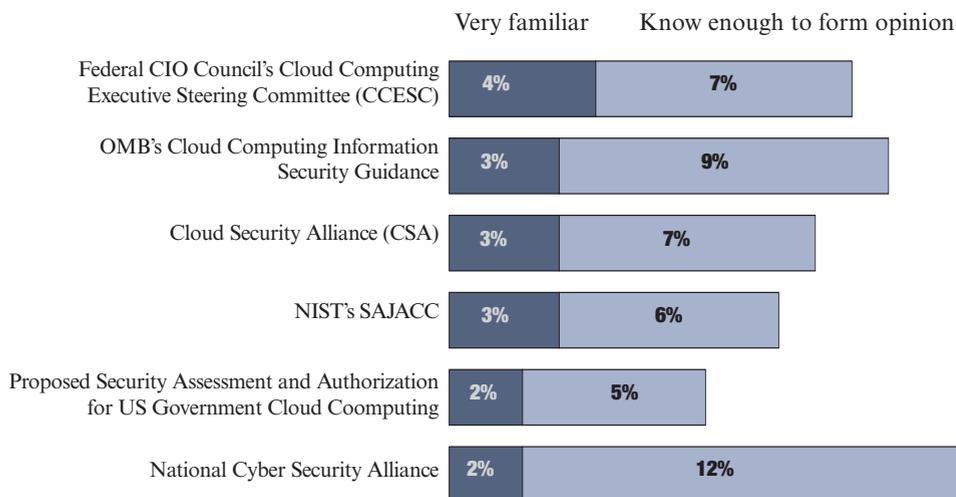
The security process started in earnest in November 2009, when the General Services Administration’s cloud office established working groups on security and standards. In February 2010, GSA launched a governmentwide security certification and accreditation process for cloud computing solutions, culminating in

and local governments receiving federal funds but required those vendors’ products to pass a federal information security test. That test, administered by NIST, involves a six-step risk management process that includes identifying and implementing security controls.

Other cloud security efforts include the National Cybersecurity Education Initiative, which aims to improve the effectiveness of the cybersecurity force, and the Cloud Security Alliance, a nonprofit organization made up of industry-leading cloud vendors to promote best practices for providing security assurance for cloud computing.

Meanwhile, the December 2010 survey found that typically only 15 percent of the respondents were familiar with any of the half-dozen major organizations focused on cloud security. However, survey respondents from organizations that had fully adopted cloud computing for at least one application were more aware of the various security initiatives.

FEW FAMILIAR WITH CLOUD-RELATED INITIATIVES FOCUSING ON SECURITY SOLUTIONS



the development of the interagency Federal Risk and Authorization Management Program. FedRAMP, spearheaded by the National Institute of Standards and Technology and backed by GSA and the Office of Management and Budget, is a program to develop a common security and continuous assessment model for clouds across government.

The momentum continued in 2010. In October, GSA announced that it had chosen 11 vendors to offer cloud-based infrastructure as a service to federal, state

Few familiar with cloud-related initiatives focusing on security solutions

Some agencies act as if security issues are well in hand. Khawaja Shams, a senior solution architect at NASA’s Jet Propulsion Laboratory, last year said security issues are surmountable. He said that instead of avoiding the cloud, JPL is working with its office of the CIO and IT security teams to make sure it can leverage the benefits of the cloud without compromising security.

Likewise, the Defense Information Systems Agency

Some say the cloud can actually enhance security

Despite the fact that most federal agencies are either concerned or very concerned about the security risks of cloud computing, a Government Accountability Office report released last year concludes that cloud computing could increase the security of information systems in federal agencies.

“The cloud enhances security by enabling data to be stored centrally with continuous and automated network analysis and protection,” said Mike Bradshaw, director of Google’s federal government division, at a July 2010 hearing held by the House Oversight and Government Reform Committee and its Government Management, Organization and Procurement Subcommittee.

