



Cloud Computing

Full Strategic Report at:

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



Inside:

To Cloud or Not to Cloud?, s2 • Keeper of the Federal Cloud, s5
Maneuvering Through the Cloud, s7 • Safety in the Clouds, s8
17 Steps to the Cloud, s9



To Cloud Or Not To Cloud?

The answer is Yes says Federal CIO Vivek Kundra! But public and private Cloud experts agree there is still much work to be done to get the Federal Government up in the Cloud.

Cloud Computing!

To evangelists it is “going where no man has gone before”; to skeptics it just “puts us behind the 8-ball to secure data”; and to many IT vets, it is “déjà vous all over again” taking us back to the days of mainframes and dumb terminals.

To Federal CIO Vivek Kundra, Cloud Computing is fundamental to the technology strategy being developed by the Obama Administration of how to get more efficiency from IT, while expanding applications and reducing costs.

To help him, he has enlisted the aid of the Federal CIO Council to formulate a Federal Cloud strategy. And to help him build the Federal Cloud, he has chosen GSA to be the point agency and Patrick Stingley to be the CTO of The Federal Cloud.

Stingley was just one of the Cloud experts, providers and potential government users that came together for the Cloud Computing Summit, April 29, 2009 in Washington, DC.

“My job is to make sure as we plan the Federal Cloud, we have the technical knowledge to carry it off,” Stingley said.

Stingley said that Cloud could be used for email, portals, remote hosting and other applications that would grow in complexity as our experience of working securely in the Cloud grows. “No single approach will work. No single approach or architecture can meet all of the government’s needs, so a tiered approach will be provided.”

NIST’s Peter Mell told Summit attendees that his agency’s working definition of Cloud Computing is “a pay-per-use model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.”

Cloud Fundamentals

“Every generation rediscovers the power of interchangeable parts; that’s what Cloud is,” Stingley proclaimed.

“Where I came from in our data center we have 5 different operating systems, all kinds of applications, 3 or 4 DBMS with multiple versions. I’d have to have 5 different stacks – one for each OS,” Stingley explained.

“What Cloud brings to the table is commodity hardware

that is the same throughout the Cloud Center. The premise of Cloud is to reduce the variability and the number of things you have to support; and by doing so that’s where your economy comes from.”

Stingley said that the goal is to build a distributed Cloud that can host applications, while at the same time providing capabilities for those applications and information that can’t – mostly for security reasons – move into the Cloud.

“A Cloud is built using commodity hardware and that’s the real key architectural tenet,” said Stingley. But even if the Cloud were ready to occupy today, the Federal government is not ready to move in. “Most applications couldn’t go there because of code and OS. What we need to do is provide a suite of services in order for people to begin a migration strategy to the Cloud.”

Why Cloud Now?

For some, Cloud is just a 21st century version of centralized mainframe computing. But philosophy aside, why is Cloud Computing a movement whose time has come?

IDC’s Teresa Bozzelli said there are two reasons. “First in government specifically, it is a cost constrained environment. As technology advances quickly to create (and refresh) infrastructure quickly gets pricy. It also can’t be done fast enough. Cost is opportunity to look at new models.”

Another reason is driven by a convergence of the amount of information we need to analyze better and the Administration’s demand for openness, transparency and accountability.

It’s driven by the need for more information and how Web 2.0 allows us to engage differently; it’s about technologies coming together such as virtualization and network bandwidth; and being able to lower costs and be faster in our deployments Bozzelli explained.

What all this is for said Bozzelli is with Cloud we are able to deal with larger amounts of data from different sources and engage collaboratively through the web to compress the timeline of knowledge sharing and decision management.

Rod Fonticilla from Booz-Allen agreed with Bozzelli about lower costs, but added while it is a better way to utilize under-used servers and resources what is really exciting about Cloud is what you can do with Cloud that you couldn’t do before.

Controversy In The Clouds

"It will cost money to move to the cloud; this isn't going to be free," said Patrick Stingley, CTO of the Federal Cloud. "Most applications are not capable of getting there so there will be retooling costs."

Retooling costs are just one of the obstacles in the way of Cloud Computing implementation. Public and private Cloud experts such as CSC CTO Yogesh Khanna point to 7 areas where solutions need to be found.

1. Vendor Lock-in – most service providers offer proprietary offerings thus an app built for one Cloud cannot be ported to another.

2. Lack of Standards – Stingley asserts there wouldn't even be Cloud Computing without standards. But that aside, if there were clear standards, then NIST wouldn't be getting involved. A lack of standards feeds the vendor lock-in problem because every provider uses a proprietary set of access protocols and programming interfaces for their cloud services.

3. Security & Compliance – There are limited security offerings for data at rest and in motion and no agreed upon compliance methods for providers to get their offerings certified (like common criteria or FISMA).

4. Trust – Cloud providers today offer limited operational visibility, if any. That won't work for the government; complete transparency is a must.

5. Service Level Agreements (SLAs) – As they say, the "devil is in the details". Enterprise class SLAs (for example four/five 9s availability) are necessary for most services.

6. Personnel – Many of the public clouds span the Globe, and thus use a Global workforce. This poses a serious problem for agencies that may wish to leverage the cloud, but have sensitive data.

7. Integration – Lots of work needs to be done to integrate cloud providers' services with enterprise services and make them work together. The task of identifying the most cost effective, secure, and reliable cloud services and orchestrating them for enterprise applications and/or users is complex.

Cloud Manifesto (www.opencloudmanifesto.org)

Then there is the Cloud Manifesto signed by more than 175 organizations and growing. The Open Cloud Manifesto establishes a core set of principles to ensure that organizations will have freedom of choice, flexibility, and openness as they take advantage of cloud computing.

Backers of the Manifesto are calling for "an objective, straightforward conversation about how this new computing paradigm will impact organizations, how it can be used with existing technologies, and the potential pitfalls of proprietary technologies that can lead to lock-in and limited choice. This document is intended to initiate a conversation that will bring together the emerging cloud computing community (both cloud users and cloud providers) around a core set of principles. We believe that these core principles are rooted in the belief that cloud computing should be as open as all other IT technologies."

And by the way, while Stingley did not say he backed the Manifesto by name, he did tell the audience that collaboration and openness are fundamentals for the Federal Cloud. So it looks as if proprietary Cloud providers are going to have to find a way to be interoperable.

Finally, check out the McKinsey Report. As reported in TechCrunch, McKinsey & Company released a report, "Clearing the Air on Cloud Computing," April 15 that claims that large corporations could lose money through the adoption of cloud computing. The report paints cloud computing as over-hyped and maintains that cloud computing services like Amazon Web Services (AWS) overcharge large companies for a service the companies could do better on their own. The study also says that while cloud computing is optimal for small and medium-sized businesses, large companies will spend less if using traditional data centers. Check out www.techcrunch.com for a lot of comments both pro and con.





65 Years of NY Times

“What excites people are the unlimited computing power and the ability to answer questions you couldn’t do before because by being able to boost computing power on demand, query time will be lowered,” said Fonicilla.

Fonicilla told the audience how the NY Times wanted to put every article it had printed from 1845 to 1912 on PDF on the web. They realized it would take years using their own IT infrastructure. So, the Times bought services from the Amazon Cloud and were able to take use the increased computing power to do the entire job in 24 hours for a cost of \$240.

**The five key inherent characteristics
common to all types of Cloud
Computing are: on-demand self-service;
ubiquitous network access; location
independent resource pooling; rapid
elasticity; and pay per use.**

Just imagine the implications for the Library of Congress and the National Archives. On January 20, 2009 200 million emails from the Bush Administration came to National Archives according to Jason Baron, an Archives attorney.

“They came on servers – real hardware and software – not in the Cloud,” explained Baron. “We will have a billion emails coming from Obama. The volumes are staggering; and the paradigm will change as data moves from servers inside government walls and is outsourced in the Cloud or somewhere else.

Challenges and Visions

Cloud Computing can be thought of as either a revolution or an evolution. Either way it signals a clear desire for the Federal government from owning its IT assets to buying IT services from a third party vendor and hosting them in a public, private or community Cloud.

Baron told the Summit there is a tension between government in the sunshine and CIOs actually moving their data to somewhere else - outside their physical control. “Who owns the servers? Are they in the U.S. or abroad? This raises profound challenges.”

One challenge is that when passing the 1950 Federal Records Act, Congress did not anticipate Cloud Computing the lawyer said, but was clear about the definition of a record and what that means as to how they are archived.

“According to the law, the definition of a Federal record includes information created and received by government agencies that are in machine readable form,” explained Baron. “So anything electronic or digitally created and received in agency is a record. The challenge is whenever we are thinking about Web 2.0 and Cloud Computing, there is an institutional driver against parking these records beyond the traditional IT structure or using a web-based application to get at these records.”

That poses a challenge as to how to meet security requirements, while meeting public and Congressional demands for transparency. And there are others who are skeptic about the promises of Cloud Computing.

Burke Cox, CTO of Platinum told 1105 Government Information Group Custom Media that “Cloud Computing hype may create false hope for those agencies who have never stared down their real challenge of an inadequate enterprise architecture.”

Further he said “there are more barriers to Cloud adoption now than benefits. For most agencies enabling SOA is a better first step that will prepare them for the maturation of a service oriented architecture infrastructure – what we call a “cloud” – as vendor and service solutions improve.”

What Cox advocates is real. Implementing Cloud Computing will not happen by the time the next budget cycle comes around. However, when solved, government will participate in a plethora of public Clouds and private Clouds. And you’ll see community Clouds that serve niche constituencies and even hybrid Clouds where you can abstract applications or services through a combination of in house infrastructure or reaching out to many multiple Clouds.

Down the road, interoperability standards will emerge so the application won’t know the difference and just go out and consume the infrastructure services from various resources.

Stingley said it takes twice the lifespan of a typical system to fully embrace a new technology. “We can start moving stuff now but the majority of the government is not position to use the Cloud effectively.” He projects that the Federal Cloud will offer a range of services to allow agencies to migrate gracefully, say over 20years – which happens to be twice the 10 year lifespan of typical system. □



Keeper of the Federal Cloud

Patrick Stingley, CTO of the Federal Cloud and his team will construct a Federal Cloud to host applications that work well in a Cloud environment and offer platform services; it will be FISMA certified so all agencies can use it.

After you “talk the talk” about a Cloud Computing strategy and building a Federal Cloud, you actually have to “walk the walk” and do something about it.

Self proclaimed propeller-head and geek Patrick Stingley, CTO of the Federal Cloud is in charge of doing something about it.

“I’m the CTO for the Federal Cloud,” Stingley told the audience at the Cloud Computing Summit. He said the Administration designated GSA as the lead, but he also made it clear that this is not GSA’s Cloud. “Everybody has part of the Cloud, it is the Federal Cloud.”

What you need to know most about Stingley is that he is ably qualified to do the job. He’s a long time government IT manager that takes his love of IT home. In his spare time at home he works using three types of virtualization systems and a NAS in his basement. “I’m the guy who builds the stuff. That’s what I do. My job is to make sure as we plan the Federal Cloud, that we have the technical knowledge to carry it off.”

A Broad Working Definition

No single approach or architecture can meet all of the governments needs so a tiered approach will be provided. “Our definition of Cloud includes more that you’ll find in Wikipedia. We are going to have IT environments that allow people to be able to bolt stuff in such as a DBMS, rent server space as needed, as well as able to use purist Cloud definition stuff,” Stingley explained.

His team will construct a Cloud to host applications that work well in a Cloud environment and offer platform services; it will be FISMA certified so all agencies can use it.

Stingley said the Federal Cloud will eventually offer tiers of services.

Tier 1 Services are all of the free services that are already out there for Web 2.0 and Social Networking such as Facebook. Since government doesn’t own these services, it needs fair use agreements for their use. GSA has just finished those agreements.

Tier 2 Services is when GSA will be making the heavy investment in contracts to provide Infrastructure as a Service, Platform as a Service and Storage as a Service.



Down The Road

“We are looking down the road at Portal services,” said Stingley. “One of key components to getting everybody on the Cloud is Portal services.”

For example according to Stingley if you are writing in Pearl or PHS and other agencies are doing the same, it would make sense to put up a Portal so you can write your code and share your code so the other people can see what you’ve written. They might help you fix a bug so quality of code improves and facilitates move to the Cloud.

Stingley also sees personalized storage as a key component on the Cloud. He calls them Web folders because it makes sense to everybody. If these folders are on the Cloud, then staff can you can be anywhere and get back to your files. This makes it much better for telework and COOP because it puts workers in position to get folders from home they can’t get by going through their VPN.

Stingley calls email the “killer app” and said Cloud will result in getting better value from your IT assets. For example, workflow could be monitored and there could be automated reporting of IT inventory and then we can offer some business intelligence tool so you can do an analysis...

“Database as a service is big,” said Stingley. “Eventually



we will write apps and talk to web service and powering it will be production quality relational database; we have to stop being driven by new releases of databases. If go to a web service DBMS, then you fix it once and won't have to spend ten years rewriting all your code and paying every time there is an update."

Cloud Architectural: Platform Unspecific

The first is to be built on an open architecture with commodity products.

Stingley said they are going to create a set of vehicles, so if you want to go to company here is the price, here is what it does, here is suite of services. Other people will be able to reuse that same contract vehicle and that's where the collaborative portal comes in to play.

"Within the Cloud we need the collaborative portal, the authentication, email service, workflow," Stingley noted. "We need a standard set of interfaces and APIs to use the stuff in the Cloud."

Stingley also advocates the Federal government become less platform specific. "This will allow us to build applications we can use for an indeterminate time because when we tie apps to specific hardware OS and specific languages that require rewriting when one or another get updated, we spend a lot an awful amount of money just to maintain our current functionality."

"We need to go to the Cloud and abstract ourselves from the hardware and OS, from the platform and doing so we will create a code base for ourselves that will allow us to continue to use software for a long period of time."

Culture Shift

As usual moving to the Cloud is not a technology issue, though there are issues to be overcome. But they pale to the shift in culture needed.

"You have a culture that needs to change and to embrace the Cloud and embrace the concept of sharing," urged Stingley. "Cloud computing is a shared service; we need to learn how to share; it's not a hard concept, but we can't agree how to do it."

A good example of this is the Federal Cloud according to Stingley. "The Federal Cloud is being put together; it is a pilot and GSA has been designated to build this."

"I've been trying to figure out what we should call this? If you want to go the Federal Cloud where would you go? Would you go to Cloud@gsa.gov? Well no, it's not GSA's Cloud; it's a shared Cloud, so www.Cloud.gov?"

Stingley said "no, it's whatever your agency is dot gov; it's your agency; it's your infrastructure; it is part of your infrastructure; not GSA's, but it's hard to get your head

around it sometimes."

The concept is Cloud is the about shared services. "We need to move away from that concept of vendor specific and platform specific implementations and take a page from the open source community and collaborate," counseled Stingley.

Easier said than done; so how are we going to get to the Cloud?

"None of the agencies that I'm aware of in the federal government could use a Cloud today," said Stingley. "Maybe put a website up to the Cloud, but most of the apps we have today are not portable enough to move into the Cloud if we had it today."

One way to go to the Cloud is for each agency to rewrite its own code and that's probably what we would do if left our own devices. A better approach and one that can have success explained Stingley one that embraces the Open Source model and puts up a collaborative space so various pieces move on to a Cloud, they share.

"But we need to do this as a government, not as a whole bunch of little armed camps," warned Stingley. "That's a big change, but it's our way to the Cloud." □



Maneuvering Through The Cloud

To cut through all the Cloud hype, NIST has come up with some terminology that clears up foggy Cloud visions.

For many, Cloud Computing seems as if it just appeared out of thin air – the latest IT fad in what seems an endless stream of silver bullet solutions to organize, manage and deliver government IT resources.

But Cloud Computing has solid roots in the early days of the Internet when computer scientists drew the network as a Cloud and didn't care where the messages went, because the Cloud hid it from us said Peter Mell, Project Lead for the NIST Cloud Computing team.

Mell told the Cloud Computing Summit audience that the first Cloud appeared around networking (TCP/IP abstraction) and the second Cloud around documents (www data extraction). The emerging Cloud abstracts infrastructure complexities of servers, applications, data, and heterogeneous platforms.

Basic Formations

There are a number of different definitions of Cloud Computing (see sidebar), but they all have five common characteristics including according to Mell: on-demand self-service; ubiquitous network access; location independent resource pooling; rapid elasticity; and pay per use. And some would add a sixth -multi-tenancy.

Mell then told the audience there are three Cloud delivery models; and to be considered "Cloud" they must be deployed on top of Cloud infrastructure that has the key characteristics:

- **Cloud Software as a Service (SaaS)** – use a provider's applications over a network
- **Cloud Platform as a Service (PaaS)** – deploy customer-created applications to a Cloud
- **Cloud Infrastructure as a Service (IaaS)** – rent processing, storage, network capacity, and other fundamental computing resources

Finally Mell said you can have an internal or external Cloud depending upon which of the four Cloud deployment models you use:

- **Private cloud** – one that your enterprise owns or leases
- **Community cloud** – a shared infrastructure for specific community such as health care
- **Public cloud** – sold to the public, mega-scale infrastructure such as Amazon or Google
- **Hybrid cloud** – composition of two or more clouds

continued on page s10

Spinning Clouds

Cloud Computing offers the prospect of dramatically increasing your computing power, being able to balance workloads with demand and paying only for the services you use. Here is how a few of the leaders in the Cloud Computing marketplace define Cloud.

NIST

A pay-per-use model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.

Gartner

A style of computing where massively scalable, IT-enabled capabilities are provided "as a service" across the Internet to multiple external customers.

IDC

An emerging IT deployment, development and delivery model enabling real time delivery of products, services and solutions over the Internet.

University of California - Berkeley

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the Data Centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The Data Center hardware and software is what we call a Cloud.

Cloud Manifesto

The key characteristics of the cloud are the ability to scale and provision computing power dynamically in a cost efficient way and the ability of the consumer (end user, organization or IT staff) to make the most of that power without having to manage the underlying complexity of the technology. The cloud architecture itself can be private (hosted within an organization's firewall) or public (hosted on the Internet).



Safety In The Clouds

A Trusted Cloud is absolutely necessary to meet all Federal security requirements and to instill confidence in the confidentiality, integrity and availability of Cloud services and associated data.

You have security concerns – and rightly so.

When your applications are run from the Cloud; when your data is stored in the Cloud; and when you don't know who else is sharing the same Cloud resources as you, it can make you a little skittish – perhaps even reluctant to even consider Cloud Computing for your organization. You may think you are giving up control and perhaps security over your data.

While some sensitive data will never move to the Cloud, for some information – especially if it faces the public – you are going to just have to get over it.

CTO of the Federal Cloud Patrick Stingley put it this way: “When when the guy running the largest organization in the planet is behind Cloud Computing, that's it.”

Cloud Advantage or Disadvantage

NIST's Peter Mell explained that there are some security advantages to Cloud. By shifting public data to an external Cloud, you reduce the exposure of the internal sensitive data and Cloud homogeneity makes security auditing/testing simpler. He also said Cloud enables automated security management and provides redundancy and Disaster Recovery advantages.

On the other hand Mell said security challenges revolve around trusting vendor's security model; the customer inability to respond to audit findings; how to obtain support for investigations; indirect administrator accountability; proprietary implementations can't be examined; and of course the “biggie” – loss of physical control.

Trusted Clouds

So, what are you to do? “In the public Clouds people tend to have no control over who touches or who sees their data,” CSC CTO Yogesh Khanna told the Cloud Summit, “and those things inherently build some angst, some anxiety among the CIOs in the federal community.”

Khanna said on the other extreme are the private Clouds (which the purists will tell you is an oxymoron because there is no such thing as a private Cloud) where you own all the assets and you control exactly where your data resides. But since everything's behind your firewall, you don't really get the economies of scale that Clouds are supposed to bring to the table. But you get all the appropriate securities.

What Khanna is proposing is a middle ground which he defines as “Trusted Clouds” which are really Clouds for a

Digital trust is completed with evidence-based confidence that systems operate as advertised, and that no unadvertised functions are occurring and that digital trust depends not only on security features but also on the ability to deliver evidence about feature operation with full transparency of control and result.

community where that community of users could be defined by whoever is delivering those services.

Khanna defined trust as the assured reliance by one party on the future behavior of another party. “Technology is indeed the source of digital trust, however the features and functions performed in the name of “security” for transactions and data are just the beginnings of digital trust,” explained Khanna.

He told the audience digital trust is completed with evidence-based confidence that systems operate as advertised, and that no unadvertised functions are occurring and that digital trust depends not only on security features but also on the ability to deliver evidence about feature operation with full transparency of control and result.

So to be safe in the Cloud you need to be part of Trusted Clouds. Khanna said “a Cloud that harmonizes the security for transactions and data with comprehensive transparency of control and result such that it conveys evidence-based confidence that systems within its environment operate as advertised, and that no unadvertised functions are occurring is a Trusted Cloud. Services rendered via a Trusted Cloud are ‘Trusted Cloud Services.’”

“A Trusted Cloud is not only possible,” exclaimed Khanna, “but absolutely necessary to meet all the Federal Government requirements and to instill confidence in the confidentiality, integrity and availability of Cloud services and associated data.” □



17 Steps To The Cloud

Cloud Computing expert Dave Linthicum tells you how to scale the clouds step-by-step.

What the government IT manager needs when getting ready to embark on their migration to the Cloud is a good template; one that defines a proven roadmap to follow.

What Cloud Computing Summit attendees learned (and now you) is that help is on the way. Cloud and SOA expert Dave Linthicum has developed a step-by-step plan to help you scale the heights. He goes through them meticulously in his new book *Cloud Computing and SOA Convergence In Your Enterprise: A Step-by-Step Guide*.

At the Summit, Linthicum outlined the plan. Afterwards he told 1105 Custom Media you can consider Cloud Computing the extension of SOA out to Cloud-delivered resources, such as storage-as-a-service, data-as-a-service, and platform-as-a-service.

“The trick is to determine which services, information, and processes are good candidates to reside in the Clouds, as well as which Cloud services should be abstracted within the existing or emerging SOA,” Linthicum said.

Do Your Homework

Linthicum says to start with your Architecture and make sure you understand your organization’s business drivers, information already under management, existing services under management and your core business processes.

In that way you can begin to look where Cloud Computing is a fit according to Linthicum. You can look to migrate to the Cloud when:

- The processes, applications, and data are largely independent.
- The points of integration are well defined.
- A lower level of security will work just fine.
- The core internal enterprise architecture is healthy.
- The Web is the desired platform.
- Cost is an issue.
- The applications are new.

While a Cloud candidate doesn’t have to meet every one of the criteria above, it does show that there are caveats – not all computing resources should exist in the Clouds and that Cloud is not always cost effective.

It shows you need to do your homework before making any move. So, Cloud may not be a fit when the opposite conditions exist:

- The processes, applications, and data are largely coupled.
- The points of integration are not well defined.
- A high level of security is required.
- The core internal enterprise architecture needs work.



Cloud Steps

In his upcoming book *Cloud Computing and SOA Convergence In Your Enterprise: A Step-by-Step Guide*, Cloud and SOA guru, Dave Linthicum, to successfully move to the Cloud you need to follow these 17 steps - without skimping on any.

- Access the business.
- Access the culture.
- Access the value.
- Understand your data.
- Understand your services.
- Understand your processes.
- Understand the Cloud resources.
- Identify candidate data.
- Identify candidate services.
- Identify candidate processes.
- Create a governance strategy.
- Create a security strategy.
- Bind candidate services to data and processes.
- Relocate services, processes, and information.
- Implement security.
- Implement governance.
- Implement operations.



- The application requires a native interface.
- The cost is an issue.
- The application is legacy.

At the Cloud Summit, Linthicum told the audience external Cloud services should function like any other enterprise application or infrastructure resource and Cloud resources should appear native.

It goes without saying that as with any purchase, you

When you have finally chosen an application to Cloud test, there are providers who have 90 days of free Cloud pilots. In that way you can truly minimize the risk.

should evaluate Cloud providers using similar validation patterns as you do with new and existing Data Center resources. You know there is going to be hype, but Cloud is not rocket science. If you feel you need to, hire a consultant as a trusted advisor.

Pilot Through The Cloud

When you have finally chosen an application to Cloud test, there are providers who have 90 days of free Cloud pilots. In that way you can truly minimize their risk by saying “let’s try it out and if happy you have the option to continue and turn that into a contract.

CSC’s Yogesh Khanna told Summit attendees to embrace the business models that Clouds offer. Security barriers are all addressable not only through technology but also through policies. Be wary of the fact that there are a lot of Clouds out there. Some of the Public Clouds (e.g. Google’s or Salesforce.com) are proprietary in nature. Because this landscape is changing so fast, it is very important to maintain a level of flexibility and don’t fall prey to “vendor lock-in”.

“Look for some level of transparency that allows you to be certain exactly where your data is and who is seeing it,” said Khanna. “Have the flexibility to see where your data is at any given point and be able to monitor the health of the Cloud that’s delivering those services to you.”

Finally Robert Ames from IBM told the audience, “The message is by following the fundamental things – the three legged stool of technology, processes and organization, you will achieve transformation.”

“If you ignore process and organ you could spend billions on Cloud and not get anywhere,” Ames cautioned. □

continued from page s7, Maneuvering Through the Cloud

where you might where you can abstract applications or services through a combination of in house infrastructure or reach out to multiple Clouds.

New NIST Cloud Publication

To help you sort out what will work and not work for you, NIST is coming to your aid. You know the government is serious about a technology when NIST gets involved.

Mell said NIST is planning to create a series of NIST Special Publications in 2009 that will focus on what problems does cloud computing solve; what are the technical characteristics of cloud; and most importantly, how can we best leverage cloud computing and obtain security – the 800 pound gorilla that needs to be solved. □

NIST is planning to create a series of NIST Special Publications in 2009 that will focus on what problems does cloud computing solve; what are the technical characteristics of cloud; and most importantly, how can we best leverage cloud computing and obtain security.
