**Introduction**

Like many private sector organizations, a lot of government entities are making big moves to cloud computing, or at least planning to deploy cloud initiatives soon. Federal, state and local agencies are discovering that cloud services such as software as a service (SaaS) or infrastructure as a service (IaaS) can offer a number of benefits, and they are launching cloud-related projects aimed at lowering costs, boosting efficiencies and increasing agility and scalability.

As part of their IT transformation and move to a cloud environment, many government agencies are migrating away from legacy systems and applications and toward industry-standard platforms with virtualized servers, storage and networking.

While there are clearly potential benefits, the shift to the cloud also comes with a number of challenges, so putting in place a strong governance program needs to be a top priority for agencies as they leverage this new computing delivery model.

These are among the key findings of a State of Cloud Computing survey of nearly 150 technology and administrative professionals at federal, state and local government agencies throughout the country, conducted by UBM Tech and HP in October 2012.

Cloud computing activity is picking up at all levels of federal, state and local government, as agencies learn about the potential benefits of services-based IT. Of the 148 survey respondents to the State of Cloud Computing, more than half (55%) say they have either recently begun deploying cloud services or have been involved in cloud initiatives for several years. Forty-five percent of the government institutions plan to launch cloud computing efforts over the next 12 months. (See Figure 1.) According to an IDG report, “Strategy Guide to the Cloud in Government and Educational Institutions,” sponsored by HP and Intel, most state and local governments have fewer funds available to develop new services and focus on innovation. But cloud computing “enables new services without requiring huge investments in hardware, software and infrastructure,” the report says.

For one State of Cloud survey respondent who is part of a team overseeing a new health system designed to manage costs and build and maintain electronic health information systems, a SaaS cloud offering may be just the right solution. One specific application area the organization is looking to address is a hospital budget regulation system, which would be used to review hospital budgets and maintain budget information in a database.
The main driver for moving to the cloud, according to the organization’s director of health system finances, is “greater versatility and the potential to get more services because of the [lower] cost.”

Half of the government entities surveyed say they are using or planning to use a mix of private and public clouds, while 39 percent say they are going with private clouds, and only 11 percent are limiting their activities to public cloud services. (See Figure 2.)

What’s pushing government agencies to use these services? The biggest driver for moving to the cloud is cost savings, cited by 65 percent of the survey respondents. This is not surprising, given that many government agencies are continually looking for ways to reduce costs at all levels of their operations.

Other key reasons for moving to the cloud include increased scalability (45%) and greater agility (43%). Fewer of the survey respondents cited a lack of internal resources and a broader effort to move government agencies to the cloud as driving factors. Improving security does not seem to be a motivator for moving to the cloud, however, as only 14 percent of the respondents cited that as a reason. (See Figure 3.)

A substantial majority (86%) of the government organizations are migrating away from legacy systems and applications and toward an industry-standard platform with virtualized servers, storage and networking, or plan to do so in the future. More than one third (37%) say most of their applications and systems are moving away from legacy environments. (See Figure 4.)

As government agencies move to the cloud they are apt to do so independently of other government agencies, according to the research. About three quarters say they are not actively collaborating with other government agencies to adopt cloud services.

---

**Survey Methodology:**

In December 2012, UBM Tech conducted an online survey on behalf of HP exploring the state of cloud computing in government.

The survey collected data from 148 government professionals who are currently using cloud services or plan to launch cloud services efforts in the next 12 months. Nearly one-third of respondents came from state government agencies, and nearly as many respondents were from the federal government, executive branch, or Department of Defense. About one-third of respondents held IT management job titles, and one in five respondents were executive agency management, executive IT management or senior security management titles.

The greatest possible margin of error for the total respondent base (N=148) is +/− 8 percentage points. UBM Tech was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.
A Host of Challenges

Moving to the cloud is not always easy, as many organizations are discovering. It often amounts to a sea change in the way applications and computing capacity are acquired and how IT processes and infrastructures are managed. Many government agencies have been operating with the same legacy systems and software licensing arrangements for years, and the move to cloud-based services can be a jolt to management and end users alike.

The most commonly cited challenge or barrier of moving from legacy systems such as physical servers to cloud environments is concern about information security and privacy. About two thirds of the survey respondents mentioned that as a challenge, by far the most common response.

This focus on security should not come as a surprise, given that many IT executives inside and outside the government have long been skittish about how well protected data will be in a cloud environment. This is especially true of public cloud services in which hosted environments are shared among multiple tenants, and it’s not always clear how effective technologies such as identity and access management and encryption will be when it comes to public cloud services.

Applications Decisions

Whether it’s because of security, privacy or reliability issues, many government entities are limiting the types of applications they run in the cloud. One half of the organizations say they are not likely to move accounting, billing and other financial applications to the cloud any time soon.

Another application not likely to move to the cloud is information security technologies (47%). One curious finding of the research is that a number of respondents say they will not likely move applications such as help desk, sales and marketing, and project management to the cloud any time soon.
The State of Cloud Computing in Government

The types of applications government agencies are most likely to put in the cloud today include email and collaboration systems (54%); enterprise applications such as enterprise resource planning (ERP) and customer relationship management (CRM) (29%); citizen-focused applications such as Department of Motor Vehicles, social services and public health services (29%); and mobile applications (29%).

Cloud Benefits: Agility and Cost Savings
Government agencies are seeing — or expecting to see — a number of benefits from moving applications and systems to the cloud.

One of the advantages of the cloud most often mentioned by service providers is the greater flexibility enabled by these offerings, and in fact the benefit most commonly cited in the study is increased agility (42%). Considering that many people view government agencies as being slow-moving bureaucracies that take far too long to respond to the needs of citizens, it is easy to see how agencies would view increased speed and agility as a valuable benefit.

Also ranked high on the list of benefits is reduced costs (38%). By eliminating or reducing capital expenses such as the purchase of physical servers and storage systems, and taking advantage of the efficiencies of SaaS and other service-based IT offerings, agencies find they can run significantly more cost-effective IT operations by moving to the cloud.

Other benefits of the cloud include better use of internal IT resources (35%), increased scalability (32%) and improved collaboration (30%). (See Figure 6.)

A Need for Governance
Clearly, many government agencies have begun moving applications and systems to the cloud, or are planning to do so in the near future. This represents a significant shift in IT culture and processes for these organizations. And while the move can present significant benefits, it can also be fraught with challenges.

Having a strong governance program in place to monitor cloud service performance, reliability and security...
The State of Cloud Computing in Government

is extremely important, according to a majority (77%) of the government IT professionals in the survey. Only 4 percent say it's not at all important. (See Figure 7.)

**Figure 7: How important is it to have a strong governance program in place to monitor cloud service performance, reliability and security?**

Sometimes cloud governance is a broad-based effort. To help ensure optimal use of cloud services among U.S. federal government agencies, the government created the Federal Risk and Authorization Management Program (FedRAMP), a program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

This approach uses a “do once, use many times” framework that saves costs, time and staff needed to conduct redundant agency security assessments, according to the U.S. General Services Administration (GSA).

The goals of FedRAMP are to accelerate the adoption of secure cloud services through reuse of assessments and authorizations; increase confidence in security of cloud solutions; achieve consistent security authorizations using a baseline set of agreed-upon standards and accredited, independent third-party assessment organizations; ensure consistent application of existing security practices; increase confidence in security assessments; and increase the use of automation and near real-time data for continuous monitoring.

FedRAMP is needed because currently each federal agency manages its own security risks and provides security assessments and authorizations for each IT system it uses, even if other agencies have assessed, authorized and deployed the same system, the GSA says. The program is mandatory for federal agency cloud deployments and service models at the low- and moderate-risk impact levels. Private cloud deployments that are intended for single organizations and implemented fully within federal facilities are the only exception.

Despite the widespread acknowledgment of the importance of cloud governance, however, much work still needs to be done in this area, according to the research. Some 60 percent of the government entities say they do not yet have a governance program in place but are planning to create such a program.

This should not come as a major surprise, since so many agencies are just now moving to the cloud. What’s a bit more troubling is that 13 percent of the respondents say they have no plans to create a governance program. (See Figure 8.)

With a strong governance program in place to manage and monitor cloud-related efforts, and close working relationships with cloud service providers, government agencies and departments can ensure that they are getting the most out of the cloud and will continue to do so for years to come.

**Figure 8: Does your organization have a strong governance program in place to monitor cloud service performance, reliability and security?**

**How Can HP Help?**

HP delivers the industry’s broadest cloud solution portfolio, backed by world-class cloud consulting services. HP Converged Cloud harnesses the power of the cloud from development to delivery and seamlessly manages the experience across the hybrid IT environment.

The HP Converged Cloud — a common architectural foundation across traditional IT and private, managed and

---

Data: UBM Tech survey of 148 government professionals at agencies which currently have or plan to launch cloud services, December 2012
public clouds — helps organizations deliver information, applications and infrastructure anywhere they are needed.

Based on HP Cloud Service Automation and Converged Infrastructure, HP CloudSystem is tailored for the requirements of organizations at various stages of cloud maturity with three offerings: HP CloudSystem Matrix, which delivers Infrastructure as a Service (IaaS) for private and hybrid cloud environments, allowing users to provision infrastructure in minutes for physical and virtual environments; HP CloudSystem Enterprise, which lets organizations deliver self-service applications and adds advanced infrastructure-to-application life-cycle management; and HP CloudSystem Service Provider, which facilitates the deployment of public and hosted private clouds that deliver complete service aggregation and management.

Cloud bursting, a feature of HP CloudSystem, enables enterprises to broker and manage service delivery across multiple clouds from a single, integrated point of control. With cloud bursting, organizations can supplement their own local resources with resources from other cloud providers to meet extra capacity demands, to extend geographic reach, or to leverage specialized infrastructure service offerings.