In addition, some say that with the cloud, data is easier to monitor and control because it is centralized and security testing is easier to manage to administer. Incident investigation and response also is faster and easier. One example is platform as a service, in which systems are automatically patched and updated by an expert software vendor, increasing the security of all data and applications hosted in it.

allows military users to run applications in production mode in its private cloud computing platform, the Rapid Access Computing Environment. Henry Sienkiewicz,

DISA CIO, said last year that RACE is more secure than commercial cloud services. He said his team applies the same information assurance process to its cloud-based applications as it does to applications that run on traditional computing platforms.

Watching your step

Even as security concerns for cloud computing continue to ease, both because of the measures being taken and because of more educated customers, experts recommend following best practices diligently. The Cloud Security Alliance recommends defining and enforcing strong password policies, considering federated authentication to delegate authentication to the organization using the cloud service and implementing user-centric authentication (systems where users, rather than service providers, control their identity credentials).

NIST recommends intense vetting of your cloud provider, comparing its security precautions with current levels of security in your on-premise implementation to ensure that the provider is achieving as good or better security levels. The agency also recommends requiring cloud computing partners to conduct risk assessments for a cloud implementation of a solution to an agency mission, ensuring that a cloud provider can map policy and procedures to any security mandate or security-driven contractual obligation you face. In addition, agencies should include procedures to audit a cloud provider’s secure coding practices. □

The Future of Cloud Computing in Government

While cloud computing will not completely replace on premises data centers for the federal government, the cloud will dominate new applications development.

Like most new technologies, cloud computing hit the IT world hard, a bright new star in the technology galaxy. And like most new and dynamic technologies, there are inevitable trade-offs.

Unlike many hot technologies that rapidly cool off and disappear almost as fast as they burst on the scene, cloud computing will become the dominant platform for new applications, as well as the most popular solution for existing applications as they age and need to be replaced, according to a new survey of 460 government officials by the 1105 Government Information Group.

For nearly 60 years, government computing was based on developing and managing applications and data centers internally. But based on the benefits of cloud computing, a majority of federal IT managers indicated that it will become a core component of government IT in five years, according to the December 2010 survey. The survey also found that only 10 percent of respondents say cloud computing is a temporary fad and won't last.

Still, there are many barriers to full cloud adoption by government. Many agencies are still worried about security, while others are hesitant to change the way they do business. Other concerns include compliance, how to integrate cloud computing with in-house systems, IT, and worries about giving up control.

But all of that is changing. Input, a marketing intelligence company that focuses on government, predicts that

government spending on cloud computing will exceed \$1.4 billion by 2015, with a compound annual growth rate of 23 percent — roughly five times the overall federal IT spending growth rate.

Cloud adoption is basically in the investigation stage, according to the survey respondents. While roughly 12 percent of the respondents have already adopted cloud computing for at least one application, 20 percent are in development, and 55 percent are investigating the technology. Hardly anyone responding to the survey indicated no interest in the technology.

Perhaps the biggest barrier to greater adoption of cloud computing in federal government has been privacy and security concerns. The government's big push to deal with those security situations — programs such as the Federal Risk and Authorization Management Program — will go a long way toward fixing them, as will industry consortia such as the Cloud Security Alliance. Cloud vendors, including IBM, Rackspace, Trend Micro, Lockheed Martin and Google. These companies are actively involved in the alliance, which seeks to provide solutions to security problems in advance of standards.

In addition, vendors have worked hard to shore up their identity management and access control methods, encryption methods, and auditing and monitoring methods, making significant progress in explaining how the clouds that they offer map to the requirements of government missions.

Leading cloud vendors are in the process of getting their clouds certified as safe and secure by the federal government during the next several years.

