Federal CFO Insights

Is the cloud in your sights?

Many technology decision-makers, notably CFOs and CIOs, are facing the reality that much of their departments' computing technology and data will likely end up "in the cloud." In fact, the cloud market is expected to grow from $40.7 billion in 2011 to $241 billion in 2020,[1] and the U.S. Federal cloud computing market may grow upwards of $10.4 billion by 2018 — about 11% of the Federal IT budget. Agencies are already grappling with the decision of what to move to cloud, when to move it, and how to transition from traditional computing models to the cloud. With big promises, and a plethora of players knocking on doors, what do agency executives need to know?

First, what is cloud? Cloud computing is an IT delivery model, that can help enable organizations not only to do things differently, but also to do different things. For this simple reason, many CFOs, along with other agency leadership, have a big stake in the game. Market forces (commodity equipment, low cost bandwidth everywhere, and major investments in automation and systems management tools), along with mandates, budget pressures and the need for modernization to meet ever increasing mission needs are rapidly changing the game. System management tools, for example, are key enablers of automating the business of IT, and they allow IT to deliver better control of much larger pools of computing resources (i.e. potential for many fewer stranded assets and reduced shadow IT within organization) — all managed on an entirely new business scale.

Decisions regarding cloud computing have impacts which are broader than just the Information Technology department, and require a productive working relationship between the CIO and the CFO. Concerns amongst Federal Government IT departments lean much more heavily toward security for government assets. Compliance-based decisions are more commonly used throughout the Federal Sector, rather than risk based decisions that are more commonly used in the commercial space.

For federal agencies, the real benefits of cloud, however, will ultimately come from an agency's increased agility in serving the mission, and the increased speed with which IT will be able to adopt technology advances. CFOs should consider a goal of supporting cloud as a means to shift IT expenditures to a lower, shallower economic curve while enabling mission growth and transformation.

Although the choice to pursue cloud computing is rather simple for some technology companies, other companies continue to struggle with how cloud can help their organization; recognizing the need for greater understanding. Likewise, for many public sector agencies, cost and budget pressures on top of mandates have caused a flurry of activities and high expectations for adoption from both mission and agency leadership. Two factors plague many organizations when it comes to cloud: (1) Education — not on the new technologies, but rather on the potential opportunities that can create positive disruption for both the business of IT and on mission operations, and (2) Implications on the back office — the downstream effect of such changes, especially for acquisitions.

Separating theory from reality

The concept behind cloud computing has existed for a long time. The basic idea is that an organization outsources the day-to-day management of IT resources or a capability (service provider owned and operated), and only buys what it requires based on base needs, then adjusts for peak or burst periods, thus creating a new acquisition paradigm. Also, and in contrast to traditional, on-premises technology, public cloud computing is delivered via the Internet.

In general, cloud computing looks like traditional hosting or outsourcing turned inside-out. With traditional government IT delivery, government furnished equipment and software is deployed highly customized to the mission or need — including customer Service Level Agreements (SLAs), followed by a mostly custom price from the hosting provider.

To the contrary, cloud service providers offer standardized services (and a published menu of prices) based on rigor and IT disciplines around a pre-determined set of offerings. The government clients must now profile and understand those offerings, and determine if the services are a close enough match to their IT services' needs; hence, the lower cost potential.

Although cloud is delivered via a utility model, many organizations may be assuming too much, treating it as a commodity buy. The market may not be there quite yet. For electricity, measured as a utility, a kilowatt-hour is a fairly stable unit. In the nascent cloud marketplace, few services are truly alike. For example, not all virtual machines nor all Software-as-a-service capabilities are completely equivalent across the marketplace. Varying qualities of service — including price/performance, resiliency for business continuity, and ease of use can differ greatly. More education is truly needed for executives to steer the organization's investments strategically, and for IT acquisitions to shift from a server specification to a services oriented procurement mindset quickly. Ultimately, the mission should be focused squarely on the capabilities provided and the quality of the service being delivered (same as with electricity), and not on the individual technology components underlying each phase in the supply chain

As an aside, cloud resources generally fall into one of four categories: public clouds, private clouds, community clouds, and hybrid clouds. Moreover, there are three basic uses (or delivery models):

1. Software (or Applications) as a Service (SaaS),
2. Platform (or IT Capabilities) as a Service (PaaS), and,
3. Infrastructure (virtual computing, storage and network resources as building blocks) as a Service (IaaS).

