Getting ahead in the cloud

The transition to cloud computing will be especially challenging for governments, given their myriad IT systems and their security, budgetary, and organizational constraints. We look at four critical actions they must take.

Kreg Nichols and Kara Sprague

Cloud computing—a computing model in which users purchase IT resources as a service, allowing them to take a pay-as-you-go approach—has deservedly garnered a lot of attention recently in both the private and public sector. Often referred to as simply "the cloud," cloud computing in many respects resembles a utility that supplies water or electric power: with the cloud, users can access IT resources at any time and from multiple locations, track their usage levels, and scale up their IT capacity as needed without large upfront investments in software or hardware. By enabling this flexibility, cloud computing improves IT efficiency—potential savings amount to 20 to 30 percent across the entire IT budget (including facilities, telecommunications, infrastructure, software, labor, and external services)—and makes IT organizations more agile. In the public sector, cloud computing will allow agencies to invest freed-up resources in mission-critical activities and become more responsive to new laws and regulations and to citizens' evolving needs.

Governments around the world have recognized the potential for cloud computing to transform the way they invest in, deploy, and access IT resources. The US federal government's "Cloud First" policy mandates that all federal agencies migrate at least three IT services to the cloud by mid-2012. The federal cloud-computing strategy, which the White House issued earlier this year, elaborates on this imperative and estimates that $20 billion—one-quarter of the

Kate Miller

US federal government's total IT spending—could potentially be reallocated to cloud-computing solutions.[1] In Europe, the vice president of the European Commission, who is also the European commissioner for digital agenda, declared that the region must become not just "cloud friendly" but "cloud active." Asia's public sector is also broadly embracing cloud computing. India's government, for example, plans to issue a cloud policy by 2012 and is seeking to deploy cloud technologies to deliver e-government services.

With the strategic imperative in place, government agencies must choose which parts of their IT environment, both legacy and new spending, to migrate to the cloud and, in each case, determine the appropriate cloud service and deployment model. (For descriptions of these options, see "Cloud basics," p. 53.) At the same time, they must create more flexible budgetary processes and funding models to support cloud-related investments and adopt new mind-sets and capabilities to realize the full benefits of cloud computing.

Based on our experience guiding clients through cloud-computing transformations and our understanding of the public sector's particular challenges, we see four critical actions that public-sector chief information officers (CIOs) must take in developing and implementing a cloud-computing strategy.

Choosing a service model

When confronting an extensive legacy IT environment, many CIOs find themselves asking, "Where do I start?" when considering what to migrate to the cloud and which service model to use. There is no single answer—the optimal service model depends on the specific requirements of each "workload" within an organization's IT environment. A workload is an integrated set of demands on IT, generally fulfilled through one or more applications. Human-resources management and financial management are two examples of workloads.

Rather than reviewing each of the potentially thousands of applications in its portfolio in detail, an organization should group applications into 30 to 50 workloads. For example, collaboration and messaging is a workload that encompasses the entire set of functionality relating to e-mail, calendaring, instant messaging, and shared workspaces. As a rule of thumb, each workload should be broad enough that a commercially available software package can deliver the required functionality. If the workload is defined too broadly, however, it will not be useful as the basis for the analyses described below.

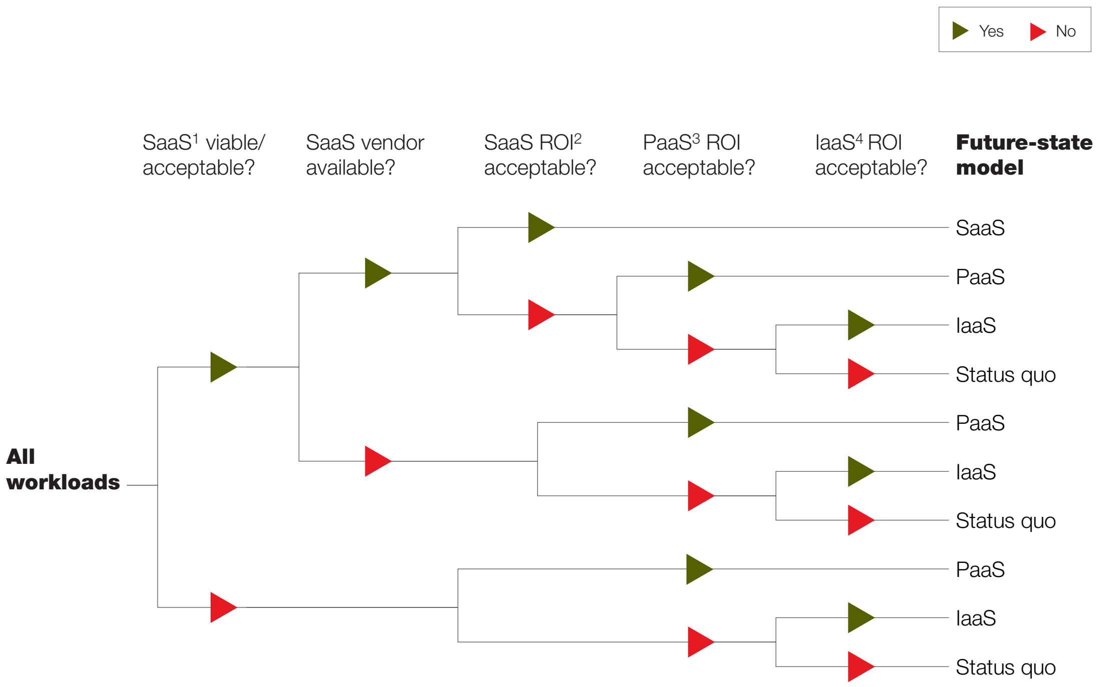
Once the agency has grouped its applications into workloads, the next step is to evaluate the performance and health of the current solution for each workload—that is, the degree to which the solution meets current and future needs. For example, does the solution work reliably on a daily basis? How easy and affordable is it to make changes to accommodate new requirements? Can the solution be rapidly scaled up to address unforeseen spikes in demand? Is end-user satisfaction with the solution high or low? The workloads that score low on this performance-and-health assessment are prime candidates for cloud migration.

For each workload it wants to migrate, the agency must then determine the optimal cloud service model: infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). Exhibit 1 illustrates a framework that can be used to make this decision. The structure of

[1] Vivek Kundra, *Federal cloud computing strategy*, Washington, DC, February 8, 2011.

Exhibit 1

A decision framework allows organizations to choose the optimal 'as a service' model.



[1] Software as a service.
[2] Return on investment.
[3] Platform as a service.
[4] Infrastructure as a service.

the decision tree will depend on an organization's priorities. For example, an organization that prioritizes speed of deployment and flexibility over the ability to customize solutions would look first to a SaaS model. The decision tree depicted in Exhibit 1 indicates a preference for SaaS adoption where possible. The organization first determines whether SaaS is a viable solution (for some public-sector workloads, for example, the security risks of placing data outside a firewall may simply be too high). If the answer is yes, the organization determines whether a SaaS vendor is available, and, if so, evaluates the economics of the SaaS model. For workloads that cannot be migrated to SaaS, the organization considers PaaS and IaaS. For some workloads, the best answer may turn out to be the status quo rather than migration to any cloud service model.

Selecting the right deployment model

Once an agency has chosen a service model, it must determine the appropriate deployment model (public, private, hybrid, or community) for each workload. The selection of the deployment model is typically based on requirements relating

Cloud basics

The US National Institute of Standards and Technology provides the following definitions for cloud service and deployment models:

Service models

Infrastructure as a service (IaaS) provides users with processing, storage, networks, and other computing infrastructure resources. The user does not manage or control the infrastructure but has control over operating systems, applications, and programming frameworks.

Platform as a service (PaaS) enables users to deploy applications developed using specified programming languages or frameworks and tools onto a cloud infrastructure. The user does not manage or control the underlying infrastructure but has control over deployed applications.

Software as a service (SaaS) enables users to access applications running on a cloud infrastructure from various end-user devices (generally through a Web browser). The user does not manage or control the underlying cloud infrastructure or individual application capabilities other than a limited number of user-specific application settings.

Deployment models

Private clouds are operated solely for one organization. They may be managed by the organization itself or by a third party, and they may be located on or off the user's premises.

Public clouds are open to the general public or a large industry group and are owned and managed by a cloud service provider. These are located off the user's premises.

Hybrid clouds combine two or more clouds (private or public) that remain unique entities but are bound together by technology that enables data and application portability.

Community clouds feature infrastructure that is shared by several organizations and supports a specific community of users. They may be managed by the user organizations or a third party, and they may be located on or off the user's premises.

Exhibit 2

Organizations can use a heat map to assess the security and manageability of workloads . . .

			1	2	3	4	5	6	7	8	9	10	11
Security	Confidentiality/ privacy	a. Commercial	🟨	🟨	🟥	🟥	🟨	🟨	🟨	🟨	🟥	🟨	🟨
		b. Personal	🟨	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟨
	Integrity	a. Authorization	🟥	🟥	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥
		b. Nonrepudiation	🟨	🟨	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥
	Availability	a. Accessibility	🟨	🟨	🟥	🟥	🟥	🟨	🟩	🟩	🟨	🟨	🟥
		b. Recovery	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟥	🟥	🟥	🟥
Manageability	Governance	a. Visibility	🟨	🟥	🟥	🟥	🟩	🟨	🟩	🟨	🟨	🟥	🟥
		b. Control	🟨	🟥	🟨	🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟥
		c. Organization	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟨	🟨	🟥
	Risk management	a. Uncertainty	🟨	🟥	🟨	🟨	🟩	🟩	🟩	🟨	🟨	🟥	🟨
		b. Exposure	🟨	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
	Compliance	a. Law	🟩	🟥	🟨	🟨	🟨	🟥	🟨	🟨	🟨	🟨	🟥
		b. Standards	🟨	🟥	🟥	🟨	🟩	🟩	🟩	🟩	🟨	🟨	🟥
		c. SLAs[1]	🟥	🟨	🟥	🟥	🟨	🟨	🟩	🟩	🟩	🟨	🟥

🟩 Non-inhibitor, lower needs

🟨 Moderate inhibitor

🟥 Strong inhibitor, higher needs

1 CRM[2]/ERM[3]/SCM[4] apps
2 Human-resources apps
3 Transaction management
4 Content distribution
5 Synchronous communication (eg, VoIP[5])
6 Asynchronous communication (eg, e-mail)
7 Other collaboration apps (eg, wiki)
8 Content creation/management
9 Engineering/app.dev./design apps
10 Information/systems management
11 Policy/audit/security

The requirements for each workload will vary among organizations

[1] Service-level agreements.
[2] Customer-relationship management.
[3] Enterprise risk management.
[4] Supply-chain management.
[5] Voice over Internet Protocol.

to IT security (confidentiality/privacy, integrity, and availability) and manageability (governance, risk management, and compliance).

We have found that concerns relating to IT security and manageability are the primary inhibitors to cloud adoption—even in the face of strategic imperatives mandating the adoption of cloud solutions. Public-sector CIOs should shift the discussion away from blanket generalizations about the unacceptability of cloud solutions to a careful examination of the relevant security and manageability issues. To facilitate this discussion, and in collaboration with key stakeholders (including the Cloud Security Alliance, a broad coalition that promotes best practices in cloud security), we have developed a framework for a comprehensive assessment of the IT security and manageability issues that organizations are likely to encounter (Exhibit 2).

. . . as well as the security and manageability of deployment models.

			1	2	3	4	5	6
Security	Confidentiality/ privacy	a. Commercial	🟩	🟩	🟩	🟩	🟥	🟥
		b. Personal	🟩	🟩	🟩	🟩	🟥	🟥
	Integrity	a. Authorization	🟩	🟩	🟩	🟩	🟨	🟨
		b. Nonrepudiation	🟩	🟩	🟩	🟩	🟨	🟥
	Availability	a. Accessibility	🟨	🟨	🟨	🟨	🟨	🟨
		b. Recovery	🟩	🟨	🟨	🟨	🟥	🟥
Manageability	Governance	a. Visibility	🟨	🟨	🟩	🟩	🟥	🟥
		b. Control	🟩	🟩	🟩	🟩	🟥	🟥
		c. Organization	🟩	🟩	🟨	🟨	🟥	🟥
	Risk management	a. Uncertainty	🟩	🟩	🟩	🟩	🟥	🟥
		b. Exposure	🟨	🟨	🟨	🟨	🟥	🟥
	Compliance	a. Law	🟩	🟩	🟩	🟩	🟩	🟨
		b. Standards	🟩	🟩	🟨	🟨	🟨	🟥
		c. SLAs[2]	🟨	🟨	🟩	🟩	🟩	🟨

🟩 Non-inhibitor, mature

🟨 Moderate inhibitor

🟥 Strong inhibitor, immature

1	Traditional IT[1]
2	Virtualized data center[1]
3	Private cloud
4	Hybrid cloud
5	Community cloud
6	Public cloud

[1] Could be either on- or off-premises, captive, or outsourced.

[2] Service-level agreements.

Each of the two heat maps in Exhibit 2 lists 14 elements of security and manageability on the vertical axis. Agencies should use the first heat map to record their workload-specific requirements for each of the 14 elements, considering the nature of the information managed by the workload, the roles or individuals with access to the workload, and the infrastructure requirements for running the workload. On the illustrative heat map shown here, the agency's concerns are mostly about authorization (for example, the verification required for users to modify or delete content), recovery (including capabilities for archiving and restoring data), and visibility (for example, monitoring and reporting capabilities). The second heat map evaluates the maturity of the solutions for each of the 14 elements offered by traditional IT, a virtualized data center,[2] and the four cloud deployment models. This evaluation shows that

[2] A virtualized data center is, like the cloud, a virtual infrastructure environment—but it does not offer the full suite of cloud-computing capabilities (such as real-time provisioning or advanced metering for charge-backs).

the agency's best choice would be a private or hybrid cloud, since these deployment models offer the most mature solutions for addressing the agency's most critical concerns.

We expect many public-sector agencies will initially choose a private or community cloud managed by a shared-service agency (such as the US federal government's General Services Administration). Indeed, in many cases, a private cloud will be more secure and manageable than existing public-sector IT systems because organizations can build security and manageability features into the overall architecture from the start, rather than having to add features to a legacy system. Public clouds may become a viable option for the public sector if they mature in their ability to address the security and manageability issues listed above.

Gaining flexibility in budgeting and funding

Public-sector organizations must make choices about their cloud-computing strategy in the face of rigid budgeting and funding cycles. Decision makers must typically secure funding years in advance, limiting their ability to redirect funding as technology advances or needs change. In cases in which funding is dedicated to individual projects rather than agencies or departments, it is difficult to invest in new IT platforms or architectures for which the business case is based on reducing the costs of future projects. What's more, individual agencies may not be able to afford the level of investment required to migrate to the cloud.

In its cloud-implementation plan, each organization must find creative ways to address existing budgeting and funding limitations. For instance, the funding request for a large IT deployment could include the cost of implementing a private cloud, as well as the costs of smaller projects that would take advantage of the new private cloud. Agencies may also consider working with IT vendors and service providers on financing options that would reduce the up-front capital needed to bootstrap public-sector cloud migrations.

The transition to cloud computing will require broad consensus within the government and tight collaboration among CIOs, finance leaders (chief financial officers, chief purchasing officers, and the central budgeting organization), and IT vendors. Public-sector CIOs can start the dialogue by developing a perspective on what the future-state IT model would be for their respective workloads if they faced no budgetary constraints. This future-state model can then form the basis for discussions between the finance and IT vendor communities regarding which workloads to migrate to the cloud and how to fund the migration. CIOs should seize the opportunity to take a fresh look at their vendor relationships. As their agencies transition to cloud computing, CIOs can explore relationships with new vendors staking a claim in the market, as well as pursue new arrangements with established vendors experimenting with ways to support cloud models.

Central budget authorities should take on the responsibility of coordinating and orchestrating the migration, aggregating requirements and demand from their constituent agencies, and interfacing with IT vendors to drive the development of solutions. These central budgeting organizations should spearhead a process to allocate appropriate funding to cross-agency IT efficiency programs. A more sustainable long-term solution will entail adopting a new service-based funding model for IT: rather than owning IT assets, agencies would share cloud services on a usage-based charge-back model. For smaller agencies in particular, this model would obviate the need to build new data centers.

Adopting new mind-sets and capabilities

In the technical transition from traditional IT to the cloud, IT staff will no longer have to procure the required hardware and software and then install, configure, and test the operating system and applications; instead, they will simply select the optimal configurations from a service catalog. The use of a service catalog—one of the most critical best practices for cloud technologies—transforms IT provisioning from a lengthy requirements-gathering discussion between IT and business users to a fast, menu-driven selection of the systems configuration most suited to the business requirements. Thus, IT organizations' current emphasis on technical skills such as software configuration or IT systems management will no longer be aligned with their needs. Instead, public-sector IT organizations must develop skills and capabilities in contract management, performance management, and continuous improvement.

The migration to the cloud will necessitate not just new skills but also a new way of managing and deploying IT staff and new core processes for IT operations. The traditional model for provisioning and accessing IT focuses on ownership of IT assets and uses input metrics (for example, the number of servers) to measure and manage performance. Cloud computing, in contrast, focuses on the utilization of IT services and relies on output metrics (such as service levels). Shifting mind-sets and behaviors from an emphasis on asset ownership to an emphasis on service utilization will not be trivial, and it will require a programmatic approach that includes training, incentives, and role modeling.

Another best practice in cloud computing is demand management through detailed reporting and charge-backs. These mechanisms are not only a means to improve funding—they also transform the role of IT by focusing business users on identifying which IT resources they truly require over time. No longer is IT merely the keeper of infrastructure and applications; it becomes a steward of business resources and fiscal responsibility.

• • •

By migrating to the cloud, public-sector organizations will be able to free up IT spend for reinvestment in mission-enabling activities or national objectives such as deficit reduction. With more agile systems and faster deployment times, they will be better at supporting key government operations and providing services to citizens. However, just as the benefits are great, so too are the challenges that must be addressed to achieve them. An investment today in the tools, capabilities, and processes required to surmount the obstacles to cloud migration is likely to yield a significant return in the long term.○

Kreg Nichols is a principal in McKinsey's Atlanta office. **Kara Sprague** is an associate principal in the San Francisco office.