“There is a lot of progress being made on the security front,” said Melvin Greer, senior fellow and chief strategist

CLOUD COMPUTING IS SEEN AS VITAL FUTURE COMPONENT IN FEDERAL IT ACTIVITIES



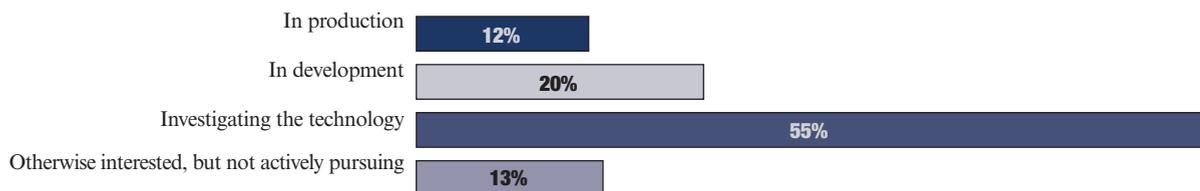
Within the next five years, cloud computing will become a core component of computing options in the federal IT environment.



Cloud computing is just a temporary fad – it won't last.

FULL SPEED AHEAD FOR CLOUD COMPUTING

(% OF RESPONDENTS INDICATING STATUS OF CLOUD COMPUTING)



of cloud computing at Lockheed Martin. “Within 18 to 24 months, cloud security will be no more of an issue for federal government than any other IT security issue.”

Another area of concern is compliance. As cloud technologies improve and as compliance requirements adapt to accommodate cloud architecture, the situation will become less of a concern.

In a November, 2010 white paper on cloud computing in the public sector, Microsoft made the analogy to e-signatures. Although they were not accepted for many documents in the early days of the Internet, acceptance became commonplace as authentication and encryption technology improved and as compliance requirements changed. Microsoft notes that the same will happen with compliance in the cloud.

The perception that agencies are giving up control over their applications, data and infrastructure has been another barrier, but that evidence is anecdotal. Indeed, the 1105 Government Information Group survey didn’t find concerns about control to be a dominant concern. 1105 Government Information Group survey respondents listed factors such as security, comfort level and perceived lack of standards as their concerns, and a perceived lack of control didn’t seem to be an issue.

Input found that the growth and strength of software as a service adoption in large organizations are proof that perceptions are changing as the trade-offs tilt in

favor of an on-demand approach. And as more success stories emerge, the perception of giving up control will be much less of an issue, said Deniece Peterson, manager of industry analysis at Input.

Another issue is concern over how to integrate a cloud computing environment with in-house IT. That will slowly dissipate, as success stories emerge and as government further embraces SaaS and service-oriented architecture. Cloud computing is a natural extension of these solutions, Peterson said, and aligns well with an incremental approach to cloud computing.

As these are being dealt with in government, industry also is doing its part, with cloud vendors becoming more aggressive in developing and improving public sector-specific cloud solutions. Many large vendors are working hard in this arena, including IBM, Microsoft, Hewlett-Packard, Google, Cisco Systems, Oracle, VMware, Citrix and Symantec.

All of these facts point to one truth: the cloud is fast becoming a permanent part of the federal government’s IT infrastructure. The concerns of federal government are real but are being dealt with quickly and likely will fade over time as the comfort factor increases, successes are celebrated, and security and other issues are put to rest.

“Within a decade, [government] will have a nearly complete cloud infrastructure,” Peterson said. □

What are SaaS, IaaS and PaaS, and why you should care

Vendors offer three different types of cloud computing. Users should mix and match.

With its cloud-first approach, there is no doubt that the federal government supports moving to cloud computing infrastructures. But there are different types of cloud models, each appropriate for certain scenarios and inappropriate for others:

- Software as a service;
- Infrastructure as a service;
- Platform as a service.

SaaS, IaaS and PaaS are delivered in several ways:

- **Public cloud:** Where the cloud infrastructure is made available to the general public or industry as well as to your agency or department and is owned by the organization selling cloud services.
- **Private cloud:** Where the cloud infrastructure is operated solely for your department or agency, and may be managed by your agency or by a third party and may exist either on-premise or off-premise.
- **Community cloud:** Where the cloud infrastructure is shared by several departments or agencies that have shared concerns — such as mission, security requirements, policy or compliance considerations — but may be managed by your agency or a third party and may exist either on-premise or off-premise.
- **Hybrid cloud:** Where the cloud infrastructure is a combination of two or more clouds (public, community or private) that are unique entities bound together by standardized or proprietary technology that enables data and application portability.

browser-based user interface.

Agencies do not need to buy, develop, install, configure and maintain application software and servers in this model — assuming an organization has the needed internal network bandwidth and suitable Internet access, everything else is outsourced. SaaS providers may host the software in their own data centers or with co-location providers, or they may outsource to an infrastructure provider.

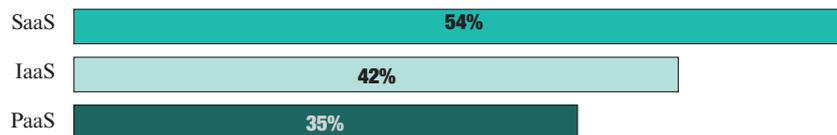
According to The Download on Cloud Computing in Government, a survey conducted in December 2010 by the 1105 Government Information Group, more than half of the 460 respondents are interested in or investigating SaaS solutions. The most popular and useful SaaS-based cloud opportunities for federal agencies include collaboration, document management, content management and project management. Roughly half of the respondents work for a civilian agency, while the other half worked for military agencies. And roughly half had non-IT titles but substantial roles in technology decision making, while the other half had IT titles.

Civilian and defense implementations of SaaS abound.

- The Army's Experience Center moved to a cloud environment to create a flexible, extendable and customizable recruitment tracking platform to track prospective recruits. The Army projects that the SaaS-based application will reduce costs to \$8 million from \$83 million and increase productivity by 33 percent.

SAAS LEADS CLOUD HIT PARADE

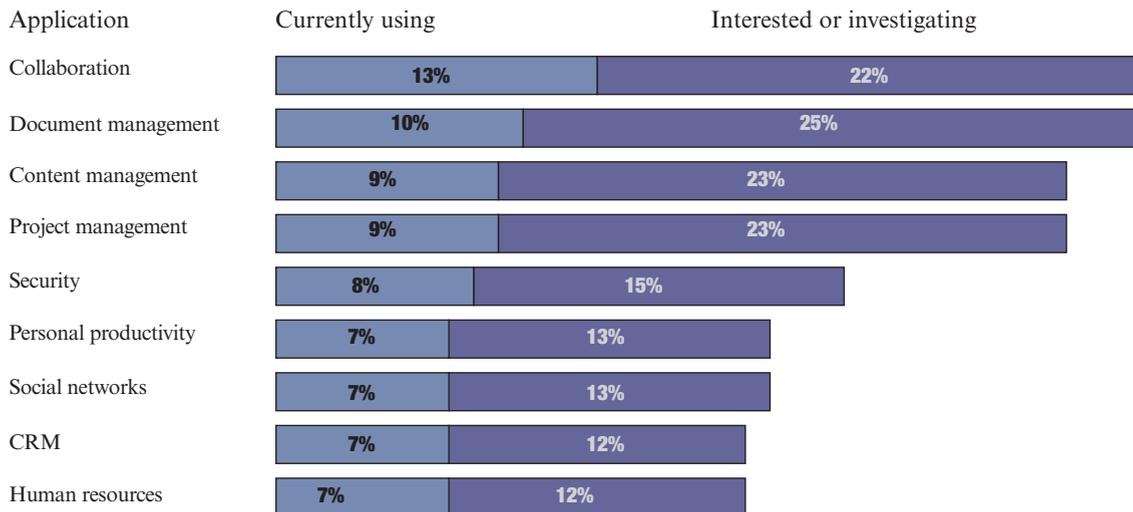
(% RESPONDENTS INDICATING INTEREST OR INVESTIGATING SPECIFIC TYPE OF CLOUD COMPUTING)



The most popular and most highly adopted cloud model is SaaS. This model allows organizations to rent remotely hosted software applications, paying for only the functionalities and computer cycles used. Applications are accessed through the Internet and a

- The Federal Labor Relations Authority replaced its decade-old, off-the-shelf case management system with a SaaS-based solution that allows users the flexibility to monitor case activity anytime and anywhere. FLRA estimates that the move to SaaS will

LEADING SAAS APPLICATIONS



reduce total costs by 88 percent in five years. It also eliminated an upfront licensing cost of \$273,000, reduced annual maintenance to \$16,800 from \$77,000 and eliminated all hardware acquisition costs.

IaaS

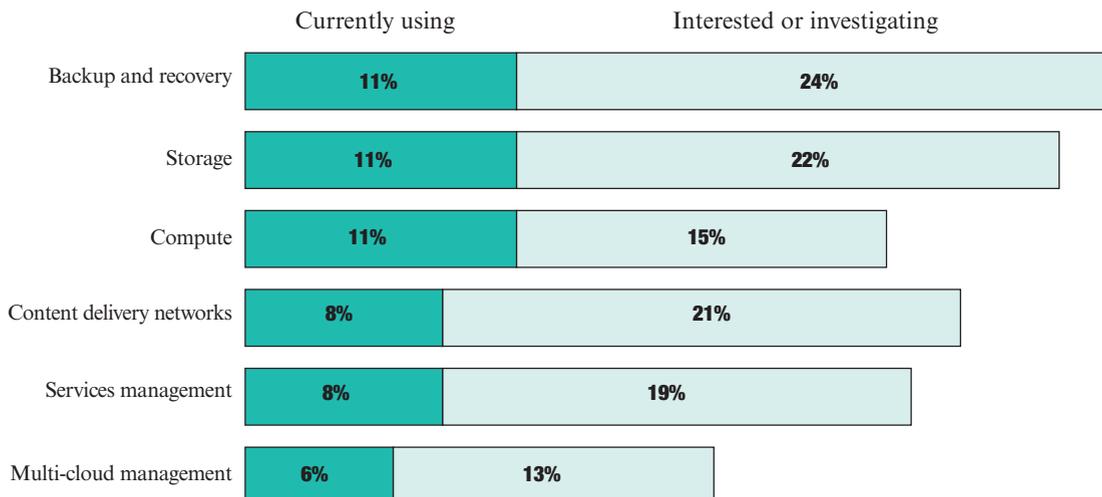
Instead of focusing on applications, IaaS focuses on the infrastructure that supports applications. IaaS puts IT data center operations — everything from processing and storage to networks — in the hands of a third party, with options available to minimize the effect if a cloud

provider has a service interruption.

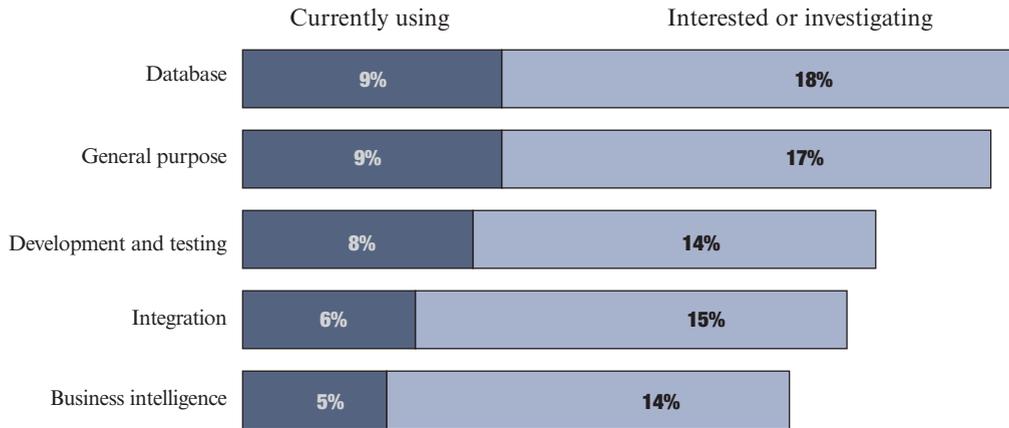
IaaS offers organizations a way to avoid buying additional servers, storage and network devices and increasing their carbon footprint, but it can take advantage of any type of software required for a mission, including operating systems and applications. The integration and management of a disparate collection of point solutions is no longer the user organization’s problem. Instead, the public cloud service provider contends with those problems.