Many individuals think of SaaS when they talk about cloud computing, which is the provisioning of software applications and end-user capability on demand. The most common mission examples are collaboration, customer (citizen) service and digital citizen engagement.

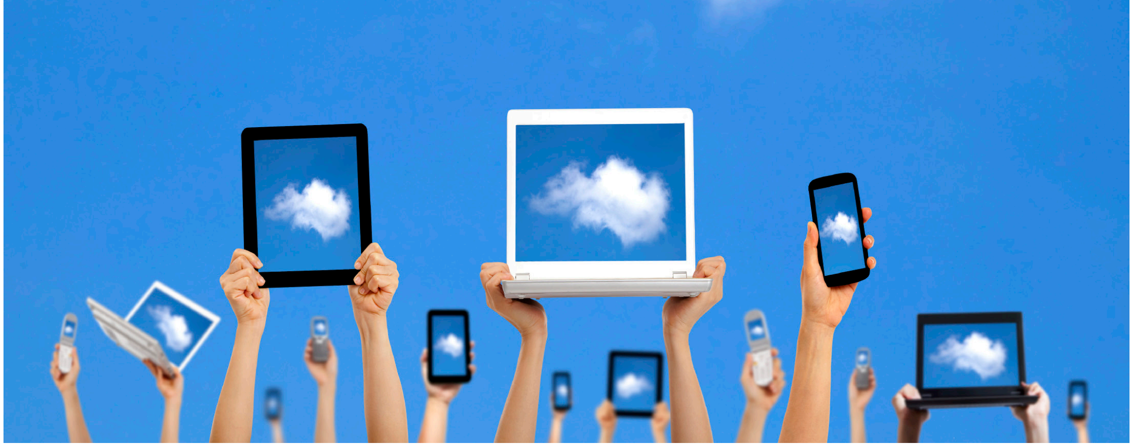
As with any initiative with notable uncertainty, agencies have started by piloting the use of cloud computing with either low-risk projects, or projects in which the on-premises computing resources would not normally be available. In reality, though, agencies are discovering that a number of programs are using unapproved cloud computing resources: program managers and government employees are opportunistically identifying technology to meet their business needs and contributing to their ability to complete tasks and satisfy mandates. Unlike the lack of penalties in the commercial space, government agencies are under the constant compliance pressures in addition to the added oversight of budget, accounting, and Inspector General offices.

The exposure to the organization for non-compliance can be high, and the practice of deploying unaccredited solutions does raise several technology governance issues:

- What would happen in your agency when programs purchase their own cloud computing technology to satisfy mission needs?
- Who has to answer for lapses in compliance?
- Have you re-examined IT governance and organizational agility as it relates to the potential of cloud computing?
- Have you examined the risk exposure related to mission activities and incorporated this into IT and organizational governance?

How do you know if cloud is right for you?

When evaluating an approved use of a cloud service, the relative costs, benefits, and risks should be examined. The benefit cited most often in interviews with select commercial CIOs and CFOs is the agility that the cloud provides; businesses are not saddled with technology infrastructure and can react more quickly to changes in technology. Many government CIOs have been promised cost savings to address tremendous budget constraints and growing demand. However, many forward- looking



CIOs are looking to cloud to increase IT's responsiveness to the mission and to quell costs as mission demands on IT continue to grow.

CIOs are charged with balancing the ever growing cyber threats in the new world of cloud computing. Considering these threats, interviewed CFOs and CIOs raised the following security concerns as they relate to cloud:[2]

- How do I know that my data is safe?
- How do I know where my data is stored?
- Is my data backed up? How will we retain control of our data, and can it be audited?
- How do I know that the provider's security controls truly meet or exceed my own? What guarantees should the cloud vendor provide?

Another concern relates to vendor dependency and potential "end game" scenarios. For example, what does an organization do when and if it needs to move from one cloud service provider to a different one?

On a positive note, CFOs and CIOs are looking to cloud vendors that may be able to provide better security and higher levels of performance than they can deliver internally. For such vendors, this is their primary line of business — and brand, and as such, they strive to hire employees who are experts in various aspects of security and their software. The vendor also has an economic stake in providing high-quality, secure, reliable services; if that cloud service fails, that vendor will quickly lose clients and revenue.