According to the 1105 Government Information Group

HOW AGENCIES ARE USING IaaS



PaaS IMPLEMENTATION USE AND INTEREST



survey, backup and recovery, along with storage, are the most popular uses of IaaS in government. The survey found that 15 percent of federal agencies are currently using IaaS services, and an additional 42 percent are interested or investigating it. And that number is sure to grow.

Several government missions currently rely on IaaS. In fact, in October 2010, the General Services Administration awarded contracts to 11 vendors for IaaS cloud services, accessible via Apps.gov.

The Federal Geospatial Data Clearinghouse’s GeoCloud Initiative used IaaS capabilities to deploy services and solutions, improving public access to geospatial data beyond in-house capabilities; increasing speed of response, reliability, failover and security; and providing better handling of peak load situations.

PaaS

PaaS delivers an entire platform in the cloud that organizations can use to develop or test applications or application services. Like all cloud-based offerings, these are run and managed by a services vendor. PaaS eliminates high upfront costs and long development cycles while simplifying deployment.

According to the 1105 Government Information Group survey, about 12 percent of federal agencies are using

some type of PaaS solution, while another 35 percent are interested or investigating it. The most popular use of PaaS environments in government is for database systems and general development, although they can also be used for business intelligence platforms, development and testing, and integrating applications.

The Treasury Department’s Office of Comptroller of the Currency moved to the cloud for its Vulnerability Assessment System, improving security, reliability and capacity, while cutting costs. Project results include a 458 percent increase in scanning, an 86 percent reduction in cost per scan, and production operation and deployment in one day.

No matter which cloud-based alternatives make sense, the benefits will quickly become clear. PaaS, IaaS and SaaS offer agencies the opportunity to build and test innovative solutions to deliver services in less time and at less cost.

“Cloud computing services help to deliver on this Administration’s commitment to provide better value for the American taxpayer by making government more efficient,” said Federal CIO Vivek Kundra in October 2010. “Cloud solutions not only help to lower the cost of government operations they also drive innovation across government.” □

The ROI of Cloud

Moving to the cloud provides a huge financial benefit to agencies that adopt the right tactic at the right time for the right mission.

The return on investment from cloud computing, when done right, is nothing short of staggering, and government agencies clearly agree. According to a December 2010 study by the 1105 Government Information Group, half of the 460 government respondents agreed that cloud computing solutions have a lower total cost of ownership (TCO) than on-premise offerings. About half also indicated that the ROI associated with new cloud computing programs will happen faster than for comparable IT initiatives implemented via traditional on-premise approaches.

Roughly half of the respondents work for a civilian agency, while the other half worked for military agencies. And roughly half had non-IT titles but substantial roles in technology decision making, while the other half had IT titles.

Other studies validate these views and even quantify the savings. The Brookings Institution estimates that federal agencies are experiencing up to a 50 percent savings overall by moving to the cloud. In fact, some types of federal cloud deployments save more, while others save somewhat less.

“When we think about information technology and the potential of cloud computing to lower the cost of government operations, drive innovation, and fundamentally change the way we deliver technology services across the board, we recognize that this is an amazing time in the very early days of cloud computing,” Federal CIO Vivek Kundra said at a Brookings event in April 2010.

Many studies, including the study from Brookings, note that although organizations accrue significant savings from all types of cloud solutions, the largest savings tend to be from public cloud implementations. Smaller but still substantial financial benefits occur from hybrid cloud infrastructures. And public reports have shown significant financial and operational benefits from private cloud implementations, as well.

The primary areas where all types of cloud solutions offer the most cost savings are direct labor (typically IT staff), hardware, software and end-user productivity.

Labor cost savings are the easiest to calculate. By off-loading software, applications or a platform to a private cloud platform, far less time is needed to administer, maintain, upgrade and troubleshoot the technologies. For example, if a systems administrator is traditionally in charge of 140 servers, that same systems administrator can be responsible for thousands of cloud-based servers.

Automated provisioning also helps significantly reduce IT management costs. In the cloud, virtual servers are provisioned as needed automatically instead of manually. This reduces downtime and compliance issues. The 2009 Cloud Computing ROI Study by IBM Research estimated that for medium-sized cloud deployments, provisioning costs will fall by roughly half; for large clouds, however, they will fall by as much as 90 percent.

IBM Research found that 81 percent of public cloud infrastructure adoption payback is due to decreased labor.

Hardware savings also are relatively easy to quantify. By relying on hardware in a public cloud, on-site hardware has to be replaced less often and less new hardware has to be purchased. That, in turn, leads to much-reduced power and cooling costs, as well as less space needed in the data center. IBM estimates that medium-sized cloud deployments lead to a 62 percent savings in a year compared with an on-premise system. For larger cloud deployments, the annual savings approaches 50 percent compared with an on-premise implementation.

MAJORITY AGREE ON THE ROI OF CLOUD COMPUTING



A cloud computing solution will have a lower total cost of ownership than an on-premise implementation.



The return on investment from a cloud initiative will occur faster than with a traditional on-premise initiative.

Measuring ROI

Measuring hard savings in areas like labor is relatively easy, but it's more difficult to measure the soft cost savings of moving to the cloud, such as higher availability, increased productivity, and anytime/anywhere access.

The first step is to create a list of Key Performance Indicators (KPI) that specifically affect your situation. For government, these would include factors such as risk, compliance, and improvement of service to people. In addition, major KPIs that all organizations need include cost, time and service quality.

Mark Skilton of the Open Group, a not-for-profit consortium dedicated to open standards, has repeatedly urged organizations to include business metrics as well, such as the speed and rate of change, optimization, rapid provisioning, increased margin and cost control, enhanced capacity utilization, and access to business skills and capability improvement.

After gathering these metrics, create a scorecard of current and future operational business and IT service needs related to cloud computing potential. Only then will you truly begin to understand the ROI of cloud.

Software savings also can be significant. Instead of buying software licenses and being responsible for recurring annual fees, organizations can opt for a pay-as-you-go model, paying only for what they use – avoiding the waste of buying seats that are never used, commonly known as shelfware – and avoiding additional fees. And because operators of large data centers can get bigger discounts, they can pass the savings on to their customers. What's more, the cloud model enables organizations to better account for ebbs and flows in usage.

End-user productivity is at least as important as the other three categories, yet it is much more difficult to quantify. Productivity improves in cloud environments for many reasons, including the ability of end users to obtain services directly from the cloud providers. That approach reduces IT department service times by tenfold or more.

In addition, services can be rolled out more quickly, with less concern about oversight and compliance and without regard for resource constraints if the service agreement includes that type of flexibility.

Getting the best ROI possible

Although it may seem counterintuitive, it's critical to spend what it takes to make the hybrid cloud infrastructure work for you. That means investing in tools that will better manage the virtualized infrastructure of the cloud; virtualization software that manages the virtual servers; and service management software that provides the visibility, control and automation needed to best manage cloud-based services.

Also, make sure to restructure your IT organization to manage the cloud infrastructure and how it maps to the services themselves, as opposed to the underlying technology. That means changing both mindsets and processes to accommodate how the cloud works. It also means training staff to specialize in demand-planning activities such as business analysis, capacity planning, requirements gathering, documentation, negotiation, project management, financial planning and portfolio management.

Taking these steps, although temporarily painful, will put the organization in a place where it can receive the most benefit — and the highest ROI — from cloud computing. □



**ENSURING
EVERY CLOUD HAS A
CYBER LINING.**

© 2011 Lockheed Martin Corporation

THIS IS HOW

| **SECURE CLOUD COMPUTING SOLUTIONS**

Improved services. Lower costs. Less waste. Government agencies are expecting great things from cloud computing. But they're also asking hard questions. About security. And privacy. At Lockheed Martin, our decades of I.T. experience across the length and breadth of the federal government have taught us not only how to manage vast amounts of information, but how to protect it as well. Making sure every bit of data in the cloud is secure is all a question of how. And it is the how that Lockheed Martin delivers.

lockheedmartin.com/how

LOCKHEED MARTIN 