Finding your cloud comfort level

The basic message for agencies is to become comfortable with cloud computing. Determine what type of applications are candidates for the cloud and which will not be moved until the distant future. Initially, choose applications that have low risk associated with them, or choose those that have a business need that cannot be fulfilled using traditional computing services. One critical aspect is to prepare for uncertainty, and to understand contract service level and security agreements with the vendor and prepare for end-game scenarios. While these contractual agreements will not prevent problems, they help organizations to understand their risks and better plan continued operations.

The Government may not be able to keep pace with commercial companies in changing and adopting new technology without looking at alternative options. Agencies should find new ways to satisfy requirements and allow the transfer of and growth of leading practices to satisfy mission needs. Agencies should drive efficiency on non-mission essential activities, and enable greater effectiveness and new capabilities to help meet ever increasing mission IT demands. By assessing on-premises applications along four dimensions — customization required, process complexity, application resiliency, and security risk — decision-makers can perform a preliminary ordering of which applications to move to a cloud environment, and when.

- **Customization required:** The extent that software or technology customization is required to align with processes or to satisfy business requirements. Instead of starting from a blank sheet, programs can now assemble mission capabilities from building blocks of services.

- **Process complexity:** The degree that organizational processes are inter-related with technology amplifies change management implications to moving to a different technology platform and delivery model. Decomposing needs in terms of services instead of systems will help ease the transition.

- **Application resiliency:** The uncertainty of "when might the service NOT be available" and the tendency to label all IT as "mission critical" further implies the shift from systems to services. Factoring in a quality of service measure will become critical components of the acquisition process.

- **Security risk:** The consequences of "what could go wrong" and the sensitivity of the data that resides in the application. Risk aversion among decision-makers also plays a role. Government is challenged with managing to risk versus compliance — and the need to balance the two is complicated by current processes and regulations.

The less prevalent these four dimensions are as they relate to technology applications, the earlier in the transition sequence a given application may be for moving to a cloud environment.

Is it time for cloudy vision?

CIOs' and CFOs' alignment around the cloud decision (as a viable and desired IT delivery model) can help them position where cloud is appropriate for their agency. An agency's cloud strategy should be supported across the agency's leadership. It's no longer just an "IT thing." The approach to determining whether cloud is appropriate involves assessing technology in the context of mission purpose and risks.

One recommendation is to start small and sample technologies with less risk and related influences on the agency's operations. Following the pilot approach and with greater comfort with cloud, an Agency can continue to shift capabilities to cloud by using an appropriate assessment-based road map.

Adopting cloud is a balancing act of trust, transparency and control. When an Agency has developed sufficient trust with a provider, and the provider can deliver sufficient transparency throughout ongoing operations, then the CIO or program director may consider shifting control of those IT services to a cloud services provider. With CFOs' and CIOs' evaluation of governance and how the availability of cloud services can impact their ability to serve the mission, they can at least help their agencies drive with the fog lights on.

Endnotes

1. Forrester Research, April 2011, "Sizing the Cloud" by Stefan Ried, PhD, Holger Kisker, PhD.
2. Interviews conducted as part of Deloitte's CFO Program Fellows & Scholars initiative which connects Deloitte practitioners ("Fellows") and professors from universities ("Scholars") to develop CFO relevant insights and research.

— Parts of this article were excerpted from a previous CFO Insight article, CFOs and CIOs: How do you know when to reach for the clouds? by Severin Grabski, associate professor and senior faculty advisor for Instructional Technology, Michigan State University; Daniel Root, manager, Deloitte Consulting LLP; and Ajit Kambil, global research director, CFO Program, Deloitte LLP.

Primary contacts — a public sector perspective

Paul Krein
Specialist Leader — Federal Office of the CTO
and Cloud Community
Deloitte Consulting LLP
pkrein@deloitte.com

Adam Cranmer
Sr. Consultant — Federal Business Risk
Deloitte & Touche LLP
acranmer@deloitte.com

Contributors
John Lee, Nathan Holst

Deloitte *Federal CFO Insights* are developed with the guidance of Roger Hill, Principal, Federal CFO Program Leader, Deloitte & Touche LLP; and Philippe Podhorecki, Manager, Federal CFO Program, Deloitte Consulting LLP.

About Deloitte's Federal CFO Program

The Federal CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help Federal finance leaders stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a leader's career — helping Federal CFOs manage the complexities of their roles, tackle their agency's most compelling challenges, and adapt to strategic shifts in the public sector environment.

For more information about Deloitte's Federal CFO Program, visit our website at www.deloitte.com/us/FederalCFO.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2013 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited.